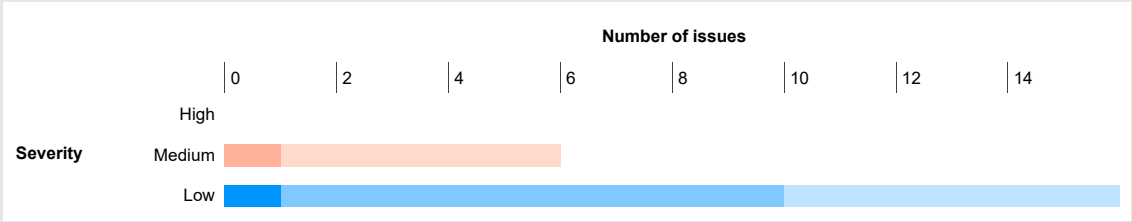
Burp Scanner Report

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	0	0	0
	Medium	0	1	5	6
	Low	1	9	6	16
	Information	267	14	0	281

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

9.5. https://testportal.zalaris.com/neptune/zmfp_photo_upload [IMAGESTR JSON parameter]

10. Cross-origin resource sharing

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/ui5theme/zalquartzlight/UI5
10.14. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/f/themes/zalquartzlight/library-parameters.json
10.15. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/m/themes/zalquartzlight/library-parameters.json
10.16. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/commons/themes/zalquartzlight/library-parameters.json
10.17. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/microchart/themes/zalquartzlight/library-parameters.json
10.18. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/tnt/themes/zalquartzlight/library-parameters.json
10.19. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/core/themes/zalquartzlight/library-parameters.json
10.20. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/layout/themes/zalquartzlight/library-parameters.json
10.21. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/table/themes/zalquartzlight/library-parameters.json
10.22. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/unified/themes/zalquartzlight/library-parameters.json
10.23. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/uxap/themes/zalquartzlight/library-parameters.json
10.24. https://testportal.zalaris.com/neptune/server/fontawesome/5.13.0/fa.js
10.25. https://testportal.zalaris.com/neptune/server/js/Core.js
10.26. https://testportal.zalaris.com/neptune/server/js/Debug.js
10.27. https://testportal.zalaris.com/neptune/server/js/IndexedDBShim.js
10.28. https://testportal.zalaris.com/neptune/server/js/crypto/aes.js
10.29. https://testportal.zalaris.com/neptune/server/js/please-wait/PleaseWait.js
10.30. https://testportal.zalaris.com/neptune/server/js/slick/Slick.js
10.31. https://testportal.zalaris.com/neptune/server/js/sun/suneditor.min.js
10.32. https://testportal.zalaris.com/neptune/server/sapui5/1.71/resources/sap-ui-core.js
10.33. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard
10.34. https://testportal.zalaris.com/neptune/zmfp_annual_statement
10.35. https://testportal.zalaris.com/neptune/zmfp_availability
10.36. https://testportal.zalaris.com/neptune/zmfp_dash_ess_lvreq_overview
10.37. https://testportal.zalaris.com/neptune/zmfp_dash_ess_next_salary
10.38. https://testportal.zalaris.com/neptune/zmfp_dash_ess_other_quotas
10.39. https://testportal.zalaris.com/neptune/zmfp_dash_ess_paid_vacation
10.40. https://testportal.zalaris.com/neptune/zmfp_dash_ess_sickness
10.41. https://testportal.zalaris.com/neptune/zmfp_dash_ess_time_reg
10.42. https://testportal.zalaris.com/neptune/zmfp_dash_ess_travel_paid
10.43. https://testportal.zalaris.com/neptune/zmfp_dash_ess_trvl_process
10.44. https://testportal.zalaris.com/neptune/zmfp_ess_payslip
10.45. https://testportal.zalaris.com/neptune/zmfp_home_screen
10.46. https://testportal.zalaris.com/neptune/zmfp_launch_ext_app
10.47. https://testportal.zalaris.com/neptune/zmfp_leave_request
10.48. https://testportal.zalaris.com/neptune/zmfp_personal_profile
10.49. https://testportal.zalaris.com/neptune/zmfp_photo_upload
10.50. https://testportal.zalaris.com/neptune/zmfp_quota_transfer
10.51. https://testportal.zalaris.com/neptune/zmfp_sal_letter
10.52. https://testportal.zalaris.com/neptune/zmfp_setup_wizard
10.53. https://testportal.zalaris.com/neptune/zmfp_team_status
10.54. https://testportal.zalaris.com/neptune/zmfp_time_entry_v2
10.55. https://testportal.zalaris.com/neptune/zmfp_time_statement
10.56. https://testportal.zalaris.com/neptune/zmfp_travel_create_expense_rep
10.57. https://testportal.zalaris.com/neptune/zmfp_travel_overview
10.58. https://testportal.zalaris.com/neptune/zmfp_universal_inbox
10.59. https://testportal.zalaris.com/neptune/zmfp_wt_compensation
10.60. https://testportal.zalaris.com/neptune/zsp_suppinfo_frontend

11. Cross-origin resource sharing: arbitrary origin trusted

11.1. https://testportal.zalaris.com/neptune/api/notifications/notifications
11.2. https://testportal.zalaris.com/neptune/efile_neptune_app_ess
11.3. https://testportal.zalaris.com/neptune/native/neptune_ajax
11.4. https://testportal.zalaris.com/neptune/public/application/neptune/nam/apk.jpg
11.5. https://testportal.zalaris.com/neptune/public/application/neptune/nam/appx.png
11.6. https://testportal.zalaris.com/neptune/public/application/neptune/nam/ipa.jpg
11.7. https://testportal.zalaris.com/neptune/public/application/zalaris_common_used/js/excel-builder.dist.min.js
11.8. https://testportal.zalaris.com/neptune/public/application/zalaris_common_used/js/imageresizer.js
11.9. https://testportal.zalaris.com/neptune/public/application/zalaris_common_used/js/jspdf.js
11.10. https://testportal.zalaris.com/neptune/public/application/zmfp_photo_upload/js/cropper1.min.js
11.11. https://testportal.zalaris.com/neptune/public/images/microsoft-azure-logo.svg
11.12. https://testportal.zalaris.com/neptune/public/media/
11.13. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5
11.14. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/f/themes/zalquartzlight/library-parameters.json
11.15. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/m/themes/zalquartzlight/library-parameters.json
11.16. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/commons/themes/zalquartzlight/library-parameters.json
11.17. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/microchart/themes/zalquartzlight/library-parameters.json
11.18. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/tnt/themes/zalquartzlight/library-parameters.json
11.19. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/core/themes/zalquartzlight/library-parameters.json
11.20. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/layout/themes/zalquartzlight/library-parameters.json
11.21. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/table/themes/zalquartzlight/library-parameters.json
11.22. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/unified/themes/zalquartzlight/library-parameters.json
11.23. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/uxap/themes/zalquartzlight/library-parameters.json
11.24. https://testportal.zalaris.com/neptune/server/fontawesome/5.13.0/fa.js
11.25. https://testportal.zalaris.com/neptune/server/js/Core.js
11.26. https://testportal.zalaris.com/neptune/server/js/Debug.js
11.27. https://testportal.zalaris.com/neptune/server/js/IndexedDBShim.js
11.28. https://testportal.zalaris.com/neptune/server/js/crypto/aes.js
11.29. https://testportal.zalaris.com/neptune/server/js/please-wait/PleaseWait.js

11.30. https://testportal.zalaris.com/neptune/server/js/slick/Slick.js
11.31. https://testportal.zalaris.com/neptune/server/js/sun/suneditor.min.js
11.32. https://testportal.zalaris.com/neptune/server/sapui5/1.71/resources/sap-ui-core.js
11.33. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard
11.34. https://testportal.zalaris.com/neptune/zmfp_annual_statement
11.35. https://testportal.zalaris.com/neptune/zmfp_availability
11.36. https://testportal.zalaris.com/neptune/zmfp_dash_ess_lvreq_overview
11.37. https://testportal.zalaris.com/neptune/zmfp_dash_ess_next_salary
11.38. https://testportal.zalaris.com/neptune/zmfp_dash_ess_other_quotas
11.39. https://testportal.zalaris.com/neptune/zmfp_dash_ess_paid_vacation
11.40. https://testportal.zalaris.com/neptune/zmfp_dash_ess_sickness
11.41. https://testportal.zalaris.com/neptune/zmfp_dash_ess_time_reg
11.42. https://testportal.zalaris.com/neptune/zmfp_dash_ess_travel_paid
11.43. https://testportal.zalaris.com/neptune/zmfp_dash_ess_trvl_process
11.44. https://testportal.zalaris.com/neptune/zmfp_ess_payslip
11.45. https://testportal.zalaris.com/neptune/zmfp_home_screen
11.46. https://testportal.zalaris.com/neptune/zmfp_launch_ext_app
11.47. https://testportal.zalaris.com/neptune/zmfp_leave_request
11.48. https://testportal.zalaris.com/neptune/zmfp_personal_profile
11.49. https://testportal.zalaris.com/neptune/zmfp_photo_upload
11.50. https://testportal.zalaris.com/neptune/zmfp_quota_transfer
11.51. https://testportal.zalaris.com/neptune/zmfp_sal_letter
11.52. https://testportal.zalaris.com/neptune/zmfp_setup_wizard
11.53. https://testportal.zalaris.com/neptune/zmfp_team_status
11.54. https://testportal.zalaris.com/neptune/zmfp_time_entry_v2
11.55. https://testportal.zalaris.com/neptune/zmfp_time_statement
11.56. https://testportal.zalaris.com/neptune/zmfp_travel_create_expense_rep
11.57. https://testportal.zalaris.com/neptune/zmfp_travel_overview
11.58. https://testportal.zalaris.com/neptune/zmfp_universal_inbox
11.59. https://testportal.zalaris.com/neptune/zmfp_wt_compensation
11.60. https://testportal.zalaris.com/neptune/zsp_suppinfo_frontend

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
/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview

14. Cross-domain POST

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-iViewID 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.portal.dsm.Terminator [ParamMapKey parameter]
15.18. 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 [%24DebugAction parameter]
15.19. 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]
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]
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]
15.22. 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]
15.23. 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]
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]
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]
15.26. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard [BUILD_VERSION JSON parameter]
15.27. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard [NUMBER_DECIMAL JSON parameter]
15.28. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard [NUMBER_GROUPING JSON parameter]
15.29. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard [TILE_INFO JSON parameter]
15.30. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard [TILE_TITLE JSON parameter]
15.31. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard [field_id parameter]
15.32. https://testportal.zalaris.com/neptune/zmfp_leave_request [field_id parameter]
15.33. https://testportal.zalaris.com/neptune/zmfp_photo_upload [IMAGESTR JSON parameter]
15.34. https://testportal.zalaris.com/neptune/zmfp_team_status [CAL_BEGDA JSON parameter]
15.35. https://testportal.zalaris.com/neptune/zmfp_team_status [CAL_ENDDA JSON parameter]
15.36. https://testportal.zalaris.com/neptune/zmfp_travel_overview [field_id parameter]
15.37. https://testportal.zalaris.com/neptune/zmfp_universal_inbox [ajax_value parameter]
15.38. https://testportal.zalaris.com/saml2/idp/sso [RelayState parameter]

15.39. https://testportal.zalaris.com/saml2/idp/sso [saml2sp parameter]
15.40. https://testportal.zalaris.com/sap/bc/gui/sap/its/webgui [~transaction parameter]

16. Suspicious input transformation (reflected)

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]
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]
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]
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]
16.5. 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/
17.3. https://testportal.zalaris.com/neptune/server/js/sun/suneditor.min.js

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/ZSP_SUPPINFO_FRONTEND
18.6. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard
18.7. 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]
22.2. 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.tar
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.js1
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/native/neptune_login_ping.1
23.39. https://testportal.zalaris.com/neptune/native/neptune_login_ping.7z
23.40. https://testportal.zalaris.com/neptune/native/neptune_login_ping.a
23.41. https://testportal.zalaris.com/neptune/native/neptune_login_ping.ar
23.42. https://testportal.zalaris.com/neptune/native/neptune_login_ping.bac
23.43. https://testportal.zalaris.com/neptune/native/neptune_login_ping.backup

23.44. https://testportal.zalaris.com/neptune/native/neptune_login_ping.bak
23.45. https://testportal.zalaris.com/neptune/native/neptune_login_ping.bz2
23.46. https://testportal.zalaris.com/neptune/native/neptune_login_ping.cbz
23.47. https://testportal.zalaris.com/neptune/native/neptune_login_ping.ear
23.48. https://testportal.zalaris.com/neptune/native/neptune_login_ping.exe
23.49. https://testportal.zalaris.com/neptune/native/neptune_login_ping.gz
23.50. https://testportal.zalaris.com/neptune/native/neptune_login_ping.inc
23.51. https://testportal.zalaris.com/neptune/native/neptune_login_ping.include
23.52. https://testportal.zalaris.com/neptune/native/neptune_login_ping.jar
23.53. https://testportal.zalaris.com/neptune/native/neptune_login_ping.lzma
23.54. https://testportal.zalaris.com/neptune/native/neptune_login_ping.old
23.55. https://testportal.zalaris.com/neptune/native/neptune_login_ping.rar
23.56. https://testportal.zalaris.com/neptune/native/neptune_login_ping.tar
23.57. https://testportal.zalaris.com/neptune/native/neptune_login_ping.tar.7z
23.58. https://testportal.zalaris.com/neptune/native/neptune_login_ping.tar.bz2
23.59. https://testportal.zalaris.com/neptune/native/neptune_login_ping.tar.gz
23.60. https://testportal.zalaris.com/neptune/native/neptune_login_ping.tar.lzma
23.61. https://testportal.zalaris.com/neptune/native/neptune_login_ping.tar.xz
23.62. https://testportal.zalaris.com/neptune/native/neptune_login_ping.war
23.63. https://testportal.zalaris.com/neptune/native/neptune_login_ping.wim
23.64. https://testportal.zalaris.com/neptune/native/neptune_login_ping.xz
23.65. https://testportal.zalaris.com/neptune/native/neptune_login_ping.zip

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/neptune/zmfp_setup_wizard

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

27.1. https://testportal.zalaris.com/neptune/ZMFP_DASH_ESS_LVREQ_OVERVIEW.view.js
27.2. https://testportal.zalaris.com/neptune/ZMFP_DASH_ESS_NEXT_SALARY.view.js
27.3. https://testportal.zalaris.com/neptune/ZMFP_DASH_ESS_OTHER_QUOTAS.view.js
27.4. https://testportal.zalaris.com/neptune/ZMFP_DASH_ESS_PAID_VACATION.view.js
27.5. https://testportal.zalaris.com/neptune/ZMFP_DASH_ESS_SICKNESS.view.js
27.6. https://testportal.zalaris.com/neptune/ZMFP_DASH_ESS_TIME_REG.view.js
27.7. https://testportal.zalaris.com/neptune/ZMFP_DASH_ESS_TRAVEL_PAID.view.js
27.8. https://testportal.zalaris.com/neptune/ZMFP_DASH_ESS_TRVL_PROCESS.view.js

28. HTML does not specify charset

28.1. https://testportal.zalaris.com/com.sap.portal.design.urdesigndata/themes/portal/sap_tradeshow_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

29. TLS certificate

1. HTTP request smuggling

Summary

Severity:	**Medium**
Confidence:	**Tentative**
Host:	**https://testportal.zalaris.com**
Path:	**/neptune/zmfp_photo_upload**

Issue description

HTTP request smuggling vulnerabilities arise when websites route HTTP requests through web servers with inconsistent HTTP parsing.

By supplying a request that different servers interpret as having different lengths, an attacker can poison the back-end TCP/TLS socket and prepend arbitrary data to the next request. Depending on the website's functionality, this can be used to bypass front-end security rules, access internal systems, poison web caches, and launch assorted attacks on users who are actively browsing the site.

Issue remediation

You can resolve all variants of this vulnerability by configuring the front-end server to exclusively use HTTP/2 when communicating with back-end systems. Alternatively, you could

ensure all servers in the chain run the same web server software with the same configuration. Disabling back-end connection reuse is likely to reduce the impact of this vulnerability, but does not mitigate all possible exploits.

Specific instances of this vulnerability can be resolved by reconfiguring the front-end server to normalize ambiguous requests before routing them onward. Alternatively, you could configure the back-end server to reject the message and close the connection when it encounters an ambiguous request.

References

- HTTP Request Smuggling
- HTTP Desync Attacks

Vulnerability classifications

- CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')
- CAPEC-33: HTTP Request Smuggling

Request 1

```
POST /neptune/zmfp_photo_upload?ajax_id=SAVE&ajax_applid=ZMFP_PHOTO_UPLOAD&sap-client=650&dxp=21100006&field_id=00096&FbMi=1857492283 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655371724869; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.f375538321d94ce5
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-f375538321d94ce5-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: keep-alive
Transfer-Encoding: chunked
Content-Length: 162299

279ed
{"GWA_PHOTO":{"EMPPHOTOURL":"","IMAGESTR":"
/2wBDAAMCAgICAgMCAgIDAwMDBAYEBAQEBAgGBgUGCQgKCgkICQkKDA8MCgsOCwkJDRENDg8QEBEQCgwSExIQEw8QEBD/2wBDAQM
...[SNIP]...
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 09:38:13 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: application/json; charset=utf-8
Content-Length: 324535
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://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

{"modeloPageUploadData":{"EMPPHOTOURL":"
/2wBDAAMCAgICAgMCAgIDAwMDBAYEBAQEBAgGBgUGCQgKCgkICQkKDA8MCgsOCwkJDRENDg8QEBEQCgwSExIQEw8QEBD/2wBDAQMDAwQDBAgEB
...[SNIP]...
```

Request 2

```
POST /neptune/zmfp_photo_upload?ajax_id=SAVE&ajax_applid=ZMFP_PHOTO_UPLOAD&sap-client=650&dxp=21100006&field_id=00096&s7X0=957260052 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655371724869; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.f375538321d94ce5
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-f375538321d94ce5-01
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: keep-alive
Transfer-Encoding: chunked
Content-Length: 162300

279ed
{"GWA_PHOTO":{"EMPPHOTOURL":"","IMAGESTR":"
/2wBDAAMCAgICAgMCAgIDAwMDBAYEBAQEBAgGBgUGCQgKCgkICQkKDA8MCgsOCwkJDRENDg8QEBEQCgwSExIQEw8QEBD/2wBDAQM
...[SNIP]...
```

---

2. Cross-site request forgery

There are 4 instances of this issue:

- /irj/servlet/prt/portal/prtroot/com.sap.portal.dsm.Terminator
- /neptune/native/fetch_csrf
- /neptune/native/neptune_login_ping.html
- /neptune/zsp_suppinfo_frontend

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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349919451; 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%253A9OWEbXwMXQNeg6gBLVUbPw--7hjmzZmqUbZjAdzxMnFpBw--%261655349966919&
SerWinIdString=&Autoclose=1000&DebugSet=&ParamMapCmd=LIST&ParamMa
...[SNIP]...
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:26:09 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/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://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
Content-Length: 304

/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen?sap-ext-sid=9OWEbXwMXQNeg6gBLVUbPw--7hjmzZmqUbZjAdzxMnFpBw--&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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655362716847; 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://jzFhbBkybNbZlHTCxS.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%253A9OWEbXwMXQNeg6gBLVUbPw--7hjmzZmqUbZjAdzxMnFpBw--%261655349966919&
SerWinIdString=&Autoclose=1000&DebugSet=&ParamMapCmd=LIST&ParamMa
...[SNIP]...
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 06:59:10 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/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://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
Content-Length: 304

/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen?sap-ext-sid=9OWEbXwMXQNeg6gBLVUbPw--7hjmzZmqUbZjAdzxMnFpBw--&sap-
sessioncmd=USR_ABORT&~SAPSessionCmd=USR_ABORT&SAPWP_A
...[SNIP]...
```

2.2. https://testportal.zalaris.com/neptune/native/fetch_csrf

Summary

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

Issue detail

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

Request 1

```
POST /neptune/native/fetch_csrf?sap-client=650 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454
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: |40a05d456dfc4d6999abcff0b7c296be.c598fe44400b4293
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-c598fe44400b4293-01
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, 16 Jun 2022 03:10:14 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
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://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
Content-Length: 88
Connection: close

FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
```

Request 2

```
POST /neptune/native/fetch_csrf?sap-client=650 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
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://DYWoaVBxztKzMKUDDd.com/
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.c598fe44400b4293
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-c598fe44400b4293-01
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, 16 Jun 2022 07:21:58 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
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://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
Content-Length: 88
Connection: close

FpYmCInd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
```

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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454
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: |40a05d456dfc4d6999abcff0b7c296be.6de84b3c161a4be8
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-6de84b3c161a4be8-01
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, 16 Jun 2022 03:10:14 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: 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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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


<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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
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://GvmRMpymlxZbLccVYf.com/
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.6de84b3c161a4be8
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-6de84b3c161a4be8-01
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, 16 Jun 2022 07:23:00 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: 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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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


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

2.4. https://testportal.zalaris.com/neptune/zsp_suppinfo_frontend

Summary

Severity:	**Medium**
Confidence:	**Tentative**
Host:	**https://testportal.zalaris.com**
Path:	**/neptune/zsp_suppinfo_frontend**

Issue detail

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

Request 1

```
POST /neptune/zsp_suppinfo_frontend?ajax_id=POR_GET_ITEM&ajax_applid=ZSP_SUPPINFO_FRONTEND&sap-client=650&dxp=21100006&field_id=00049 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655350119630; 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
X-Requested-With: XMLHttpRequest
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, 16 Jun 2022 03:28:45 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; charset=utf-8
content-length: 213
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://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

{"modeloVerticalLayoutData":
{"ITEMID":"00000000","UCN":"","CLIENT":"","CDATE":"","CTIME":"000000","UNAME":"","TLOCK":false,"TLOCKBY":"","ROLES":"","BUKRS":"","EMAIL":"","PHONE":"","LOCKED_TEXT":"","IN
...[SNIP]...

Request 2

POST /neptune/zsp_suppinfo_frontend?ajax_id=POR_GET_ITEM&ajax_applid=ZSP_SUPPINFO_FRONTEND&sap-client=650&dxp=21100006&field_id=00049 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655364518414; 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://SeuYfPtgsayRsEkCCz.com/
Content-Type: application/json
X-Requested-With: XMLHttpRequest
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, 16 Jun 2022 07:28:43 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: 213
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://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

{"modeloVerticalLayoutData":
{"ITEMID":"00000000","UCN":"","CLIENT":"","CDATE":"","CTIME":"000000","UNAME":"","TLOCK":false,"TLOCKBY":"","ROLES":"","BUKRS":"","EMAIL":"","PHONE":"","LOCKED_TEXT":"","IN

...[SNIP]...

---

3. Session token in URL

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://testportal.zalaris.com**
Path:	**/webdynpro/resources/sap.com/sso~otp~wd/OTP**

Issue detail

The URL in the request appears to contain a session token within the query string:

- https://testportal.zalaris.com/webdynpro/resources/sap.com/sso~otp~wd/OTP?sap-wd-appwndid=84f3e05bed2411ecaca400000013abbe&sap-wd-cltwndid=84f3e05aed2411ec8a3600000013abbe&sap-wd-norefresh=X&sap-wd-secure-id=7kg80OqroAjKFuQbUgkIMA%3D%3D&sap-sessioncmd=unload

Issue background

Sensitive information within URLs may be logged in various locations, including the user's browser, the web server, and any forward or reverse proxy servers between the two endpoints. URLs may also be displayed on-screen, bookmarked or emailed around by users. They may be disclosed to third parties via the Referer header when any off-site links are followed. Placing session tokens into the URL increases the risk that they will be captured by an attacker.

Issue remediation

Applications should use an alternative mechanism for transmitting session tokens, such as HTTP cookies or hidden fields in forms that are submitted using the POST method.

Vulnerability classifications

- CWE-200: Information Exposure
- CWE-384: Session Fixation
- CWE-598: Information Exposure Through Query Strings in GET Request
- CAPEC-593: Session Hijacking

Request 1

```
GET /webdynpro/resources/sap.com/sso~otp~wd/OTP?sap-wd-appwndid=84f3e05bed2411ecaca400000013abbe&sap-wd-cltwndid=84f3e05aed2411ec8a3600000013abbe&sap-wd-norefresh=X&sap-wd-secure-id=7kg80OqroAjKFuQbUgkIMA%3D%3D&sap-sessioncmd=unload HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655414366207; 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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 307 Temporary Redirect
Date: Thu, 16 Jun 2022 21:19:28 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
location: https://testportal.zalaris.com/nea/v1/authenticate?neaRelayState=ZHQPORTAL%3ahttps%3a%2f%2ftestportal.zalaris.com%2fwebdynpro%2fresources%2fsap.com%2fsso%7eotp%7ewd%2fOTP%3fsap-wd-appwndid%3d84f3e05bed2411ecaca400000013abbe%26sap-wd-cltwndid%3d84f3e05aed2411ec8a3600000013abbe%26sap-wd-norefresh%3dX%26sap-wd-secure-id%3d7kg80OqroAjKFuQbUgkIMA%253D%253D%26sap-sessioncmd%3dunload
content-length: 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
X-Content-Type-Options: nosniff
Connection: close
```

4. 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

4.1. 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

Request 1

```
GET /irj/portal HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:32 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
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://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: PortalAlias=portal; Path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 13739

<!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]...
```

4.2. 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**

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=20180424152222 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349919451; 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, 16 Jun 2022 03:26:10 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
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://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
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]...
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]...
```

4.3. 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, 16 Jun 2022 03:08:30 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-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://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: com.sap.engine.security.authentication.original_application_url=GET#0kzh
%2F%2FAyUjkjm0k4o9RrxRftCqGFdLeQFH%2FAmJoT4DKc%2BOmwgCXg2GlZ4RP3V7tycXIkpU0%2FS63yj263pKn4UdBlhVyCnQD069VrKFuZLwzz6L%2Fv6GHnjf2isj8lCQV8cX
X09dqvnNMnZ5cmoql0Su99%2F7%2BCWYKXUq7585jQ3tAxV7Cv34kfrFoloYCja%2Fi4StuoDaQcAPOJnW5jpcR3CPo1GEwl6%2B5l9TL931O7YtM%3D;Path=/nea
/v1/authenticate;HttpOnly; SameSite=None; Secure
set-cookie: saplb_PORTAL=(J2EE1289120)1289150; 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]...
```

4.4. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: 20220616 053046 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: 9A62C15D94D21020E10000000ADC9967
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://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]...
/_merge',["./isPlainObject"],function(a){"use 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]...
```

4.5. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:50 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
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://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
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]...

---

5. 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 static code analysis, which may lead to false positives that are not actually exploitable. The relevant code and execution paths should be reviewed 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:32 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
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://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: PortalAlias=portal; Path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 13739

<!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,en-GB;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/97.0.4692.71 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:33:13 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: application/x-javascript
last-modified: Fri, 11 Mar 2022 05:02:00 GMT
cache-control: max-age=604800
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://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

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;portalUrl=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=portalUrl;
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;`

---

6. 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 static code analysis, which may lead to false positives that are not actually exploitable. The relevant code and execution paths should be reviewed 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

6.1. 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349919451
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, 16 Jun 2022 03:26:04 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
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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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


//** 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);`

6.2. 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349919451
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, 16 Jun 2022 03:26:04 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
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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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


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

6.3. 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=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW&XPROFILE=ESS&
XQUERY=ZSTKPTMC1_REG_TIME_ESS HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349919451; 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, 16 Jun 2022 03:26:23 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; 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://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: 5828

<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_tradeshow_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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349919451
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, 16 Jun 2022 03:26:04 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
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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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


//** 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);`

6.4. 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=ZSTKPTMC1_REG_TIME_ESS HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349919451; 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, 16 Jun 2022 03:26:23 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; 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://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: 5828

<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_tradeshow_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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349919451
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, 16 Jun 2022 03:26:04 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
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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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


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

6.5. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:32 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
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://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: 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_tradeshow_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,en-GB;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/97.0.4692.71 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:33:15 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/x-javascript
last-modified: Tue, 30 Nov 2021 05:06:49 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://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


//** 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(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);`

6.6. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:32 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
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://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: 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_tradeshow_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,en-GB;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/97.0.4692.71 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:33:15 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/x-javascript
last-modified: Tue, 30 Nov 2021 05:06:49 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://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


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

6.7. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:39 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
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: 13343

<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_tradeshow_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,en-GB;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/97.0.4692.71 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:33:15 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/x-javascript
last-modified: Tue, 30 Nov 2021 05:06:49 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://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


//** 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(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);`

6.8. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:39 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
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: 13343

<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_tradeshow_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,en-GB;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/97.0.4692.71 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:33:15 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/x-javascript
last-modified: Tue, 30 Nov 2021 05:06:49 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://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


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

7. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:38 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
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 06:39:42 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://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

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

---

8. 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, 16 Jun 2022 03:08:29 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
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]...
```

9. Cross-site scripting (reflected)

There are 5 instances of this issue:

- /neptune/zalaris_launchpad_standard [NUMBER_DECIMAL JSON parameter]
- /neptune/zalaris_launchpad_standard [NUMBER_GROUPING JSON parameter]
- /neptune/zalaris_launchpad_standard [TILE_INFO JSON parameter]
- /neptune/zalaris_launchpad_standard [TILE_TITLE JSON parameter]
- /neptune/zmfp_photo_upload [IMAGESTR 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

9.1. 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 **qxqxr<script>alert(1)</script>vpfvrafy3b3** 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349014046
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-type: text/plain
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.9254b0426ad34dfa
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-9254b0426ad34dfa-01
Content-Length: 5175
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":{},"WA_CLIENT_INFO":{"BUILD_VERSION":"21.10.0006"},"IT_APP_CACHE":{},"IT_GUID":{},"WA_MENU_LIST":{},"WA_CATEGORY":{},"WA_USER_DEFAULT":
{"DATFM":"1","DCPFM":"","LANGU":"E","TZONE":"","TZONE_DESCRIPT":"","TIMEFM":"0","NUMBER_GROUPING":"","NUMBER_DECIMAL":"qxqxr<script>alert(1)
<\/script>vpfvrafy3b3","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, 16 Jun 2022 09:02:26 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: 409663
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://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

{"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_DESCRIPT":"","TIMEFM":"0","NUMBER_GROUPING":"","NUMBER_DECIMAL":"qxqxr<script>alert(1)
</script>vpfvrafy3b3","EDIT":true},"modelAppCacheImageDataUpdateData":[2,"GUID","CONTENT"],"modelAppCacheGlobalSettingsData":
{"GLOBAL_STYLE":"","RUNTIME_LANGUAGE":"E","BANNER":"","APP_START":""},"modelAppCacheSplitViewDat
...[SNIP]...
```

9.2. 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 **apuo2<script>alert(1)</script>jcdvbdlenoi** 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&dxp=21100006&field_id=00384&
ajax_value=PORTAL%7CD%7C%7C%7C HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349014046
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-type: text/plain
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.9254b0426ad34dfa
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-9254b0426ad34dfa-01
Content-Length: 5175
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":{},"WA_CLIENT_INFO":{"BUILD_VERSION":"21.10.0006"},"IT_APP_CACHE":{},"IT_GUID":{},"WA_MENU_LIST":{},"WA_CATEGORY":{},"WA_USER_DEFAULT":
{"DATFM":"1","DCPFM":"","LANGU":"E","TZONE":"","TZONE_DESCRIPT":"","TIMEFM":"0","NUMBER_GROUPING":"apuo2<script>alert(1)
<\/script>jcdvbdlenoi","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, 16 Jun 2022 08:49:08 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: 409663
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://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

{"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_DESCRIPT":"","TIMEFM":"0","NUMBER_GROUPING":"apuo2<script>alert(1)
</script>jcdvbdlenoi","NUMBER_DECIMAL":"","EDIT":true},"modelAppCacheImageDataUpdateData":[2,"GUID","CONTENT"],"modelAppCacheGlobalSettingsData":
{"GLOBAL_STYLE":"","RUNTIME_LANGUAGE":"E","BANNER":"","APP_START":""},"model
...[SNIP]...
```

9.3. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard [TILE_INFO JSON parameter]

Summary

Severity: **Information**

Confidence: **Certain**

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

Path: **/neptune/zalaris_launchpad_standard**

Issue detail

The value of the **TILE_INFO** JSON parameter is copied into the HTML document as plain text between tags. The payload **a56ws<script>alert(1)</script>ub678ujlies** was submitted in the TILE_INFO 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=SAVE_USER_FAV&ajax_applid=ZALARIS_LAUNCHPAD_STANDARD&sap-client=650&dxp=21100006&field_id=00385
HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655350055042; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-type: text/plain
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.5d717e5d02854e6d
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-5d717e5d02854e6d-01
Content-Length: 3647
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_FAV_LIST":[{"IMAGEDATA":"","ICON_IMAGEDATA":"","IMAGE_CONTENT":"","STATEFUL":false,"PARENTS":"","URL_LONG":"/irj/servlet/prt/portal/prtroot
/com.sap.ip.bi.designstudio.nw.portal.ds?APPLICATION=ZGE
...[SNIP]...
"CHART_GUID":"","MANIFEST":"","TILE_TEXT":"","GUID":"00163EDC07D11ED9A79A9EE959EF27CE","NAME":"Registered
time","APPLID":"","ACTIVATED":true,"TILE_ICON":"sap-icon://line-chart-time-axis","TILE_INFO":"a56ws<script>alert(1)<\/script>ub678ujlies","TILE_TITLE":"Registered
time","TILE_TYPE":"","TILE_NUMBER":"","TILE_UNIT":"","TILE_INFOSTATE":"None","UPDDAT":"20190819","UPDTIM":"102158","UPDNAM":"VJSP","CREDAT":"20190702","CRET
IM":"162330","CRE
...[SNIP]...
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 08:27:41 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: 266
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://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

{"modelAppCacheTilesFavData":
[9,"GUID","SORT","BACK_WIDTH","TILE_HEIGHT","FORCE_ROW","TILE_TITLE","TILE_INFO","NATURAL_WIDTH","NATURAL_HEIGHT","00163EDC07D11ED9A79A9EE959EF
27CE",2,"Small","",false,"Registered time","a56ws<script>alert(1)</script>ub678ujlies","",""]}
```

9.4. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard [TILE_TITLE JSON parameter]

Summary

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

Issue detail

The value of the **TILE_TITLE** JSON parameter is copied into the HTML document as plain text between tags. The payload **e6x8y<script>alert(1)</script>frrqc** was submitted in the TILE_TITLE 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=SAVE_USER_FAV&ajax_applid=ZALARIS_LAUNCHPAD_STANDARD&sap-client=650&dxp=21100006&field_id=00385
HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655350055042; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.5d717e5d02854e6d
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-5d717e5d02854e6d-01
Content-Length: 3647
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_FAV_LIST":[{"IMAGEDATA":"","ICON_IMAGEDATA":"","IMAGE_CONTENT":"","STATEFUL":false,"PARENTS":"","URL_LONG":"/irj/servlet/prt/portal/prtroot
/com.sap.ip.bi.designstudio.nw.portal.ds?APPLICATION=ZGE
...[SNIP]...
TILE_TEXT":"","GUID":"00163EDC07D11ED9A79A9EE959EF27CE","NAME":"Registered time","APPLID":"","ACTIVATED":true,"TILE_ICON":"sap-icon://line-chart-time-
axis","TILE_INFO":"","TILE_TITLE":"Registered timee6x8y<script>alert(1)
<\/script>frrqc","TILE_TYPE":"","TILE_NUMBER":"","TILE_UNIT":"","TILE_INFOSTATE":"None","UPDDAT":"20190819","UPDTIM":"102158","UPDNAM":"VJSP","CREDAT":"2019070
2","CRETIM":"162330","CRENAM":"VJSP","SORT":"00002","VIS
...[SNIP]...
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 08:29:38 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: 260
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://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

{"modelAppCacheTilesFavData":
[9,"GUID","SORT","BACK_WIDTH","TILE_HEIGHT","FORCE_ROW","TILE_TITLE","TILE_INFO","NATURAL_WIDTH","NATURAL_HEIGHT","00163EDC07D11ED9A79A9EE959EF
27CE",2,"Small","",false,"Registered timee6x8y<script>alert(1)</script>frrqc","","","",""]}
```

9.5. https://testportal.zalaris.com/neptune/zmfp_photo_upload [IMAGESTR JSON parameter]

Summary

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

Issue detail

The value of the **IMAGESTR** JSON parameter is copied into the HTML document as plain text between tags. The payload **jmxol<script>alert(1)</script>tjc93j4ojn5** was submitted in the IMAGESTR 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_photo_upload?ajax_id=SAVE&ajax_applid=ZMFP_PHOTO_UPLOAD&sap-client=650&dxp=21100006&field_id=00096 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349983849; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-type: text/plain
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.f375538321d94ce5
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-f375538321d94ce5-01
Content-Length: 162285
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GWA_PHOTO":{"EMPPHOTOURL":"","IMAGESTR":"data:image\/jpeg;base64,\/9j\/4AAQSkZJRgABAQAAAQABAAD
\/2wBDAAMCAgICAgMCAgIDAwMDBAYEBAQEBAgGBgUGCQgKCgkICQkKDA8MCgsOCwkJDRENDg8QEBEQCgwSExIQEw8QEBD\/2wBDAQMDA
...[SNIP]...
UncfUEDGbJwOlVYqwVJlhPYVSRSRJTGNZgOO9ACr90VLJYFgKLBYYCSSTVFC0AJnJoAWgBCe1AC0AITQAo6UABOKAEFACk4oAQHJoAWgBM5NAC0AIT2FAC0ABOKAJov9
WK0jsYz3B3CDnr6UN2EotkO4sSTSi7myVgqthixnMgqL3Y0T9KZRDLJn5V6dzUtktn\/2Q==jmxol<script>alert(1)<\/script>tjc93j4ojn5"}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 09:02:50 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/json; charset=utf-8
Content-Length: 324576
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://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

{"modeloPageUploadData":{"EMPPHOTOURL":"
/2wBDAAMCAgICAgMCAgIDAwMDBAYEBAQEBAgGBgUGCQgKCgkICQkKDA8MCgsOCwkJDRENDg8QEBEQCgwSExIQEw8QEBD/2wBDAQMDAwQDBAgEB
...[SNIP]...
7mUncfUEDGbJwOlVYqwVJIhPYVSRSRJTGNZgOO9ACr90VLJYFgKLBYYCSSTVFC0AJnJoAWgBCe1AC0AITQAo6UABOKAEFACk4oAQHJoAWgBM5NAC0AIT2FAC0ABOKAJo
v9WK0jsYz3B3CDnr6UN2EotkO4sSTSi7myVgqthixnMgqL3Y0T9KZRDLJn5V6dzUtktn/2Q==jmxol<script>alert(1)</script>tjc93j4ojn5"}}
```

---

10. Cross-origin resource sharing

There are 60 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/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_lvreq_overview
- /neptune/zmfp_dash_ess_next_salary
- /neptune/zmfp_dash_ess_other_quotas
- /neptune/zmfp_dash_ess_paid_vacation
- /neptune/zmfp_dash_ess_sickness
- /neptune/zmfp_dash_ess_time_reg
- /neptune/zmfp_dash_ess_travel_paid
- /neptune/zmfp_dash_ess_trvl_process

- /neptune/zmfp_ess_payslip
- /neptune/zmfp_home_screen
- /neptune/zmfp_launch_ext_app
- /neptune/zmfp_leave_request
- /neptune/zmfp_personal_profile
- /neptune/zmfp_photo_upload
- /neptune/zmfp_quota_transfer
- /neptune/zmfp_sal_letter
- /neptune/zmfp_setup_wizard
- /neptune/zmfp_team_status
- /neptune/zmfp_time_entry_v2
- /neptune/zmfp_time_statement
- /neptune/zmfp_travel_create_expense_rep
- /neptune/zmfp_travel_overview
- /neptune/zmfp_universal_inbox
- /neptune/zmfp_wt_compensation
- /neptune/zsp_suppinfo_frontend

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

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.

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
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363557512
```

Response 1

```
HTTP/1.1 200 OK
```

```
Date: Thu, 16 Jun 2022 07:17:46 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: 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 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.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

{"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.

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=1100
HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349578618
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.03366d2d5fad4107
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-03366d2d5fad4107-01
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, 16 Jun 2022 03:19:30 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; 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://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

{"modelpageDetailViewerData":
{"PERNR":"00000000","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.

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MbIRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:21:44 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: 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://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

{}
```

10.4. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:24:12 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: 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://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

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

.....7$ &,7,,,,77,,,/,,1,,,+,0,,,,,,4,,-4,,,,-,,4,,,,,,/,.,.....
...[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.

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842

Response 1

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:24:31 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/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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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

.PNG
.
...IHDR.....>..z....tEXtSoftware.Adobe ImageReadyq.e<...&iTXtXML: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.

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842

Response 1

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:25:36 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: image/jpeg
content-length: 4096
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://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

.....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.

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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655364518414
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, 16 Jun 2022 07:31:01 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: 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://*.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
```

```
!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]...
```

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.

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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655364518414
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, 16 Jun 2022 07:30:53 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/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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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

/*
* 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]...
```

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.

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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655364518414; 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, 16 Jun 2022 07:32:17 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
Content-Length: 307551
dxp-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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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

!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.

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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655364518414
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, 16 Jun 2022 07:31:54 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-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: 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://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

/*!
* 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.

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655364518414
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:36:08 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: image/svg+xml
Content-Length: 3651
dxp-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://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

<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.

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655364518414
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:31:45 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
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://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
```

10.13. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655364518414
```

Response 1

```
HTTP/1.1 200 OK
Date: 20220616 093439 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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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
```

10.14. 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.

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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
```

```
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
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, 16 Jun 2022 07:44:00 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: application/json
content-length: 977
dxp-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://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

{
  "css-selector": "sapFAvatarColorAccent@{accentIndex}",
  "color-param": "sapUiAccent@{accentIndex}",
  "_sap_f_DynamicPageHeader_PaddingBottom": "1rem",
  "_sap_f_Card_ContentPadding": "1rem",
  "_sap_
...[SNIP]...
```

10.15. 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
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, 16 Jun 2022 07:44:09 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
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://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

{
  "_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]...
```

10.16. 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
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, 16 Jun 2022 07:45:34 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: 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://*.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

{
  "_sap_suite_ui_commons_StatusIndicator_SmallLabelMargin": "0.375rem",
  "_sap_suite_ui_commons_StatusIndicator_MediumLabelMargin": "0.5rem",
  "_sap_suite_ui_commons_StatusIndicator_LargeLabelMargin"
...[SNIP]...
```

10.17. 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
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, 16 Jun 2022 07:45:29 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: 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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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

{
  "_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]...
```

10.18. 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
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, 16 Jun 2022 07:44:21 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/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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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

{
  "_sap_tnt_NavigationList_ItemHeight": "2.75rem",
  "_sap_tnt_NavigationList_NoIconsGroupPadding": "1rem",
  "_sap_tnt_NavigationList_NoIconsNestedItemPadding": "2rem",
  "_sap_tnt_ToolHeader_ITHOverfl
...[SNIP]...
```

10.19. 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
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, 16 Jun 2022 07:45:01 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
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://*.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

{
  "sapBrandColor": "#3079BF",
  "sapHighlightColor": "#265f96",
  "sapBaseColor": "#fff",
  "sapShellColor": "#fff",
  "sapBackgroundColor": "#f9f9fd",
  "sapFontFamily": "\"72full\", Arial, Helvetica, sa
...[SNIP]...
```

10.20. 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
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, 16 Jun 2022 07:45:08 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
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://*.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

{
  "_sap_ui_layout_ColumnLayout_formColumnMaxXL": "4",
  "_sap_ui_layout_ColumnLayout_formColumnMaxL": "3",
  "_sap_ui_layout_ColumnLayout_formColumnMaxM": "2",
  "_sap_ui_layout_ColumnLayout_formColumnM
...[SNIP]...
```

10.21. 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
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, 16 Jun 2022 07:47:18 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
Content-Length: 6448
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
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://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

{
  "_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]...
```

10.22. 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
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, 16 Jun 2022 07:47:31 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: 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
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://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

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

10.23. 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
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, 16 Jun 2022 07:47:09 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
content-length: 492
dxp-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://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

{
  "sapUiFiori3AnchorBarBottomShadow": "inset 0 -0.0625rem #d9d9d9",
  "sapUiFiori3ABUnderlineOffsetAndHeight": "0.188rem",
  "sapUiFiori3ABUnderlineTopRadius": "0.125rem",
  "sapUiFiori3HSBottomShadow":
...[SNIP]...
```

10.24. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:46:18 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: 71860
dxp-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://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

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]...
```

10.25. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:46:22 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
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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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 AppCache=
{Initialized:!1,Encrypted:"",CurrentUname:"",CurrentApp:"",CurrentConfig:"",CurrentLanguage:"",AppVersion:"",StartApp:"",navNotif:!1,Url:"",UrlBase:"",Client:"",Passcode:"",Auth:"",en
able
...[SNIP]...
```

10.26. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:46:53 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/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://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

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]...
```

10.27. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
```

Response 1

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:46:56 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
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://*.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 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]...

10.28. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146

Response 1

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:48:06 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/x-javascript
Content-Length: 15627
dxp-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://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

/*
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]...
```

10.29. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:48:18 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/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://*.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

/*! 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]...
```

10.30. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MbIRdOCLc/kjOPX0D/p|1655349014046|1655365359146
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:48:28 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: 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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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

/*! 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]...

10.31. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365719420

Response 1

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:50:23 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: 2328807
dxp-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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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

!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]...

10.32. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365719420

Response 1

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:50:41 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: 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 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.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]...
```

10.33. 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&dxp=21100006&
field_id=00053&ajax_value=ZMFP_SETUP_WIZARD HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655350119630; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.2530fa39f249449a
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-2530fa39f249449a-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, 16 Jun 2022 03:29:24 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: 172
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://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

{"modelAppCacheAppTimestampData":{"APPLID":"ZMFP_SETUP_WIZARD","LANGUAGE":"","UPDDAT":"20220616","UPDTIM":"002944","INVALID":false,"DESCR":"MFP:
Application Setup Wizard"}}
```

10.34. 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&dxp=21100006&field_id=00113 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349841642
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.4c0e1ca49a174eef
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-4c0e1ca49a174eef-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, 16 Jun 2022 03:24:02 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: application/json; charset=utf-8
content-length: 88
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://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"]}
```

10.35. 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&dxp=21100006&field_id=00111 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349649037
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.9c175d389d4f4e3d
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-9c175d389d4f4e3d-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, 16 Jun 2022 03:20:50 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/json; charset=utf-8
content-length: 957
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://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":
[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]...
```

10.36. https://testportal.zalaris.com/neptune/zmfp_dash_ess_lvreq_overview

Summary

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

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_lvreq_overview?ajax_id=GET_ESS_LEAVE_REQUESTS&ajax_applid=ZMFP_DASH_ESS_LVREQ_OVERVIEW&sap-client=650&dxp=21100006&field_id=00061 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349428759
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.6284344f2b304768
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-6284344f2b304768-01
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, 16 Jun 2022 03:17:09 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: 862
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://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

{"modelleaveReqDialogTableData":
[9,"USER_ID","LEAVE_TYPE_ICON","START_DATE","END_DATE","START_TIME","END_TIME","STATUS_ICON","STATUS_COLOR","DESCRIPTION","00034448","sap-icon://general-leave-request",
...[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.

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&dxp=21100006&field_id=00089 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349075680
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.aeabb0a80e07450e
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-aeabb0a80e07450e-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, 16 Jun 2022 03:11:26 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: 1570
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://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

{"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_dash_ess_other_quotas

Summary

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

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_other_quotas?ajax_id=GET_ESS_OTHER_QUOTAS&ajax_applid=ZMFP_DASH_ESS_OTHER_QUOTAS&sap-client=650&dxp=21100006&
field_id=00041 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349428759
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.fd5ceef397014551
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-fd5ceef397014551-01
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, 16 Jun 2022 03:17:30 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/json; charset=utf-8
content-length: 409
```

```
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://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

{"modeltabOtherQuotasData":[6,"USER_ID","TIME_TEXT","DEDUCT_BEGIN","DEDUCT_END","ENTITLE","AVAILABLE","650-00034448","Time off
overtimer","20220101","20221231","15.00 Hours","0.00 Hours","650-00034448
...[SNIP]...
```

10.39. https://testportal.zalaris.com/neptune/zmfp_dash_ess_paid_vacation

Summary

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

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_paid_vacation?ajax_id=GET_ESS_PAID_VACATION&ajax_applid=ZMFP_DASH_ESS_PAID_VACATION&sap-client=650&dxp=21100006&
field_id=00047 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349356829
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.b246abcccaa14049
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-b246abcccaa14049-01
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, 16 Jun 2022 03:16:52 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: application/json; charset=utf-8
content-length: 260
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://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

{"modelpaidVacDialogTableData":
[7,"PERNR","QUOTA_TEXT","DATE_FROM","DATE_TO","ENTITLED","AVAILABLE","UOM","00034448","Vacation","20220101","20221231",25.00000,25.00000,"Days","00034448","
Vacation from
...[SNIP]...
```

10.40. https://testportal.zalaris.com/neptune/zmfp_dash_ess_sickness

Summary

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

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_sickness?ajax_id=GET_SICKNESS&ajax_applid=ZMFP_DASH_ESS_SICKNESS&sap-client=650&dxp=21100006&field_id=00021 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349428759
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.a7776eb903b94895
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-a7776eb903b94895-01
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, 16 Jun 2022 03:18:01 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: 846
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://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

{"modelDataSicknessESSData":[8,"NAME","PERNR","PERIOD","MONTH","PERCENTAGE","RE_CALC_DAYS","WDAYS","YEAR_MON","Jostein Hansen","00034448",7,"JUL",0,"0
","22.00 ","202107","Jostein Hansen","00034448",8
...[SNIP]...
```

10.41. https://testportal.zalaris.com/neptune/zmfp_dash_ess_time_reg

Summary

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

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_time_reg?ajax_id=GET_TIME_REGISTRATION&ajax_applid=ZMFP_DASH_ESS_TIME_REG&sap-client=650&dxp=21100006&field_id=00061
HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349075680
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.3f56ce107bba4660
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-3f56ce107bba4660-01
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, 16 Jun 2022 03:11:58 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: 615
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://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

{"modelcalTimeRegESSData":[2,"Date","Type","2022/06/04","NonWorking","2022/06/05","Type01","2022/06/05","NonWorking","2022/06/06","Type01","2022
/06/06","NonWorking","2022/06/07","Type08","2022/06/11",
...[SNIP]...
```

10.42. https://testportal.zalaris.com/neptune/zmfp_dash_ess_travel_paid

Summary

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

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_travel_paid?ajax_id=GET_TRAVEL_PAID_DETAILS&ajax_applid=ZMFP_DASH_ESS_TRAVEL_PAID&sap-client=650&dxp=21100006&
field_id=00046 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349208750
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.d5e5b1f11b44437a
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-d5e5b1f11b44437a-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, 16 Jun 2022 03:14:01 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: 159
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://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

{"modeltravelPaidTableData":
[11,"TRAVEL_TYPE","START_DATE","END_DATE","START_TIME","END_TIME","REASON","COUNTRY","DESTINATION","AMOUNT","CURRENCY","PAY_DATE"]}
```

10.43. https://testportal.zalaris.com/neptune/zmfp_dash_ess_trvl_process

Summary

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

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_trvl_process?ajax_id=GET_TRAVEL_PROC_DETAILS&ajax_applid=ZMFP_DASH_ESS_TRVL_PROCESS&sap-client=650&dxp=21100006&
field_id=00031 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349356829
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.2a37a397872f4c5d
```

```
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-2a37a397872f4c5d-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, 16 Jun 2022 03:16:46 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: 215
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://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

{"modeltabTrvlExpProcESSData":
[16,"USER_ID","TRAVEL_TYPE","REINR","BEGDA","BEGDA_TIME","ENDDA","ENDDA_TIME","REASON","DESTINATION","AMOUNT","CURRENCY","STATUS","APPROVER_B
OOL","APPROVER","APPROVED_BOO
...[SNIP]...
```

10.44. 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_PAYSLIP&sap-client=650&dxp=21100006&field_id=00198 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349075680
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
```

```
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.ca0304eb118e4395
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-ca0304eb118e4395-01
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, 16 Jun 2022 03:11:39 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: 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://*.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

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

10.45. 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=TIME_KPI&ajax_applid=ZMFP_HOME_SCREEN&sap-client=650&dxp=21100006&field_id=00186 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349147219
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.521542939e854955
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-521542939e854955-01
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, 16 Jun 2022 03:13:28 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; charset=utf-8
content-length: 195
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://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

{"modeloHBoxTimeRegData":{"ICON":"sap-icon://zal/Time-registratiom-
Outline","START_TEXT":"","VALUE":"50,5","END_TEXT":"","SEVERITY":"Error","APP_ID":"ZMFP_TIME_ENTRY_V2","URL":"","VISIBLE":true}}
```

10.46. https://testportal.zalaris.com/neptune/zmfp_launch_ext_app

Summary

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

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_launch_ext_app?ajax_id=GET_URL&ajax_applid=ZMFP_LAUNCH_EXT_APP&sap-client=650&dxp=21100006&field_id=00046&ajax_value=releaseNotes
HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655350119630; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.10921339f2e84cfa
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-10921339f2e84cfa-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, 16 Jun 2022 03:28:57 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; charset=utf-8
content-length: 67
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://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

{"modelextURLData":{"EXT_URL":"https://testwiki.zalaris.com/zsol"}}
```

10.47. 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&dxp=21100006&field_id=00253 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
```

```
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349208750
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.2a5e530e5a9645b4
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-2a5e530e5a9645b4-01
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, 16 Jun 2022 03:13:38 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: 46270
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://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

{"modeloPageStartData":
{"COUNT_ALL":13,"COUNT_APPROVED":11,"COUNT_REJECTED":0,"COUNT_SENT":2,"COUNT_POSTED":0,"COUNT_ACC":6,"COUNT_DELETED":0,"WRK_BEGDA":"202206
17"},"modelListStatusData":[14,"TYPE","
...[SNIP]...
```

10.48. 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=00849 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655350055042; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.ebe5c2f6cf9c4df8
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-ebe5c2f6cf9c4df8-01
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, 16 Jun 2022 03:27:37 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/json; charset=utf-8
Content-Length: 162559
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://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

{"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]...
```

10.49. 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349983849; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.a117a742d398460f
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-a117a742d398460f-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, 16 Jun 2022 03:27:07 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/json; charset=utf-8
content-length: 57
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://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

{"modeloPageUploadData":{"EMPPHOTOURL":"","IMAGESTR":""}}
```

10.50. https://testportal.zalaris.com/neptune/zmfp_quota_transfer

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://testportal.zalaris.com**
Path:	**/neptune/zmfp_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/zmfp_quota_transfer?ajax_id=SYNC&ajax_applid=ZMFP_QUOTA_TRANSFER&sap-client=650&dxp=21100006&field_id=00030 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349718611
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.8a27ef206327486e
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-8a27ef206327486e-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, 16 Jun 2022 03:21:59 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: application/json; charset=utf-8
Content-Length: 1375
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://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

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

10.51. https://testportal.zalaris.com/neptune/zmfp_sal_letter

Summary

Severity: **Information**

Confidence: **Certain**

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

Path: **/neptune/zmfp_sal_letter**

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_sal_letter?ajax_id=SYNC&ajax_applid=ZMFP_SAL_LETTER&sap-client=650&dxp=21100006&field_id=00019 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349841642
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.3b2be7adcca54379
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-3b2be7adcca54379-01
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, 16 Jun 2022 03:24:57 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; charset=utf-8
content-length: 633
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://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":[7,"ZYEAR","ZMONTH","MOLGA","BUKRS","LTYPE","LNAME","ZPAY_DATE","2022","06","20","","SALAR","SALARY
LETTER","20220606","2022","04","20","","BONUS","BONUS LETTER","20220412","202
...[SNIP]...
```

10.52. https://testportal.zalaris.com/neptune/zmfp_setup_wizard

Summary

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

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_setup_wizard?ajax_id=GET_DATA&ajax_applid=ZMFP_SETUP_WIZARD&sap-client=650&dxp=21100006&field_id=00012 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655350119630; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.83f15385e45045b1
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-83f15385e45045b1-01
Content-Length: 14
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_DATA":{}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:29:24 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: 26664
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://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

{"modeloPageData":{"ROLE":"","ROLEID":"1FA","ROLETYPE":"","WIZTYPE":"1","SYSID":"ZEQ","SHOW_OTP":"","STEP1_OPT2_TXT":"Via Zalaris HR Portal: download the app by
scanning the QR-code which you can find
...[SNIP]...
```

10.53. 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MbIRdOCLc/kjOPX0D/p|1655349014046|1655349208750
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.33e55f351ef14f24
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-33e55f351ef14f24-01
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":1655317800000,"CAL_ENDDA":1655922599000,"EXP_BEGDA":"20220616","EXP_ENDDA":"20220622","ALL":false}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:13:49 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; charset=utf-8
Content-Length: 2162
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://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
```

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

10.54. 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349075680
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.a43de384b0dd4cfd
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-a43de384b0dd4cfd-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, 16 Jun 2022 03:12:08 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: 78864
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://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

{"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]...
```

10.55. 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349718611
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.245efe6e474a4e02
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-245efe6e474a4e02-01
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, 16 Jun 2022 03:22:37 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/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://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":[8,"PABRJ","PABRP","BEGDA","ENDDA","AMOUNT1","AMOUNT2","PDF_SRC","FIL_KEY","2022","03","20220301","20220329"," 157.50","0.00","","03.2022","2022","02"
...[SNIP]...

10.56. 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349718611
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.e61af9b390bd4b64
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-e61af9b390bd4b64-01
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, 16 Jun 2022 03:22:57 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; 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://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

{"modelInputData":
{"PERNR":"00034448","REINR":"0000000000","WIID":"000000000000","FROM_INBOX":false,"FROM_INBOX_HIST":false,"SIMULATE":false,"ROLE":"ESS","PLANREQUEST":"","FOR_EDIT":false,"DATV1":"202
...[SNIP]...

10.57. https://testportal.zalaris.com/neptune/zmfp_travel_overview

Summary

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

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_overview?ajax_id=GET_CCC_IMPORTS&ajax_applid=ZMFP_TRAVEL_OVERVIEW&sap-client=650&dxp=21100006&field_id=00159 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349356829
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.77ed77fc9d824986
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-77ed77fc9d824986-01
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, 16 Jun 2022 03:16:00 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: application/json; charset=utf-8
Content-Length: 110259
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://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

{"modelCCCListData":
[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","FRONT","RE
...[SNIP]...

10.58. 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349075680
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.d4dab665c6e74f54
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-d4dab665c6e74f54-01
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, 16 Jun 2022 03:11:19 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: 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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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":
[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]...

10.59. 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349841642
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.ce66464f76214123
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-ce66464f76214123-01
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, 16 Jun 2022 03:24:23 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/json; charset=utf-8
Content-Length: 32015
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://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":
[72,"PERNR","DATE_CHAN","TIME_CHAN","REC_ID","REC_TYPE","REF_ID","INFTY","SUBTY","UUID","LOCKED","BEGDA","BEGDA_SHOW","BEGDA_VS","BEGDA_EN","WAGE_TYPE","WT_TEXT","WAGE_TYPE_VS",
...[SNIP]...

10.60. https://testportal.zalaris.com/neptune/zsp_suppinfo_frontend

Summary

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

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/zsp_suppinfo_frontend?ajax_id=POR_GET_ITEM&ajax_applid=ZSP_SUPPINFO_FRONTEND&sap-client=650&dxp=21100006&field_id=00049 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655350119630; 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
X-Requested-With: XMLHttpRequest
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, 16 Jun 2022 03:28:45 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; charset=utf-8
content-length: 213
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://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

{"modeloVerticalLayoutData":
{"ITEMID":"00000000","UCN":"","CLIENT":"","CDATE":"","CTIME":"000000","UNAME":"","TLOCK":false,"TLOCKBY":"","ROLES":"","BUKRS":"","EMAIL":"","PHONE":"","LOCKED_TEXT":"","IN
...[SNIP]...

---

11. Cross-origin resource sharing: arbitrary origin trusted

There are 60 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/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_lvreq_overview
- /neptune/zmfp_dash_ess_next_salary
- /neptune/zmfp_dash_ess_other_quotas
- /neptune/zmfp_dash_ess_paid_vacation
- /neptune/zmfp_dash_ess_sickness
- /neptune/zmfp_dash_ess_time_reg
- /neptune/zmfp_dash_ess_travel_paid
- /neptune/zmfp_dash_ess_trvl_process
- /neptune/zmfp_ess_payslip
- /neptune/zmfp_home_screen
- /neptune/zmfp_launch_ext_app

- /neptune/zmfp_leave_request
- /neptune/zmfp_personal_profile
- /neptune/zmfp_photo_upload
- /neptune/zmfp_quota_transfer
- /neptune/zmfp_sal_letter
- /neptune/zmfp_setup_wizard
- /neptune/zmfp_team_status
- /neptune/zmfp_time_entry_v2
- /neptune/zmfp_time_statement
- /neptune/zmfp_travel_create_expense_rep
- /neptune/zmfp_travel_overview
- /neptune/zmfp_universal_inbox
- /neptune/zmfp_wt_compensation
- /neptune/zsp_suppinfo_frontend

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

11.1. 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://ctzmzbpganpb.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
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://ctzmzbpganpb.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363557512
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:17:48 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: 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 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.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

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

11.2. 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://qipyacmkjuma.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=1100
HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MbIRdOCLc/kjOPX0D/p|1655349014046|1655364518414; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.03366d2d5fad4107
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-03366d2d5fad4107-01
Origin: https://qipyacmkjuma.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, 16 Jun 2022 07:30:03 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: 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://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

{"modelpageDetailViewerData":
{"PERNR":"00000000","ENAME":"","DOCART":"","DEL_DATE":"","KEYW1":"","KEYW2":"","KEYW3":"","KEYW4":"","KEYW5":"","KEYW6":"","KEYW7":"","KEYW8":"","DOCART_TEX
T":"","FILENAME
...[SNIP]...
```

11.3. 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://bgavzflvfpln.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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://bgavzflvfpln.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:21:46 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: 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://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

{}
```

11.4. 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 that allows access from any domain.

The application allowed access from the requested origin **https://jypkvcdiaubs.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/apk.jpg HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://jypkvcdiaubs.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:24:14 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: 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://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

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

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

11.5. 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://uiallhhtkxon.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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://uiallhhtkxon.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842

Response 1

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:24:33 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: 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:// data: blob: https://maps.googleapis.com:443 https://*.hana.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

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

11.6. 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://zhcenjapykft.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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://zhcenjapykft.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842

Response 1

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:25:38 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: image/jpeg
content-length: 4096
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://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

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

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

11.7. 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://dooliyiaefsa.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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655364518414
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://dooliyiaefsa.com

Response 1

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:31:05 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-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://*.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

!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]...

11.8. 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://bybrkftwgtqt.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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655364518414
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://bybrkftwgtqt.com

Response 1

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:30:54 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-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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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

/*
* 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]...
```

11.9. 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://himjwjknqgeb.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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655364518414; 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://himjwjknqgeb.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:32:21 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: 307551
dxp-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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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

!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,I,i,o,a,h,C,T
...[SNIP]...

11.10. 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://apppwgmsktlo.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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655364518414
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://apppwgmsktlo.com

Response 1

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:31:56 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
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: 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://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

/*!
* 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]...
```

11.11. 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://eerdhjugjgcy.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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://eerdhjugjgcy.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655364518414
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:36:10 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: image/svg+xml
Content-Length: 3651
dxp-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://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

<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]...
```

11.12. 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://blnvccbinqku.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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://blnvccbinqku.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655364518414
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:31:47 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
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://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
```

11.13. 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://srbacpzmdday.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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://srbacpzmdday.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655364518414
```

Response 1

```
HTTP/1.1 200 OK
Date: 20220616 093441 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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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
```

11.14. 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://ccnojzykrkbq.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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
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://ccnojzykrkbq.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:44:02 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: application/json
content-length: 977
dxp-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://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

{
  "css-selector": "sapFAvatarColorAccent@{accentIndex}",
  "color-param": "sapUiAccent@{accentIndex}",
  "_sap_f_DynamicPageHeader_PaddingBottom": "1rem",
  "_sap_f_Card_ContentPadding": "1rem",
  "_sap_
...[SNIP]...
```

11.15. 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://akfqficgkdid.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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
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://akfqficgkdid.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:44:11 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: 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://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

{
  "_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]...
```

11.16. 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://hfmrgpoqxiui.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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
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://hfmrgpoqxiui.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:45:36 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
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://*.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

{
  "_sap_suite_ui_commons_StatusIndicator_SmallLabelMargin": "0.375rem",
  "_sap_suite_ui_commons_StatusIndicator_MediumLabelMargin": "0.5rem",
  "_sap_suite_ui_commons_StatusIndicator_LargeLabelMargin"
```

...[SNIP]...

11.17. 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 that allows access from any domain.

The application allowed access from the requested origin **https://blsyvgdvuoiy.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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
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://blsyvgdvuoiy.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:45:31 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
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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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

{
```

"_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]...

11.18. 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://ztvmtnvplqgm.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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
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://ztvmtnvplqgm.com

Response 1

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:44:23 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/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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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

{
  "_sap_tnt_NavigationList_ItemHeight": "2.75rem",
  "_sap_tnt_NavigationList_NoIconsGroupPadding": "1rem",
  "_sap_tnt_NavigationList_NoIconsNestedItemPadding": "2rem",
  "_sap_tnt_ToolHeader_ITHOverfl
...[SNIP]...
```

11.19. 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://fgbswouachwv.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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
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://fgbswouachwv.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:45:02 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: 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://*.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

{
  "sapBrandColor": "#3079BF",
  "sapHighlightColor": "#265f96",
  "sapBaseColor": "#fff",
  "sapShellColor": "#fff",
  "sapBackgroundColor": "#f9f9fd",
  "sapFontFamily": "\"72full\", Arial, Helvetica, sa
...[SNIP]...
```

11.20. 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 that allows access from any domain.

The application allowed access from the requested origin **https://fzdmnszydqde.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/layout/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
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://fzdmnszydqde.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:45:10 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: 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://*.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

{
  "_sap_ui_layout_ColumnLayout_formColumnMaxXL": "4",
  "_sap_ui_layout_ColumnLayout_formColumnMaxL": "3",
  "_sap_ui_layout_ColumnLayout_formColumnMaxM": "2",
  "_sap_ui_layout_ColumnLayout_formColumnM
...[SNIP]...
```

11.21. 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://voovdpjnwpqe.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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
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://voovdpjnwpqe.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:47:20 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
Content-Length: 6448
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
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://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

{
  "_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]...
```

11.22. 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://hcajqrcdzrrg.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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
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://hcajqrcdzrrg.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:47:32 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: 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
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://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

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

11.23. 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://aamrdcxfgfwy.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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
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://aamrdcxfgfwy.com

Response 1

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:47:10 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
dxp-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://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

{
  "sapUiFiori3AnchorBarBottomShadow": "inset 0 -0.0625rem #d9d9d9",
  "sapUiFiori3ABUnderlineOffsetAndHeight": "0.188rem",
  "sapUiFiori3ABUnderlineTopRadius": "0.125rem",
  "sapUiFiori3HSBottomShadow":
...[SNIP]...
```

11.24. 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 that allows access from any domain.

The application allowed access from the requested origin **https://djonqcewcbat.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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://djonqcewcbat.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:46:21 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: 71860
dxp-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://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

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]...

11.25. 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://ktkywdxiimfw.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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://ktkywdxiimfw.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
```

Response 1

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:46:28 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: 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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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 AppCache=
{Initialized:!1,Encrypted:"",CurrentUname:"",CurrentApp:"",CurrentConfig:"",CurrentLanguage:"",AppVersion:"",StartApp:"",navNotif:!1,Url:"",UrlBase:"",Client:"",Passcode:"",Auth:"",enable
...[SNIP]...

11.26. 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://jhtwkwsbwphm.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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://jhtwkwsbwphm.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146

Response 1

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:46:55 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/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://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

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]...
```

11.27. 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://qqqilhrlbhce.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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://qqqilhrlbhce.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:46:58 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/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://*.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 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]...
```

11.28. 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://zapvhmivxcoc.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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://zapvhmivxcoc.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:48:08 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: 15627
dxp-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://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

/*
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]...
```

11.29. 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://myuykvojlzgj.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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://myuykvojlzgj.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365359146
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:48:19 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: 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://*.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

/*! 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]...
```

11.30. 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://szzipfigowjz.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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://szzipfigowjz.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MbIRdOCLc/kjOPX0D/p|1655349014046|1655365359146
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:48:30 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: 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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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

/*! 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]...
```

11.31. 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://ssbpcxgiwfbj.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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://ssbpcxgiwfbj.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365719420
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:50:30 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: 2328807
dxp-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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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

!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]...
```

11.32. 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://kcvrjvqumnrd.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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Origin: https://kcvrjvqumnrd.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365719420
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:50:46 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: 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 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.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]...
```

11.33. 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://jvpztmmhuyks.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&dxp=21100006&
field_id=00053&ajax_value=ZMFP_SETUP_WIZARD HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655365719420; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.2530fa39f249449a
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-2530fa39f249449a-01
Origin: https://jvpztmmhuyks.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, 16 Jun 2022 07:57:19 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
content-type: application/json; charset=utf-8
content-length: 172
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://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

{"modelAppCacheAppTimestampData":{"APPLID":"ZMFP_SETUP_WIZARD","LANGUAGE":"","UPDDAT":"20220616","UPDTIM":"002944","INVALID":false,"DESCR":"MFP:
Application Setup Wizard"}}
```

11.34. 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://uaytqujxyrju.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&dxp=21100006&field_id=00113 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655367520974; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.4c0e1ca49a174eef
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-4c0e1ca49a174eef-01
Origin: https://uaytqujxyrju.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, 16 Jun 2022 08:20:40 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: 88
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://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"]}
```

11.35. 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://qmwvvbackfaw.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&dxp=21100006&field_id=00111 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655367520974; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.9c175d389d4f4e3d
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-9c175d389d4f4e3d-01
Content-Length: 47
Origin: https://qmwvvbackfaw.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, 16 Jun 2022 08:22:55 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: 1235
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://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":
[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]...
```

11.36. https://testportal.zalaris.com/neptune/zmfp_dash_ess_lvreq_overview

Summary

Severity: **Information**

Confidence: **Certain**

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

Path: **/neptune/zmfp_dash_ess_lvreq_overview**

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://bivmwpcudyxo.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_lvreq_overview?ajax_id=GET_ESS_LEAVE_REQUESTS&ajax_applid=ZMFP_DASH_ESS_LVREQ_OVERVIEW&sap-client=650&dxp=21100006&
field_id=00061 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655367520974; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.6284344f2b304768
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-6284344f2b304768-01
Origin: https://bivmwpcudyxo.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, 16 Jun 2022 08:23:03 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: 862
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://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

{"modelleaveReqDialogTableData":
[9,"USER_ID","LEAVE_TYPE_ICON","START_DATE","END_DATE","START_TIME","END_TIME","STATUS_ICON","STATUS_COLOR","DESCRIPTION","00034448","sap-
icon://general-leave-request",
...[SNIP]...
```

11.37. 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://csbgxgvpubjj.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&dxp=21100006&field_id=00089 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655367520974; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.aeabb0a80e07450e
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-aeabb0a80e07450e-01
Origin: https://csbgxgvpubjj.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, 16 Jun 2022 08:22:27 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/json; charset=utf-8
Content-Length: 1570
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://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

{"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]...
```

11.38. https://testportal.zalaris.com/neptune/zmfp_dash_ess_other_quotas

Summary

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

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://lqqwogsixiqp.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_other_quotas?ajax_id=GET_ESS_OTHER_QUOTAS&ajax_applid=ZMFP_DASH_ESS_OTHER_QUOTAS&sap-client=650&dxp=21100006&
field_id=00041 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655367520974; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.fd5ceef397014551
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-fd5ceef397014551-01
Origin: https://lqqwogsixiqp.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, 16 Jun 2022 08:23:45 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; charset=utf-8
content-length: 409
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://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

{"modeltabOtherQuotasData":[6,"USER_ID","TIME_TEXT","DEDUCT_BEGIN","DEDUCT_END","ENTITLE","AVAILABLE","650-00034448","Time off overtimer","20220101","20221231","15.00 Hours","0.00 Hours","650-00034448
...[SNIP]...

11.39. https://testportal.zalaris.com/neptune/zmfp_dash_ess_paid_vacation

Summary

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

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://ayvoozhnzidv.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_paid_vacation?ajax_id=GET_ESS_PAID_VACATION&ajax_applid=ZMFP_DASH_ESS_PAID_VACATION&sap-client=650&dxp=21100006&field_id=00047 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655368061457; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.b246abcccaa14049
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-b246abcccaa14049-01
Origin: https://ayvoozhnzidv.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, 16 Jun 2022 08:28:36 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: application/json; charset=utf-8
content-length: 260
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://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

{"modelpaidVacDialogTableData":
[7,"PERNR","QUOTA_TEXT","DATE_FROM","DATE_TO","ENTITLED","AVAILABLE","UOM","00034448","Vacation","20220101","20221231",25.00000,25.00000,"Days","00034448","
Vacation from
...[SNIP]...

11.40. https://testportal.zalaris.com/neptune/zmfp_dash_ess_sickness

Summary

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

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://cxijnufkmbcw.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_sickness?ajax_id=GET_SICKNESS&ajax_applid=ZMFP_DASH_ESS_SICKNESS&sap-client=650&dxp=21100006&field_id=00021 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655368121518; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.a7776eb903b94895
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-a7776eb903b94895-01
Origin: https://cxijnufkmbcw.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, 16 Jun 2022 08:30:20 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: 846
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://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

{"modelDataSicknessESSData":[8,"NAME","PERNR","PERIOD","MONTH","PERCENTAGE","RE_CALC_DAYS","WDAYS","YEAR_MON","Jostein Hansen","00034448",7,"JUL",0,"0","22.00 ","202107","Jostein Hansen","00034448",8
...[SNIP]...

11.41. https://testportal.zalaris.com/neptune/zmfp_dash_ess_time_reg

Summary

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

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://ugrpzdiewfgj.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_time_reg?ajax_id=GET_TIME_REGISTRATION&ajax_applid=ZMFP_DASH_ESS_TIME_REG&sap-client=650&dxp=21100006&field_id=00061 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655368121518; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.3f56ce107bba4660
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-3f56ce107bba4660-01
Origin: https://ugrpzdiewfgj.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, 16 Jun 2022 08:31:11 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: 615
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://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

{"modelcalTimeRegESSData":[2,"Date","Type","2022/06/04","NonWorking","2022/06/05","Type01","2022/06/05","NonWorking","2022/06/06","Type01","2022
/06/06","NonWorking","2022/06/07","Type08","2022/06/11",
...[SNIP]...
```

11.42. https://testportal.zalaris.com/neptune/zmfp_dash_ess_travel_paid

Summary

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

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://cmjgwocsmnnn.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_travel_paid?ajax_id=GET_TRAVEL_PAID_DETAILS&ajax_applid=ZMFP_DASH_ESS_TRAVEL_PAID&sap-client=650&dxp=21100006&
field_id=00046 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655368121518; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.d5e5b1f11b44437a
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-d5e5b1f11b44437a-01
Origin: https://cmjgwocsmnnn.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, 16 Jun 2022 08:30:26 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: 159
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://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

{"modeltravelPaidTableData":
[11,"TRAVEL_TYPE","START_DATE","END_DATE","START_TIME","END_TIME","REASON","COUNTRY","DESTINATION","AMOUNT","CURRENCY","PAY_DATE"]}
```

11.43. https://testportal.zalaris.com/neptune/zmfp_dash_ess_trvl_process

Summary

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

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://dyuaaewitark.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_trvl_process?ajax_id=GET_TRAVEL_PROC_DETAILS&ajax_applid=ZMFP_DASH_ESS_TRVL_PROCESS&sap-client=650&dxp=21100006&
field_id=00031 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655368121518; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.2a37a397872f4c5d
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-2a37a397872f4c5d-01
Origin: https://dyuaaewitark.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, 16 Jun 2022 08:30:18 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: 215
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://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

{"modeltabTrvlExpProcESSData":
[16,"USER_ID","TRAVEL_TYPE","REINR","BEGDA","BEGDA_TIME","ENDDA","ENDDA_TIME","REASON","DESTINATION","AMOUNT","CURRENCY","STATUS","APPROVER_B
OOL","APPROVER","APPROVED_BOO
...[SNIP]...
```

11.44. 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.

The application allowed access from the requested origin **https://jggdacaafkad.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_ess_payslip?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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655368121518; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.ca0304eb118e4395
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-ca0304eb118e4395-01
Origin: https://jggdacaafkad.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, 16 Jun 2022 08:31:49 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; 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://*.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

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

11.45. 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 that allows access from any domain.

The application allowed access from the requested origin **https://ptjspndffizf.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=TIME_KPI&ajax_applid=ZMFP_HOME_SCREEN&sap-client=650&dxp=21100006&field_id=00186 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655368121518; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
```

```
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.521542939e854955
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-521542939e854955-01
Origin: https://ptjspndffizf.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, 16 Jun 2022 08:33:55 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: 195
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://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

{"modeloHBoxTimeRegData":{"ICON":"sap-icon://zal/Time-registratiom-
Outline","START_TEXT":"","VALUE":"50,5","END_TEXT":"","SEVERITY":"Error","APP_ID":"ZMFP_TIME_ENTRY_V2","URL":"","VISIBLE":true}}
```

11.46. https://testportal.zalaris.com/neptune/zmfp_launch_ext_app

Summary

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

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://bkhblestwyad.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_launch_ext_app?ajax_id=GET_URL&ajax_applid=ZMFP_LAUNCH_EXT_APP&sap-client=650&dxp=21100006&field_id=00046&ajax_value=releaseNotes
HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655368722017; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.10921339f2e84cfa
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-10921339f2e84cfa-01
Origin: https://bkhblestwyad.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, 16 Jun 2022 08:39:18 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: 67
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://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

{"modelextURLData":{"EXT_URL":"https://testwiki.zalaris.com/zhsr"}}
```

11.47. 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://rwwaxecwwvqm.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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
```

```
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655369322516; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.2a5e530e5a9645b4
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-2a5e530e5a9645b4-01
Content-Length: 47
Origin: https://rwwaxecwwvqm.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, 16 Jun 2022 08:55:32 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; charset=utf-8
Content-Length: 46270
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://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

{"modeloPageStartData":
{"COUNT_ALL":13,"COUNT_APPROVED":11,"COUNT_REJECTED":0,"COUNT_SENT":2,"COUNT_POSTED":0,"COUNT_ACC":6,"COUNT_DELETED":0,"WRK_BEGDA":"202206
17"},"modelListStatusData":[14,"TYPE","
...[SNIP]...
```

11.48. 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://qpuknsnonwvt.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=00849 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655368962270; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.ebe5c2f6cf9c4df8
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-ebe5c2f6cf9c4df8-01
Content-Length: 15
Origin: https://qpuknsnonwvt.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, 16 Jun 2022 08:47:38 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: 162559
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://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

{"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]...
```

11.49. 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://aocqdunaaqpl.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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655368962270; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.a117a742d398460f
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-a117a742d398460f-01
Origin: https://aocqdunaaqpl.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, 16 Jun 2022 08:44:51 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; 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://*.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

{"modeloPageUploadData":{"EMPPHOTOURL":"
/2wBDAAMCAgICAgMCAgIDAwMDBAYEBAQEBAgGBgUGCQgKCgkICQkKDA8MCgsOCwkJDRENDg8QEBEQCgwSExIQEw8QEBD/2wBDAQMDAwQDBAgEB
...[SNIP]...
```

11.50. https://testportal.zalaris.com/neptune/zmfp_quota_transfer

Summary

Severity:	**Information**
Confidence:	**Certain**

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

Path: **/neptune/zmfp_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://uikmjifdpdbm.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_quota_transfer?ajax_id=SYNC&ajax_applid=ZMFP_QUOTA_TRANSFER&sap-client=650&dxp=21100006&field_id=00030 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655368722017; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.8a27ef206327486e
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-8a27ef206327486e-01
Content-Length: 32
Origin: https://uikmjifdpdbm.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, 16 Jun 2022 08:42:48 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: 1375
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://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

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

11.51. https://testportal.zalaris.com/neptune/zmfp_sal_letter

Summary

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

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://ssarljhhvjae.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_sal_letter?ajax_id=SYNC&ajax_applid=ZMFP_SAL_LETTER&sap-client=650&dxp=21100006&field_id=00019 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655368722017; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.3b2be7adcca54379
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-3b2be7adcca54379-01
Origin: https://ssarljhhvjae.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, 16 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/json; charset=utf-8
content-length: 633
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://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":[7,"ZYEAR","ZMONTH","MOLGA","BUKRS","LTYPE","LNAME","ZPAY_DATE","2022","06","20","","SALAR","SALARY
LETTER","20220606","2022","04","20","","BONUS","BONUS LETTER","20220412","202
```

```
...[SNIP]...
```

11.52. https://testportal.zalaris.com/neptune/zmfp_setup_wizard

Summary

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

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://picpiztuusdf.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_setup_wizard?ajax_id=GET_DATA&ajax_applid=ZMFP_SETUP_WIZARD&sap-client=650&dxp=21100006&field_id=00012 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655369322516; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.83f15385e45045b1
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-83f15385e45045b1-01
Content-Length: 14
Origin: https://picpiztuusdf.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_DATA":{}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 08:49:57 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; charset=utf-8
Content-Length: 26664
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://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

{"modeloPageData":{"ROLE":"","ROLEID":"1FA","ROLETYPE":"","WIZTYPE":"1","SYSID":"ZEQ","SHOW_OTP":"","STEP1_OPT2_TXT":"Via Zalaris HR Portal: download the app by scanning the QR-code which you can find
...[SNIP]...
```

11.53. 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://fhqcmscplznd.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&dxp=21100006&field_id=00020 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655369923091; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.33e55f351ef14f24
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-33e55f351ef14f24-01
Content-Length: 142
Origin: https://fhqcmscplznd.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":1655317800000,"CAL_ENDDA":1655922599000,"EXP_BEGDA":"20220616","EXP_ENDDA":"20220622","ALL":false}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 09:00:59 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/json; charset=utf-8
Content-Length: 2162
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://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

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

11.54. 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://fnhfapknxlfo.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&dxp=21100006&field_id=01034 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655369863038; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.a43de384b0dd4cfd
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-a43de384b0dd4cfd-01
Content-Length: 15
Origin: https://fnhfapknxlfo.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, 16 Jun 2022 08:58:37 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/json; charset=utf-8
Content-Length: 78864
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://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

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

11.55. 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://vrsftirxewya.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&dxp=21100006&field_id=00111 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655369322516; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.245efe6e474a4e02
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-245efe6e474a4e02-01
Content-Length: 42
Origin: https://vrsftirxewya.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, 16 Jun 2022 08:56:51 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; 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://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":[8,"PABRJ","PABRP","BEGDA","ENDDA","AMOUNT1","AMOUNT2","PDF_SRC","FIL_KEY","2022","03","20220301","20220329"," 157.50","
0.00","","03.2022","2022","02"
...[SNIP]...
```

11.56. 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://gknrmcnlxwhe.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&dxp=21100006&field_id=00072 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655369923091; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.e61af9b390bd4b64
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-e61af9b390bd4b64-01
Content-Length: 15
Origin: https://gknrmcnlxwhe.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, 16 Jun 2022 09:00:37 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/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://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

{"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]...
```

11.57. https://testportal.zalaris.com/neptune/zmfp_travel_overview

Summary

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

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://xamnkjlckptb.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_overview?ajax_id=GET_CCC_IMPORTS&ajax_applid=ZMFP_TRAVEL_OVERVIEW&sap-client=650&dxp=21100006&field_id=00159 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655369923091; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.77ed77fc9d824986
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-77ed77fc9d824986-01
Content-Length: 15
Origin: https://xamnkjlckptb.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, 16 Jun 2022 09:02:02 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: application/json; charset=utf-8
Content-Length: 110259
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://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

{"modelCCCListData":
[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","FRONT","RE
...[SNIP]...
```

11.58. 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://pfocwpmbwajg.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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655369923091; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.d4dab665c6e74f54
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-d4dab665c6e74f54-01
Origin: https://pfocwpmbwajg.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, 16 Jun 2022 09:06:34 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; 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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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":
[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]...
```

11.59. 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 that allows access from any domain.

The application allowed access from the requested origin **https://xyaeodtznmag.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_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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655369923091; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
```

```
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.ce66464f76214123
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-ce66464f76214123-01
Content-Length: 31
Origin: https://xyaeodtznmag.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, 16 Jun 2022 09:08:21 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/json; charset=utf-8
Content-Length: 32015
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://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":
[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]...
```

11.60. https://testportal.zalaris.com/neptune/zsp_suppinfo_frontend

Summary

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

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://ktwtpdxwxefh.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/zsp_suppinfo_frontend?ajax_id=POR_GET_ITEM&ajax_applid=ZSP_SUPPINFO_FRONTEND&sap-client=650&dxp=21100006&field_id=00049 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
```

```
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655364518414; 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
X-Requested-With: XMLHttpRequest
Origin: https://ktwtpdxwxefh.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, 16 Jun 2022 07:28:45 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; charset=utf-8
content-length: 213
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://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

{"modeloVerticalLayoutData":
{"ITEMID":"00000000","UCN":"","CLIENT":"","CDATE":"","CTIME":"000000","UNAME":"","TLOCK":false,"TLOCKBY":"","ROLES":"","BUKRS":"","EMAIL":"","PHONE":"","LOCKED_TE
XT":"","IN
...[SNIP]...
```

---

12. Referer-dependent response

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 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
/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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349983849; 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

XPROFILE=ESS&XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW&
ClientWindowID=WID1655349984817&%24Roundtrip=true&%24DebugAction=null
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:02:48 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
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
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: 8530

<!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?XPROFILE=ESS&
```

```
XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349983849; 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

XPROFILE=ESS&XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW&
ClientWindowID=WID1655349984817&%24Roundtrip=true&%24DebugAction=null
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:02:48 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
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
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: 8553

<!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 3 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

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:32 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
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://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: PortalAlias=portal; Path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 13739

<!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]...
<!--
EPCM.relaxDocumentDomain();
EPCM.init( {
Level:1,
DynamicTop:false, // [service=true nestedWinOnAlias=false]
UAType:9, // [Chrome]
UAVersion:97.0,
UAPlatform:1, // [Win]
UIPMode:"2", // [Default=2, User=0, Personalize=false]
UIPModeOptions:"",
UIPWinFeatures:"",
UIPPortalPath:"https://testportal.zalaris.com:443/irj/portal",
UIPPopupComp:"https://testportal.zalaris.co
...[SNIP]...
```

Request 2

```
GET /irj/portal HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
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
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655350991634
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:57:01 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
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://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: PortalAlias=portal; Path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 13739

<!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]...
<!--
EPCM.relaxDocumentDomain();
EPCM.init( {
Level:1,
DynamicTop:false, // [service=true nestedWinOnAlias=false]
UAType:31, // [Safari]
UAVersion:5.1,
UAPlatform:3, // [Mac]
UIPMode:"2", // [Default=2, User=0, Personalize=false]
UIPModeOptions:"",
UIPWinFeatures:"",
UIPPortalPath:"https://testportal.zalaris.com:443/irj/portal",
UIPPopupComp:"https://testportal.zalaris.co
...[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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:32 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
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://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: 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_tradeshow_plus/common
...[SNIP]...
<!--
EPCM.relaxDocumentDomain();
EPCM.init( {
Level:1,
DynamicTop:false, // [service=true nestedWinOnAlias=false]
UAType:9, // [Chrome]
UAVersion:97.0,
UAPlatform:1, // [Win]
UIPMode:"2", // [Default=2, User=0, Personalize=false]
UIPModeOptions:"",
UIPWinFeatures:"",
UIPPortalPath:"https://testportal.zalaris.com:443/irj/portal",
UIPPopupComp:"https://testportal.zalaris.co
...[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
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
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655351891862
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 04:01:50 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://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: 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_tradeshow_plus/common
...[SNIP]...
<!--
EPCM.relaxDocumentDomain();
EPCM.init( {
Level:1,
DynamicTop:false, // [service=true nestedWinOnAlias=false]
UAType:31, // [Safari]
UAVersion:5.1,
UAPlatform:3, // [Mac]
UIPMode:"2", // [Default=2, User=0, Personalize=false]
UIPModeOptions:"",
UIPWinFeatures:"",
UIPPortalPath:"https://testportal.zalaris.com:443/irj/portal",
UIPPopupComp:"https://testportal.zalaris.co
...[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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:39 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
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: 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]...
<!--
EPCM.relaxDocumentDomain();
EPCM.init( {
Level:1,
DynamicTop:false, // [service=true nestedWinOnAlias=false]
UAType:9, // [Chrome]
UAVersion:97.0,
UAPlatform:1, // [Win]
UIPMode:"2", // [Default=2, User=0, Personalize=false]
UIPModeOptions:"",
UIPWinFeatures:"",
UIPPortalPath:"https://testportal.zalaris.com:443/irj/portal",
UIPPopupComp:"https://testportal.zalaris.co
...[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
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
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655361515763
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 06:40:43 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
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: 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]...
<!--
EPCM.relaxDocumentDomain();
EPCM.init( {
Level:1,
DynamicTop:false, // [service=true nestedWinOnAlias=false]
UAType:31, // [Safari]
UAVersion:5.1,
UAPlatform:3, // [Mac]
UIPMode:"2", // [Default=2, User=0, Personalize=false]
UIPModeOptions:"",
UIPWinFeatures:"",
UIPPortalPath:"https://testportal.zalaris.com:443/irj/portal",
UIPPopupComp:"https://testportal.zalaris.co
...[SNIP]...
```

---

14. Cross-domain POST

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

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

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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349014046
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, 16 Jun 2022 03:10:22 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
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://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: 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="PFJlc3BvbnNlIHhtbG5zPSJ1cm46b2FzaXM6bmFtZXM6dGM6U0FNTDoyLjA6cHJvdG9jb2wiIHhtbG5zOm5zMj0idXJuOm9hc2lzOm5hbWVzOnRjOlNBTUw6Mi4wOmFzc2VydGlvbiIgeG1sbnM6bnMzP
...[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/zalaris_launchpad_standard [TILE_INFO JSON parameter]
- /neptune/zalaris_launchpad_standard [TILE_TITLE JSON parameter]
- /neptune/zalaris_launchpad_standard [field_id parameter]
- /neptune/zmfp_leave_request [field_id parameter]
- /neptune/zmfp_photo_upload [IMAGESTR JSON parameter]
- /neptune/zmfp_team_status [CAL_BEGDA JSON parameter]
- /neptune/zmfp_team_status [CAL_ENDDA JSON parameter]
- /neptune/zmfp_travel_overview [field_id 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]

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?lb8nv3g9sm=1 HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:53:31 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: 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://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: PortalAlias=portal; Path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 13773

<!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":"1655289020460","sap-ep-ul":"en","searchProvidersTS":"0"}';var cacheTimeStampsRep = jsonCacheTimeStampsRep.parseJSON();var
globalQueryString = '[{"value":"1","key":"lb8nv3g9sm"}]';var globalPostBody = null;var initConfiguration = function(){LSAPI.AFPPlugin.configuration.init('{"NavPrefix":{"mode6":"/irj
/servlet/prt/portal/prteventname/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_ANALYSISparsnio11b&XSYSTEM=SAP_BW&XPROFILE=ESS&
XQUERY=ZSTKPTMC1_REG_TIME_ESS HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349919451; 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, 16 Jun 2022 03:55:55 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
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://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: 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_tradeshow_plus/common
...[SNIP]...
signstudioPreview","page0ivu0");
pageSupport._addIViewBank("page0ivu0",new iviewBank("","",pageSupport.URL,1,"0","XPROFILE\x3dESS\x26XQUERY\x3dZSTKPTMC1_REG_TIME_ESS\x26APPLICATION
\x3dZGENERIC_ANALYSISparsnio11b\x26XSYSTEM\x3dSAP_BW","GET","false"));
</script>
...[SNIP]...
om.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_T
```

```
IME_ESS&amp;APPLICATION&#x3d;ZGENERIC_ANALYSISparsnio11b&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**

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=ESSs8fdentkct&
XQUERY=ZSTKPTMC1_REG_TIME_ESS HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349919451; 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, 16 Jun 2022 04:02:34 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
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://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: 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_tradeshow_plus/common
...[SNIP]...
com.sap.ip.bi\x2fPages\x2fcom.sap.ip.bi.designstudio\x2fcom.sap.ip.bi.designstudioPreview","page0ivu0");
pageSupport._addIViewBank("page0ivu0",new iviewBank("","",pageSupport.URL,1,"0","XPROFILE\x3dESSs8fdentkct\x26XQUERY\x3dZSTKPTMC1_REG_TIME_ESS
```

```
\x26APPLICATION\x3dZGENERIC_ANALYSIS\x26XSYSTEM\x3dSAP_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.designstudioPreview&#x3f;XPROFILE&#x3d;ESSs8fdentkct&amp;XQUERY&#x3d;ZSTKPTMC1_REG_TIME_ESS&amp;APPLICATION&#x3d;ZGENERIC_ANALYSIS&amp;XSYSTEM&#x3d;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=ZSTKPYMC2_ABS_OVERVIEW_ESScfjs1oqc2v HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349919451
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, 16 Jun 2022 04:06:00 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
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://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: 5856

<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_tradeshow_plus/common
...[SNIP]...
designstudio\x2fcom.sap.ip.bi.designstudioPreview","page0ivu0");
pageSupport._addIViewBank("page0ivu0",new iviewBank("","",pageSupport.URL,1,"0","XPROFILE\x3dESS\x26XQUERY\x3dZSTKPYMC2_ABS_OVERVIEW_ESScfjs1oqc2v
\x26APPLICATION\x3dZGENERIC_ANALYSIS\x26XSYSTEM\x3dSAP_BW","GET","false"));
</script>
...[SNIP]...
ct&#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;ZSTKPYMC2_ABS_OVERVIEW_ESScfjs1oqc2v&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**

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_BW3ujqvz5av8&XPROFILE=ESS&
XQUERY=ZSTKPTMC1_REG_TIME_ESS HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349919451; 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, 16 Jun 2022 03:59:16 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; 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://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: 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_tradeshow_plus/common
...[SNIP]...
age0ivu0");
pageSupport._addIViewBank("page0ivu0",new iviewBank("","",pageSupport.URL,1,"0","XPROFILE\x3dESS\x26XQUERY\x3dZSTKPTMC1_REG_TIME_ESS\x26APPLICATION
\x3dZGENERIC_ANALYSIS\x26XSYSTEM\x3dSAP_BW3ujqvz5av8","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_BW3ujqvz5av8" 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?rs5v50ky3a=1 HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:55:25 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
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://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: 5598

<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_tradeshow_plus/common
...[SNIP]...
```

```
orm_add_ons\x2fcom.sap.ip.bi\x2fPages\x2fcom.sap.ip.bi.designstudio\x2fcom.sap.ip.bi.designstudioPreview","page0ivu0");
pageSupport._addIViewBank("page0ivu0",new iviewBank("","",pageSupport.URL,1,"0","rs5v50ky3a\x3d1","GET","false"));
</script>
...[SNIP]...
#x2f;prtroot&#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;rs5v50ky3a&#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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349919451; 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=9OWEbXwMXQNeg6gBLVUbPw--7hjmzZmqUbZjAdzxMnFpBw--&Language=EN&XSYSTEM=SAP_BW&XQUERY=ZSTKPYMC2_ABS_OVERVIEW_ESS&
APPLICATION=ZGENERIC_ANALYSIS3hwc34wa4g&XPROFILE=ESS
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:06:21 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
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://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 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]...
designstudioPreview\x26XQUERY\x3dZSTKPYMC2_ABS_OVERVIEW_ESS\x26sap\x2dext\x2dsid\x3d9OWEbXwMXQNeg6gBLVUbPw\x2d\x2d7hjmzZmqUbZjAdzxMnFpBw
\x2d\x2d\x26XSYSTEM\x3dSAP_BW\x26APPLICATION\x3dZGENERIC_ANALYSIS3hwc34wa4g\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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655350055042; 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-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=H0sejibh46nh&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_OU9XRWJYd01YUU5lZzZnQkxWVWJQdy0taGZ3M3lPbUpD
...[SNIP]...
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 04:58:27 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: 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://*.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

<?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_REF\x27,\x27CROSSTAB\x27,0\x5d,\x5b\x27HEADER_WIDTH\x27,\x27__HEADER_WIDTH__\x27,0\x5d,\x5b\x27BI_COMMAND_TYPE\x27,\x27UPDATE_HEADER_WIDTH\x27,0\x5d\x5d,true
\x29\x3b","clientheaderhpos":"0sejibh46nh","contextmenucmd":"sap.zen.request.zenSendCommandArrayWoEventWZenPVT\x28\x5b\x5b\x27COL\x27,\x27__COL__\x27,0\x5d,\x5b\x27DOM_REF_ID\x27,\x27__DOM_REF_ID__\x27,0\x5d,\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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349919451; 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=9OWEbXwMXQNeg6gBLVUbPw--7hjmzZmqUbZjAdzxMnFpBw--&Language=EN8hemysvqd5&XSYSTEM=SAP_BW&XQUERY=ZSTKPYMC2_ABS_OVERVIEW_ESS&APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS

Response 1

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 04:58:39 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; 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://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 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\x3d9OWEbXwMXQNeg6gBLVUbPw\x2d\x2d7hjmzZmqUbZjAdzxMnFpBw\x2d\x2d\x26XSYSTEM\x3dSAP_BW
\x26APPLICATION\x3dZGENERIC_ANALYSIS\x26XPROFILE\x3dESS\x26Language\x3dEN8hemysvqd5"
};
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]

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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349919451; 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=9OWEbXwMXQNeg6gBLVUbPw--7hjmzZmqUbZjAdzxMnFpBw--&Language=EN&XSYSTEM=SAP_BW&XQUERY=ZSTKPYMC2_ABS_OVERVIEW_ESS&
APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESSnyg0x776nd
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:10:01 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: 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://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 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\x3d9OWEbXwMXQNeg6gBLVUbPw\x2d\x2d7hjmzZmqUbZjAdzxMnFpBw\x2d\x2d\x26XSYSTEM
\x3dSAP_BW\x26APPLICATION\x3dZGENERIC_ANALYSIS\x26XPROFILE\x3dESSnyg0x776nd\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]

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 **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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349919451; 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=9OWEbXwMXQNeg6gBLVUbPw--7hjmzZmqUbZjAdzxMnFpBw--&Language=EN&XSYSTEM=SAP_BW&XQUERY=ZSTKPYMC2_ABS_OVERVIEW_ESSf1ephnh7xy&
APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:03:32 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: 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://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 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\x253Aportal_content\x252Fcom.sap.pct\x252Fplatform_add_ons\x252Fcom.sap.ip.bi\x252FPages\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudioPreview\x26XQUERY\x3dZSTKPYMC2_ABS_OVERVIEW_ESSf1ephnh7xy\x26sap\x2dext\x2dsid\x3d9OWEbXwMXQNeg6gBLVUbPw\x2d\x2d7hjmzZmqUbZjAdzxMnFpBw\x2d\x2d\x26XSYSTEM\x3dSAP_BW\x26APPLICATION\x3dZGENERIC_ANALYSIS\x26XPROFILE\x3dESS\x26Language\x3dEN"
};
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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349919451; 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=9OWEbXwMXQNeg6gBLVUbPw--7hjmzZmqUbZjAdzxMnFpBw--&Language=EN&XSYSTEM=SAP_BW7fgf8wnsij&XQUERY=ZSTKPYMC2_ABS_OVERVIEW_ESS&APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS

Response 1

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:00:59 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: 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://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 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\x3d9OWEbXwMXQNeg6gBLVUbPw\x2d\x2d7hjmzZmqUbZjAdzxMnFpBw\x2d\x2d\x26XSYSTEM\x3dSAP_BW7fgf8wnsij\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?0vb6fgdqzm=1 HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 04:50:05 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: 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 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.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 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 : "d918b98620ab4f5199b29e607b8f256c",
  urlPrefix : "zen",
  urlParameters : "0vb6fgdqzm\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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349919451; 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=9OWEbXwMXQNeg6gBLVUbPw--7hjmzZmqUbZjAdzxMnFpBw--&Language=EN&XSYSTEM=SAP_BW&XQUERY=ZSTKPYMC2_ABS_OVERVIEW_ESS&
APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS&ihfldtq0c7=1
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:21:07 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; charset=UTF-8
Content-Length: 2462
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu: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

<!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\x2dbw\x2diViewID\x3dpcd\x253Aportal_content\x252Fcom.sap.pct\x252Fplatform_add_ons\x252Fcom.sap.ip.bi\x252FPages\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudioPreview\x26ihfldtq0c7\x3d1\x26XQUERY\x3dZSTKPYMC2_ABS_OVERVIEW_ESS\x26sap\x2dext\x2dsid\x3d9OWEbXwMXQNeg6gBLVUbPw\x2d\x2d7hjmzZmqUbZjAdzxMnFpBw\x2d\x2d\x26XSYSTEM\x3dSAP_BW\x26APPLICATION\x3dZGENERIC_ANALYSIS\x26XPROFILE\x
...[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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349919451; 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.designstudioPreviewemkbfodir7&sap-ext-sid=9OWEbXwMXQNeg6gBLVUbPw--7hjmzZmqUbZjAdzxMnFpBw--&Language=EN&XSYSTEM=SAP_BW&XQUERY=ZSTKPYMC2_ABS_OVERVIEW_ESS&APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS

Response 1

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 04:53:29 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: 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://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 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\x2diViewID\x3dpcd\x253Aportal_content\x252Fcom.sap.pct\x252Fplatform_add_ons\x252Fcom.sap.ip.bi\x252FPages\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudioPreviewemkbfodir7\x26XQUERY\x3dZSTKPYMC2_ABS_OVERVIEW_ESS\x26sap\x2dext\x2dsid\x3d9OWEbXwMXQNeg6gBLVUbPw\x2d\x2d7hjmzZmqUbZjAdzxMnFpBw\x2d\x2d\x26XSYSTEM\x3dSAP_BW\x26APPLICATION\x3dZGENERIC_ANALYSIS\x26XPROFILE\x3dESS
...[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]

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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349919451; 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=9OWEbXwMXQNeg6gBLVUbPw--7hjmzZmqUbZjAdzxMnFpBw--tt31rbwe9w&Language=EN&XSYSTEM=SAP_BW&XQUERY=ZSTKPYMC2_ABS_OVERVIEW_ESS&
APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 04:56:17 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: 2463
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu: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

<!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 : "9OWEbXwMXQNeg6gBLVUbPw\x2d\x2d7hjmzZmqUbZjAdzxMnFpBw\x2d\x2dtt31rbwe9w",
   urlPrefix : "zen",
   urlParameters : "sap\x2dbw\x2diViewID\x3dpcd\x253Aportal_content\x252Fcom.sap.pct\x252Fplatform_add_ons\x252Fcom.sap.ip.bi\x252FPages
\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudioPreview\x26XQUERY\x3dZSTKPYMC2_ABS_OVERVIEW_ESS\x26sap\x2dext\x2dsid
\x3d9OWEbXwMXQNeg6gBLVUbPw\x2d\x2d7hjmzZmqUbZjAdzxMnFpBw\x2d\x2dtt31rbwe9w\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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349919451; 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%253A9OWEbXwMXQNeg6gBLVUbPw--7hjmzZmqUbZjAdzxMnFpBw--%2616555349966919&
SerWinIdString=&Autoclose=1000&DebugSet=&ParamMapCmd=LIST&ParamMapKey=com.sap.portal.dsm.ParamMap%3aGx1655349965174x23xfmpzdbdle5
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 06:44:15 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/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://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
Content-Length: 314

/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen?sap-ext-sid=9OWEbXwMXQNeg6gBLVUbPw--7hjmzZmqUbZjAdzxMnFpBw--&sap-
sessioncmd=USR_ABORT&~SAPSessionCmd=USR_ABORT&SAPWP_ACTIVE=1&sap-ep-tstamp=1655361757625&
dsmguid=1655361855934|#!#|comsapportaldsmParamMapGx1655349965174x23xfmpzdbdle5
```

15.18. 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 [%24DebugAction 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 **%24DebugAction** 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349983849; 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

XPROFILE=ESS&XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW&
ClientWindowID=WID1655349984817&%24Roundtrip=true&%24DebugAction=nullqmk9emltk6
```

Response 1

```
HTTP/1.1 200 OK
```

```
Date: Thu, 16 Jun 2022 06:53:45 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
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
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="nullqmk9emltk6">
...[SNIP]...
```

15.19. 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:	**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 **APPLICATION** 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_ANALYSISd0yf7ip849&XSYSTEM=SAP_BW HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349983849; 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

XPROFILE=ESS&XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW&
ClientWindowID=WID1655349984817&%24Roundtrip=true&%24DebugAction=null
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 06:43:14 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
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
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="APPLICATION" value="ZGENERIC_ANALYSISd0yf7ip849">
...[SNIP]...
<input type="hidden" name="APPLICATION" value="ZGENERIC_ANALYSISd0yf7ip849">
...[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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349983849; 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

XPROFILE=ESS&XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW&
ClientWindowID=WID1655349984817h5miqrrv0b&%24Roundtrip=true&%24DebugAction=null
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 06:50:30 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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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: 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="ClientWindowID" value="WID1655349984817h5miqrrv0b">
...[SNIP]...
<!--
    var trueWindowID = EPCM.getUniqueWindowId();
    if (trueWindowID != "WID1655349984817h5miqrrv0b") {
    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]

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=ESS8wxlw9qnr1&
XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349983849; 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, 16 Jun 2022 06:38:42 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; 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://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: 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="ESS8wxlw9qnr1">
...[SNIP]...
```

15.22. 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:	**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 **XQUERY** 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=ESS&
XQUERY=ZSTKPTMC1_REG_TIME_ESSwax3b8r686&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349983849; 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, 16 Jun 2022 06:41:09 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
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: 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_ESSwax3b8r686">
...[SNIP]...
```

15.23. 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]

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 **XSYSTEM** 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_BWjivc4xku6j HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349983849; 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

XPROFILE=ESS&XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW&
ClientWindowID=WID1655349984817&%24Roundtrip=true&%24DebugAction=null
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 06:45:05 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
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
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_BWjivc4xku6j">
...[SNIP]...
<input type="hidden" name="XSYSTEM" value="SAP_BWjivc4xku6j">
...[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?i7vqaod5g4=1 HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 06:38:15 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
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: 5121

<!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="i7vqaod5g4" 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?XPROFILE=ESS&
XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349983849; 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

XPROFILE=ESS&XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW&
ClientWindowID=WID1655349984817&%24Roundtrip=true&%24DebugAction=null&k74qq9hqvt=1
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 06:58:18 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; 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://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: 8583

<!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="k74qq9hqvt" 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349014046
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.9254b0426ad34dfa
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-9254b0426ad34dfa-01
Content-Length: 5175
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":{},"WA_CLIENT_INFO":{"BUILD_VERSION":"zydd2c34ur"},"IT_APP_CACHE":{},"IT_GUID":{},"WA_MENU_LIST":{},"WA_CATEGORY":{},"WA_USER_DEFAULT":
{"DATFM":"1","DCPFM":"","LANGU":"E","TZONE":"","TZONE_DESCRIPT":"","TIMEFM":"0","NUMBER_GROUPING":"","NUMBER_DECI
...[SNIP]...
```

Response 1

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 16 Jun 2022 08:22:10 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: 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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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

<HTML><HEAD>
```

```
<TITLE>500 SAP Internal Server Error</TITLE>
</HEAD><BODY>
<H1>500 SAP Internal Server Error</H1>
ERROR: zydd2c34ur 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349014046
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.9254b0426ad34dfa
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-9254b0426ad34dfa-01
Content-Length: 5175
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":{},"WA_CLIENT_INFO":{"BUILD_VERSION":"21.10.0006"},"IT_APP_CACHE":{},"IT_GUID":{},"WA_MENU_LIST":{},"WA_CATEGORY":{},"WA_USER_DEFAULT":
{"DATFM":"1","DCPFM":"","LANGU":"E","TZONE":"","TZONE_DESCRIPT":"","TIMEFM":"0","NUMBER_GROUPING":"","NUMBER_DECIMAL":"np7p2jpyuk","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, 16 Jun 2022 09:01:48 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: 409632
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://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

{"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_DESCRIPT":"","TIMEFM":"0","NUMBER_GROUPING":"","NUMBER_DECIMAL":"np7p2jpyuk","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&dxp=21100006&field_id=00384&
ajax_value=PORTAL%7CD%7C%7C%7C HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349014046
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.9254b0426ad34dfa
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-9254b0426ad34dfa-01
Content-Length: 5175
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":{},"WA_CLIENT_INFO":{"BUILD_VERSION":"21.10.0006"},"IT_APP_CACHE":{},"IT_GUID":{},"WA_MENU_LIST":{},"WA_CATEGORY":{},"WA_USER_DEFAULT":
{"DATFM":"1","DCPFM":"","LANGU":"E","TZONE":"","TZONE_DESCRIPT":"","TIMEFM":"0","NUMBER_GROUPING":"om9y1wvona","NUMBER_DECIMAL":"","EDIT":true},"WA_CO
RE":
{"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, 16 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: application/json; charset=utf-8
Content-Length: 409632
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://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

{"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_DESCRIPT":"","TIMEFM":"0","NUMBER_GROUPING":"om9y1wvona","NUMBER_DECIMAL":"","EDIT":true},"modelAppCacheImageDataUpdateData":[2,"GUID","CONTENT"],"modelAppCacheGlobalSettingsData":{"GLOBAL_STYLE":"","RUNTIME_LANGUAGE":"E","BANNER":"","APP_START":""},"model
...[SNIP]...

15.29. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard [TILE_INFO JSON parameter]

Summary

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

Issue detail

The value of the **TILE_INFO** JSON parameter is copied into the application's response.

Request 1

POST /neptune/zalaris_launchpad_standard?ajax_id=SAVE_USER_FAV&ajax_applid=ZALARIS_LAUNCHPAD_STANDARD&sap-client=650&dxp=21100006&field_id=00385 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655350055042; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.5d717e5d02854e6d
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-5d717e5d02854e6d-01
Content-Length: 3647
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_FAV_LIST":[{"IMAGEDATA":"","ICON_IMAGEDATA":"","IMAGE_CONTENT":"","STATEFUL":false,"PARENTS":"","URL_LONG":"/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds?APPLICATION=ZGE
...[SNIP]...
"CHART_GUID":"","MANIFEST":"","TILE_TEXT":"","GUID":"00163EDC07D11ED9A79A9EE959EF27CE","NAME":"Registered time","APPLID":"","ACTIVATED":true,"TILE_ICON":"sap-icon://line-chart-time-axis","TILE_INFO":"0k3wirjhdm","TILE_TITLE":"Registered time","TILE_TYPE":"","TILE_NUMBER":"","TILE_UNIT":"","TILE_INFOSTATE":"None","UPDDAT":"20190819","UPDTIM":"102158","UPDNAM":"VJSP","CREDAT":"20190702","CRETIM":"162330","CRE
...[SNIP]...

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 08:27:36 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: 235
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://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

{"modelAppCacheTilesFavData":
[9,"GUID","SORT","BACK_WIDTH","TILE_HEIGHT","FORCE_ROW","TILE_TITLE","TILE_INFO","NATURAL_WIDTH","NATURAL_HEIGHT","00163EDC07D11ED9A79A9EE959EF
27CE",2,"Small","",false,"Registered time","0k3wirjhdm","",""]}
```

15.30. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard [TILE_TITLE JSON parameter]

Summary

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

Issue detail

The value of the **TILE_TITLE** JSON parameter is copied into the application's response.

Request 1

```
POST /neptune/zalaris_launchpad_standard?ajax_id=SAVE_USER_FAV&ajax_applid=ZALARIS_LAUNCHPAD_STANDARD&sap-client=650&dxp=21100006&field_id=00385
HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655350055042; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.5d717e5d02854e6d
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-5d717e5d02854e6d-01
Content-Length: 3647
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_FAV_LIST":[{"IMAGEDATA":"","ICON_IMAGEDATA":"","IMAGE_CONTENT":"","STATEFUL":false,"PARENTS":"","URL_LONG":"/irj/servlet/prt/portal/prtroot
/com.sap.ip.bi.designstudio.nw.portal.ds?APPLICATION=ZGE
...[SNIP]...
```

TILE_TEXT":"","GUID":"00163EDC07D11ED9A79A9EE959EF27CE","NAME":"Registered time","APPLID":"","ACTIVATED":true,"TILE_ICON":"sap-icon://line-chart-time-axis","TILE_INFO":"","TILE_TITLE":"Registered timebup900hxqp","TILE_TYPE":"","TILE_NUMBER":"","TILE_UNIT":"","TILE_INFOSTATE":"None","UPDDAT":"20190819","UPDTIM":"102158","UPDNAM":"VJSP","CREDAT":"20190702","CRETIM":"162330","CRENAM":"VJSP","SORT":"00002","VIS
...[SNIP]...

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 08:29:34 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; charset=utf-8
content-length: 235
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://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

{"modelAppCacheTilesFavData":
[9,"GUID","SORT","BACK_WIDTH","TILE_HEIGHT","FORCE_ROW","TILE_TITLE","TILE_INFO","NATURAL_WIDTH","NATURAL_HEIGHT","00163EDC07D11ED9A79A9EE959EF27CE",2,"Small","",false,"Registered timebup900hxqp","","","",""]}
```

15.31. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard [field_id parameter]

Summary

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

Issue detail

The value of the **field_id** request parameter is copied into the application's response.

Request 1

```
POST /neptune/zalaris_launchpad_standard?ajax_id=GET_TELEMETRY_APP&ajax_applid=ZALARIS_LAUNCHPAD_STANDARD&sap-client=650&dxp=21100006&
field_id=80287hyjkactrpb HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349718611
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.986a5c12b7a74866
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-986a5c12b7a74866-01
Content-Length: 64
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_TELEMETRY_APP":{"GUID":"00163EDC07D11EE79DF031B99EC46A0F"}}
```

Response 1

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 16 Jun 2022 08:03:50 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: 214
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu: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

<HTML><HEAD>
<TITLE>500 SAP Internal Server Error</TITLE>
</HEAD><BODY>
<H1>500 SAP Internal Server Error</H1>
ERROR: 80287hyjkactrpb cannot be interpreted as a number (termination: RABAX_STATE)<P>
</
...[SNIP]...
```

15.32. https://testportal.zalaris.com/neptune/zmfp_leave_request [field_id parameter]

Summary

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

Issue detail

The value of the **field_id** request parameter is copied into the application's response.

Request 1

```
POST /neptune/zmfp_leave_request?ajax_id=SYNC&ajax_applid=ZMFP_LEAVE_REQUEST&sap-client=650&dxp=21100006&field_id=00253khtvywcsug HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349208750
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.2a5e530e5a9645b4
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-2a5e530e5a9645b4-01
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/1.1 500 Internal Server Error
Date: Thu, 16 Jun 2022 08:37:00 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: 214
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu: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

<HTML><HEAD>
<TITLE>500 SAP Internal Server Error</TITLE>
</HEAD><BODY>
<H1>500 SAP Internal Server Error</H1>
ERROR: 00253khtvywcsug cannot be interpreted as a number (termination: RABAX_STATE)<P>
</
...[SNIP]...
```

15.33. https://testportal.zalaris.com/neptune/zmfp_photo_upload [IMAGESTR JSON parameter]

Summary

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

Issue detail

The value of the **IMAGESTR** JSON parameter is copied into the application's response.

Request 1

```
POST /neptune/zmfp_photo_upload?ajax_id=SAVE&ajax_applid=ZMFP_PHOTO_UPLOAD&sap-client=650&dxp=21100006&field_id=00096 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349983849; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.f375538321d94ce5
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-f375538321d94ce5-01
Content-Length: 162285
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
```

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

{"GWA_PHOTO":{"EMPPHOTOURL":"","IMAGESTR":"data:image\/jpeg;base64,\V9j\/4AAQSkZJRgABAQAAAQABAAD
\/2wBDAAMCAgICAgMCAgIDAwMDBAYEBAQEBAgGBgUGCQgKCgkICQkKDA8MCgsOCwkJDRENDg8QEBEQCgwSExIQEw8QEBD\/2wBDAQMDA
...[SNIP]...
UncfUEDGbJwOlVYqwVJIhPYVSRSRJTGNZgOO9ACr90VLJYFgKLBYYCSSTVFC0AJnJoAWgBCe1AC0AITQAo6UABOKAEFACk4oAQHJoAWgBM5NAC0AIT2FAC0ABOKAJov9
WK0jsYz3B3CDnr6UN2EotkO4sSTSi7myVgqthixnMgqL3Y0T9KZRDLJn5V6dzUtktn\/2Q==wbdxhunps6"}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 09:01:47 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: 324545
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://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

{"modeloPageUploadData":{"EMPPHOTOURL":"
/2wBDAAMCAgICAgMCAgIDAwMDBAYEBAQEBAgGBgUGCQgKCgkICQkKDA8MCgsOCwkJDRENDg8QEBEQCgwSExIQEw8QEBD/2wBDAQMDAwQDBAgEB
...[SNIP]...
7mUncfUEDGbJwOlVYqwVJIhPYVSRSRJTGNZgOO9ACr90VLJYFgKLBYYCSSTVFC0AJnJoAWgBCe1AC0AITQAo6UABOKAEFACk4oAQHJoAWgBM5NAC0AIT2FAC0ABOKAJo
v9WK0jsYz3B3CDnr6UN2EotkO4sSTSi7myVgqthixnMgqL3Y0T9KZRDLJn5V6dzUtktn/2Q==wbdxhunps6"}}
```

15.34. 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349208750
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
```

```
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.33e55f351ef14f24
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-33e55f351ef14f24-01
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":"1655317800000cxqlzkslzn","CAL_ENDDA":1655922599000,"EXP_BEGDA":"20220616","EXP_ENDDA":"20220622","ALL":false}}
```

Response 1

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 16 Jun 2022 08:48:11 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: 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://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

<HTML><HEAD>
<TITLE>500 SAP Internal Server Error</TITLE>
</HEAD><BODY>
<H1>500 SAP Internal Server Error</H1>
ERROR: 1655317800000cxqlzkslzn cannot be interpreted as a number (termination: RABAX_STATE)<P>
...[SNIP]...
```

15.35. 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349208750
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.33e55f351ef14f24
```

```
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-33e55f351ef14f24-01
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":1655317800000,"CAL_ENDDA":"1655922599000fnofu1vuj2","EXP_BEGDA":"20220616","EXP_ENDDA":"20220622","ALL":false}}
```

Response 1

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 16 Jun 2022 08:50:42 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; 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://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

<HTML><HEAD>
<TITLE>500 SAP Internal Server Error</TITLE>
</HEAD><BODY>
<H1>500 SAP Internal Server Error</H1>
ERROR: 1655922599000fnofu1vuj2 cannot be interpreted as a number (termination: RABAX_STATE)<P>
...[SNIP]...
```

15.36. https://testportal.zalaris.com/neptune/zmfp_travel_overview [field_id parameter]

Summary

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

Issue detail

The value of the **field_id** request parameter is copied into the application's response.

Request 1

```
POST /neptune/zmfp_travel_overview?ajax_id=GET_CCC_IMPORTS&ajax_applid=ZMFP_TRAVEL_OVERVIEW&sap-client=650&dxp=21100006&field_id=00159yjfgvmbfdm
HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349356829
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.77ed77fc9d824986
```

```
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-77ed77fc9d824986-01
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/1.1 500 Internal Server Error
Date: Thu, 16 Jun 2022 08:55:21 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
content-length: 214
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu: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

<HTML><HEAD>
<TITLE>500 SAP Internal Server Error</TITLE>
</HEAD><BODY>
<H1>500 SAP Internal Server Error</H1>
ERROR: 00159yjfgvmbfdm cannot be interpreted as a number (termination: RABAX_STATE)<P>
</
...[SNIP]...
```

15.37. 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&dxp=21100006&field_id=00018&
ajax_value=31mvxn81qrb0 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349075680
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.d4dab665c6e74f54
```

```
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-d4dab665c6e74f54-01
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, 16 Jun 2022 08:59:48 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: 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://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

<HTML><HEAD>
<TITLE>500 SAP Internal Server Error</TITLE>
</HEAD><BODY>
<H1>500 SAP Internal Server Error</H1>
ERROR: 31mvxn81qrb0 cannot be interpreted as a number (termination: RABAX_STATE)<P>
</BOD
...[SNIP]...
```

15.38. 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=nVJbT8IwFP4rS99Zt2m20TDIAiEhQWO4%2BOCLKd0BGrt29nSg%2FnrrBAMP%2BuDbSfvdztcORm%2B1Cg5gURpdkDiMSABamErqXUHWq2kvJ6PhAH
mtkoaVrdvrBby2gC7wRI3s%2B6YgrdXMcJTlNK8BmRNsWd7NWRJGrLHGGWEUCUpEsM5bjY3Gtga7BHuQAtaLeUH2zjXIKHVe%2FShfZPjBFbcSQ2Fq2qh2JzVSzz8ocPTLF9GQ
YOLRUnPX5b%2BUaIx1XF2JdGGprBraUWeTgjxXeZLCJtluqkyIPK22uehnt370U5bl3MMQW5hpdFy7giRRkvSitBenq%2BiGJX0Wx2E%2FTZ9I8Hhu0e9MTp2xjmwvy%2Fq7K35uiAz
%2F08eAXtr%2BPNy995lNHoyS4j0olTLHsQXuoCDOtkCCqbE1d78ni8O4O5FVb9tBWauxASG3EipChyfb6x8y%2FAQ%3D&RelayState=-T9051-https%3a
%2f%2ftestwiki.zalaris.com%2fzhsr3lq3cgqioz HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655350119630; 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-site
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 09:07:16 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;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://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: 1747

<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="-T9051-https://testwiki.zalaris.com/zhsr3lq3cgqioz"/>
...[SNIP]...
```

15.39. 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=55pkkn634s HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 09:06:29 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: 1821
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu: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

<?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;55pkkn634s&quot;.</span>
...[SNIP]...
```

15.40. 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=72noid81gp HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 09:09:12 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: 19959
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://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>
<head>

<meta http-equiv="cache-control" content="no-cache">
<title>SAP GUI for HTML</title>
<link id="urStdCssLink" class="sapThemeMetaData-UR-ls" rel="STYLESHEET" href="
...[SNIP]...
<script type="text/javascript">document.forms["webguiStartForm"].elements["~tx"].value = decodeURIComponent("72noid81gp");</script>
...[SNIP]...
<script type="text/javascript">document.forms["webguiStartForm"].elements["~transaction"].value = decodeURIComponent("72noid81gp");</script>
...[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/zmfp_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 **g226gmho21%41tko7taq8la** 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 **g226gmho21Atko7taq8la** 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=g226gmho21%2541tko7taq8la&XSYSTEM=SAP_BW HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349983849; 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

XPROFILE=ESS&XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW&
ClientWindowID=WID1655349984817&%24Roundtrip=true&%24DebugAction=null
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 06:44:10 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
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
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: 8545

<!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="g226gmho21Atko7taq8la">
...[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]

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 **pixchnhk6f%41h4mvhbr4nq** 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 **pixchnhk6fAh4mvhbr4nq** 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=pixchnhk6f%2541h
4mvhbr4nq&XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349983849; 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

XPROFILE=ESS&XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW&
ClientWindowID=WID1655349984817&%24Roundtrip=true&%24DebugAction=null
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 06:40:09 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
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
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="pixchnhk6fAh4mvhbr4nq">
...[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 **xgg0nnqfgy%41rohs8xxfs5** 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 **xgg0nnqfgyArohs8xxfs5** 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=xgg0nnqfgy%2541rohs8xxfs5&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349983849; 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

XPROFILE=ESS&XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW&
ClientWindowID=WID1655349984817&%24Roundtrip=true&%24DebugAction=null
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 06:42:18 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; 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://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: 8535

<!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="xgg0nnqfgyArohs8xxfs5">
...[SNIP]...
```

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]

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 **XSYSTEM** request parameter, and echo the result in the response.

The payload **vupdq56lyn%41o91io58dw3** was submitted in the XSYSTEM parameter. This payload contains the %41 sequence, corresponding to the character 'A'. The input was copied into the application's response as **vupdq56lynAo91io58dw3** 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=ZGENERIC_ANALYSIS&XSYSTEM=vupdq56lyn%2541o91io58dw3 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349983849; 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

XPROFILE=ESS&XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW&
ClientWindowID=WID1655349984817&%24Roundtrip=true&%24DebugAction=null
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 06:46:02 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
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
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="XSYSTEM" value="vupdq56lynAo91io58dw3">
...[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 **4rlhgf3t8u%413k7idmshe7** 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 **4rlhgf3t8uA3k7idmshe7** 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&dxp=21100006&field_id=00018&
ajax_value=4rlhgf3t8u%25413k7idmshe7 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349075680
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.d4dab665c6e74f54
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-d4dab665c6e74f54-01
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, 16 Jun 2022 09:01:18 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; 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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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

<HTML><HEAD>
<TITLE>500 SAP Internal Server Error</TITLE>
</HEAD><BODY>
<H1>500 SAP Internal Server Error</H1>
ERROR: 4rlhgf3t8uA3k7idmshe7 cannot be interpreted as a number (termination: RABAX_STATE)<P>
...[SNIP]...
```

17. Cross-domain Referer leakage

There are 3 instances of this issue:

- /nea/v1/authenticate
- /neptune/
- /neptune/server/js/sun/suneditor.min.js

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, 16 Jun 2022 03:08:30 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-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://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: com.sap.engine.security.authentication.original_application_url=GET#0kzh
%2F%2FAyUjkjm0k4o9RrxRftCqGFdLeQFH%2FAmJoT4DKc%2BOmwgCXg2GlZ4RP3V7tycXlkpU0%2FS63yj263pKn4UdBlhVyCnQD069VrKFuZLwzz6L%2Fv6GHnjf2isj8lCQV8cX
X09dqvnNMnZ5cmoql0Su99%2F7%2BCWYKXUq7585jQ3tAxV7Cv34kfrFoloYCja%2Fi4StuoDaQcAPOJnW5jpcR3CPo1GEwl6%2B5l9TL931O7YtM%3D;Path=/nea
/v1/authenticate;HttpOnly; SameSite=None; Secure
set-cookie: saplb_PORTAL=(J2EE1289120)1289150; 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw
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, 16 Jun 2022 03:09:56 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: 1889559
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
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://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: 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]...
```

17.3. 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 page was loaded from a URL containing a query string:

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

The response contains the following link to another domain:

- https://katex.org/docs/supported.html

Request 1

```
GET /neptune/server/js/sun/suneditor.min.js?21.10.0006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; 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: 20220616 051014 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: 2328807
dxp-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-cache-control: +86400
sap-isc-etag: C2C0DC5F147F0375E10000000ADC9967
sap-isc-uagent: 0
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://*.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

!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]...
<label>'+t.dialogBox.mathBox.inputLabel+' (<a href="https://katex.org/docs/supported.html" target="_blank">KaTeX</a>
...[SNIP]...
```

18. Cross-domain script include

There are 7 instances of this issue:

- /irj/portal
- /nea/v1/authenticate
- /neptune/
- /neptune/ZMFP_DASH_ESS_NEXT_SALARY.view.js
- /neptune/ZSP_SUPPINFO_FRONTEND
- /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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:32 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
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://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: PortalAlias=portal; Path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 13739

<!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%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, 16 Jun 2022 03:08:30 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-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://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: com.sap.engine.security.authentication.original_application_url=GET#0kzh
%2F%2FAyUjkjm0k4o9RrxRftCqGFdLeQFH%2FAmJoT4DKc%2BOmwgCXg2GlZ4RP3V7tycXIkpU0%2FS63yj263pKn4UdBlhVyCnQD069VrKFuZLwzz6L%2Fv6GHnjf2isj8lCQV8cX
X09dqvnNMnZ5cmoql0Su99%2F7%2BCWYKXUq7585jQ3tAxV7Cv34kfrFoloYCja%2Fi4StuoDaQcAPOJnW5jpcR3CPo1GEwl6%2B5l9TL931O7YtM%3D;Path=/nea
/v1/authenticate;HttpOnly; SameSite=None; Secure
set-cookie: saplb_PORTAL=(J2EE1289120)1289150; 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw
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, 16 Jun 2022 03:09:56 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: 1889559
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
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://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: 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:40 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/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://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

<!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/ZSP_SUPPINFO_FRONTEND

Summary

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

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/ZSP_SUPPINFO_FRONTEND HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655350055042; 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, 16 Jun 2022 03:28:39 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: 24466
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-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://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="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="sap_goldreflection"
data-sap-ui-libs="sap.ui.layout,sap.m,sap.ui.commons">
</script>
...[SNIP]...
```

18.6. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:46 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: 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://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="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="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]...
```

18.7. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:47 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: 35120
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://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="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]...
```

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:32 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
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://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: PortalAlias=portal; Path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 13739

<!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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw
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, 16 Jun 2022 03:09:56 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: 1889559
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
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://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: 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 **jwr055mma6** 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%2fredirectjwr055mma6 HTTP/1.1
Host: testportal.zalaris.com
Cookie: com.sap.engine.security.authentication.original_application_url=GET#0kzh
%2F%2FAyUjkjm0k4o9RrxRftCqGFdLeQFH%2FAmJoT4DKc%2BOmwgCXg2GlZ4RP3V7tycXlkpU0%2FS63yj263pKn4UdBlhVyCnQD069VrKFuZLwzz6L%2Fv6GHnjf2isj8lCQV8cX
X09dqvnNMnZ5cmoql0Su99%2F7%2BCWYKXUq7585jQ3tAxV7Cv34kfrFoloYCja%2Fi4StuoDaQcAPOJnW5jpcR3CPo1GEwl6%2B5l9TL931O7YtM%3D; saplb_PORTAL=
(J2EE1289120)1289150
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: 123
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=u%2FGb4qHVAEb1R0xtVO%2FXdGFGDA8%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, 16 Jun 2022 06:43:46 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: 94
location: https://testportal.zalaris.com/ep/redirectjwr055mma6
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu: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
set-cookie: MYSAPSSO2=; expires=Thu, 01-Jan-1970 00:00:00 GMT; path=/ ; domain=.zalaris.com; SameSite=None; Secure
set-cookie: com.sap.security.sso.OTPSESSIONID=; 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
</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 static code analysis, which may lead to false positives that are not actually exploitable. The relevant code and execution paths should be reviewed 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:32 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
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://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: PortalAlias=portal; Path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 13739

<!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,en-GB;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/97.0.4692.71 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:33:13 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: application/x-javascript
last-modified: Fri, 11 Mar 2022 05:02:00 GMT
cache-control: max-age=604800
```

```
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://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

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.AFPPlugin.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, 16 Jun 2022 03:08:30 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-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://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: com.sap.engine.security.authentication.original_application_url=GET#0kzh
%2F%2FAyUjkjm0k4o9RrxRftCqGFdLeQFH%2FAmJoT4DKc%2BOmwgCXg2GlZ4RP3V7tycXlkpU0%2FS63yj263pKn4UdBlhVyCnQD069VrKFuZLwzz6L%2Fv6GHnjf2isj8lCQV8cX
X09dqvnNMnZ5cmoql0Su99%2F7%2BCWYKXUq7585jQ3tAxV7Cv34kfrFoloYCja%2Fi4StuoDaQcAPOJnW5jpcR3CPo1GEwl6%2B5l9TL931O7YtM%3D;Path=/nea
/v1/authenticate;HttpOnly; SameSite=None; Secure
set-cookie: saplb_PORTAL=(J2EE1289120)1289150; 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 static code analysis, which may lead to false positives that are not actually exploitable. The relevant code and execution paths should be reviewed 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**

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 **8dfayjih1a** 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=8dfayjih1a HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 12:26:27 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: 19959
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://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>
<head>

<meta http-equiv="cache-control" content="no-cache">
<title>SAP GUI for HTML</title>
<link id="urStdCssLink" class="sapThemeMetaData-UR-ls" rel="STYLESHEET" href="
...[SNIP]...
<script type="text/javascript">document.forms["webguiStartForm"].elements["~tx"].value = decodeURIComponent("8dfayjih1a");</script>
...[SNIP]...
```

Static analysis

The value of the **~transaction** request parameter is copied into a JavaScript string literal. The payload **8dfayjih1a** 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("8dfayjih1a");`

Dynamic analysis

The value of the **~transaction** request parameter is copied into a JavaScript string literal. The payload **8dfayjih1a** was submitted in the ~transaction parameter.

The string containing the payload is then passed to **input.value**.

The previous value reached the sink as:

```
iqjoohh6il
```

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=: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=: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 **8dfayjih1a** 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=8dfayjih1a HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 12:26:27 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: 19959
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://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>
<head>

<meta http-equiv="cache-control" content="no-cache">
<title>SAP GUI for HTML</title>
<link id="urStdCssLink" class="sapThemeMetaData-UR-ls" rel="STYLESHEET" href="
...[SNIP]...
<script type="text/javascript">document.forms["webguiStartForm"].elements["~transaction"].value = decodeURIComponent("8dfayjih1a");</script>
...[SNIP]...

Static analysis

The value of the **~transaction** request parameter is copied into a JavaScript string literal. The payload **8dfayjih1a** 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("8dfayjih1a");`

Dynamic analysis

The value of the **~transaction** request parameter is copied into a JavaScript string literal. The payload **8dfayjih1a** was submitted in the ~transaction parameter.

The string containing the payload is then passed to **input.value**.

The previous value reached the sink as:

```
ml6lr5gvs1
```

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=: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=:457:170
```

---

23. Backup file

There are 65 instances of this issue:

- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/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/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

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655355511140
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 04:59:03 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/octet-stream;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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

dummyNotUsed
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/fqdd.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655355511140
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 04:59:05 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: 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://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

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**

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655355511140
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 04:59:17 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-gzip;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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

dummyNotUsed
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/sly.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655355511140
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 05:00:19 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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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
```

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655355511140
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:04:17 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/java-archive;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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

dummyNotUsed

Request 2

GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/sgih.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655355511140

Response 2

HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 05:05:20 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: 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://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

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655355511140
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 04:59:11 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 08:29:39 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://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
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/qmxb.js.exe HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655355511140
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 04:59:14 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: 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://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
```

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**

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655355511140
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:03:41 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-gzip;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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
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/hxh.js.gz HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655355511140
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 05:04:46 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: 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://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
```

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**

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356111218
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:09:09 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/java-archive;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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
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/hyge.js.jar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356111218

Response 2

HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 05:10:14 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: 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://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

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;

```
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655357312062
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:31:14 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-rar-compressed;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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
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/etiv.js.rar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655357312062
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 05:32:19 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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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
```

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**

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356351259
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:14:42 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-tar;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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
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/hswy.js.tar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356351259
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 05:15:47 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: 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://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

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**

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356711504

Response 1

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:20:16 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/x-gzip;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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
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/pgnykde.js.tar.gz HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356711504
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 05:21:21 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
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://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
```

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356711504
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:25:45 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/zip;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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
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/vskx.js.zip HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356711504
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 05:26:51 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: 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://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
```

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356711504
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:25:35 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-rar-compressed;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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

dummyNotUsed
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/rapd.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356711504
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 05:26:37 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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356111218
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:09:41 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-tar;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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

dummyNotUsed
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/fceu.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356111218
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 05:10:45 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: 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://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
```

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356351259
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:15:02 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: application/x-gzip;charset=UTF-8
```

```
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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

dummyNotUsed
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/fzpiklt.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356351259
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 05:16:04 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://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
```

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**

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356711504
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:20:20 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/zip;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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

dummyNotUsed
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/febh.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356711504
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 05:21:22 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: 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://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
```

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**

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.exe HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356351259
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:13:37 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/octet-stream;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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

dummyNotUsed
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/dwkw.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356351259
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 05:14:39 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: 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://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
```

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 HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356711504
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:18:52 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-gzip;charset=UTF-8
```

```
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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

dummyNotUsed
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/aua.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356711504
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 05:19:54 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; 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://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
```

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**

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.jar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356711504
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:24:07 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/java-archive;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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

dummyNotUsed
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/onbq.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356711504
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 05:25:09 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://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

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356351259
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:13:21 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/octet-stream;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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
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/hpuz.js.exe HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
```

```
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356351259
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 05:14:29 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: 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://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
```

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356711504
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:19:32 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/x-gzip;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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
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/pnc.js.gz HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356711504
```

Response 2

HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 05:20:43 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: 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://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

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356711504
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:25:06 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/java-archive;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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
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/xhbp.js.jar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655356711504
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 05:26:17 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: 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://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
```

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655358152788
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:48:23 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-rar-compressed;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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
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/tidr.js.rar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655358152788
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 05:49:27 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://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
```

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.tar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655357312062
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:30:51 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/x-tar;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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
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/wloe.js.tar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655357312062

Response 2

HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 05:31:59 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://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

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655357312062

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:36:44 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-gzip;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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
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/qhwjglx.js.tar.gz HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655357312062
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 05:37:52 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: 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://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
```

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655357912631
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:42:53 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/zip;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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
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/ujqe.js.zip HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655357912631
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 05:44:01 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: 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://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

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**

Request 1

GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.rar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655358152788

Response 1

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:45:17 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-rar-compressed;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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

dummyNotUsed
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/zgbh.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655358152788
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 05:46:19 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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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
```

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**

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.tar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655357312062
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:29:26 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/x-tar;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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

dummyNotUsed
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/llcf.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655357312062
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 05:30:28 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: 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://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
```

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: **/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.gz HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655357312062
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:34:44 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-gzip;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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

dummyNotUsed
```

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/dtivsao.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655357312062
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 05:35:45 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: 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://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

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**

Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.zip HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655357912631
```

Response 1

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 05:40:02 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: application/zip;charset=UTF-8
cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 08:29:39 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://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

dummyNotUsed

Request 2

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/khwf.js HTTP/1.1
```

```
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655357912631
```

Response 2

```
HTTP/1.1 404 Not Found
Date: Thu, 16 Jun 2022 05:41:04 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://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
```

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?dxp=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842; 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: FpYmCInd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.a24fa30e4dbe4255
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-a24fa30e4dbe4255-01
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
Content-Type: application/x-www-form-urlencoded
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:21:33 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/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: 20220611102426
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://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
```

Request 2

```
POST /neptune/n.view.js1?dxp=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.a24fa30e4dbe4255
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-a24fa30e4dbe4255-01
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
Content-Type: application/x-www-form-urlencoded
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:21:36 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; 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://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

<!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"> <img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512">
...[SNIP]...
404 Not found <h1 class="mb-3 bd-text-purple-bright">Page not found</h1> Sorry, but it looks like that the page you are looking for is not available. Try too search again or go back to the previous page. Go back
...[SNIP]...
<footer class="zal-footer"> <img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23">
...[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?dxp=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.a24fa30e4dbe4255
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-a24fa30e4dbe4255-01
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
Content-Type: application/x-www-form-urlencoded
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:21:50 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/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: 20220611102426
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://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

Request 2

POST /neptune/w.view.js2?dxp=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.a24fa30e4dbe4255
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-a24fa30e4dbe4255-01
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
Content-Type: application/x-www-form-urlencoded

Response 2

HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:21:53 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
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://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

<!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"><img
class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512">
...[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"><img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23">
...[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?dxp=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.a24fa30e4dbe4255
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-a24fa30e4dbe4255-01
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
Content-Type: application/x-www-form-urlencoded
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:20:58 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/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: 20220611102426
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://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
```

Request 2

```
POST /neptune/coyyxkt.view.js_backup?dxp=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.a24fa30e4dbe4255
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-a24fa30e4dbe4255-01
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
Content-Type: application/x-www-form-urlencoded
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:21:01 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/javascript; 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://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

<!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"> <img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512">
...[SNIP]...
404 Not found <h1 class="mb-3 bd-text-purple-bright">Page not found</h1> Sorry, but it looks like that the page you are looking for is not available. Try too search again or go back to the previous page. Go back
...[SNIP]...
<footer class="zal-footer"> <img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23">
...[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?dxp=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.a24fa30e4dbe4255
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-a24fa30e4dbe4255-01
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
Content-Type: application/x-www-form-urlencoded
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:20:23 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
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220611102426
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://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
```

Request 2

```
POST /neptune/twpy.view.js_bak?dxp=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.a24fa30e4dbe4255
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-a24fa30e4dbe4255-01
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
Content-Type: application/x-www-form-urlencoded
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:20:26 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/javascript; 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://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

<!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"><img
class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512">
...[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"><img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23">
...[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?dxp=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.a24fa30e4dbe4255
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-a24fa30e4dbe4255-01
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
Content-Type: application/x-www-form-urlencoded
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:19:47 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/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: 20220611102426
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://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
```

Request 2

```
POST /neptune/fipv.view.js_old?dxp=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
```

```
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.a24fa30e4dbe4255
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-a24fa30e4dbe4255-01
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
Content-Type: application/x-www-form-urlencoded
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:19:50 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: application/javascript; 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://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

<!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"><img
class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512">
...[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"><img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23">
...[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?dxp=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.a24fa30e4dbe4255
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-a24fa30e4dbe4255-01
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
Content-Type: application/x-www-form-urlencoded
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:20:41 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/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: 20220611102426
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://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
```

Request 2

```
POST /neptune/xcs.view.jsbak?dxp=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.a24fa30e4dbe4255
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-a24fa30e4dbe4255-01
```

```
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
Content-Type: application/x-www-form-urlencoded
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:20:43 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/javascript; 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://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

<!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"><img
class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512">
...[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"><img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23">
...[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?dxp=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.a24fa30e4dbe4255
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-a24fa30e4dbe4255-01
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
Content-Type: application/x-www-form-urlencoded
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:21:15 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
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: 20220611102426
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://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
```

Request 2

```
POST /neptune/flh.view.jsinc?dxp=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MbIRdOCLc/kjOPX0D/p|1655349014046|1655363917842; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.a24fa30e4dbe4255
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-a24fa30e4dbe4255-01
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
Content-Type: application/x-www-form-urlencoded
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:21:19 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: application/javascript; 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://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

<!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"><img
class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512">
...[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"><img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23">
...[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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.a24fa30e4dbe4255
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-a24fa30e4dbe4255-01
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
Content-Type: application/x-www-form-urlencoded
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:20:05 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/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: 20220611102426
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://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
```

Request 2

```
POST /neptune/rjv.view.jsold?dxp=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.a24fa30e4dbe4255
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-a24fa30e4dbe4255-01
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
Content-Type: application/x-www-form-urlencoded
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:20:08 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/javascript; 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://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

<!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"> <img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512">
...[SNIP]...
404 Not found <h1 class="mb-3 bd-text-purple-bright">Page not found</h1> Sorry, but it looks like that the page you are looking for is not available. Try too search again or go back to the previous page. Go back
...[SNIP]...
<footer class="zal-footer"> <img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23">
...[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~?dxp=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.a24fa30e4dbe4255
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-a24fa30e4dbe4255-01
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
Content-Type: application/x-www-form-urlencoded

Response 1

HTTP/1.1 200 OK

```
Date: Thu, 16 Jun 2022 07:19:14 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: 20220611102426
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://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
```

Request 2

```
POST /neptune/p.view.js~?dxp=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.a24fa30e4dbe4255
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-a24fa30e4dbe4255-01
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
Content-Type: application/x-www-form-urlencoded
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:19:17 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/javascript; 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://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

<!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"> <img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512">
...[SNIP]...
404 Not found <h1 class="mb-3 bd-text-purple-bright">Page not found</h1> Sorry, but it looks like that the page you are looking for is not available. Try too search again or go back to the previous page. Go back
...[SNIP]...
<footer class="zal-footer"> <img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23">
...[SNIP]...

23.38. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:19:05 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://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


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

Request 2

```
GET /neptune/native/yy.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:19:07 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/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://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 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"><img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"></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"><img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"></div></div></footer></body>
...[SNIP]...
```

23.39. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:19:40 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: 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
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/nny.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:19:43 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: 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://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 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"><img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"></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><footer class="zal-footer"><div class="container-fluid"><div
class="text-center p-md-5"><img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"></div></div></footer></body>
...[SNIP]...
```

23.40. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:19:19 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: 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
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/hq.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:19:21 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
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://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 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"><img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"></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><footer class="zal-footer"><div class="container-fluid"><div
class="text-center p-md-5"><img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"></div></div></footer></body>
...[SNIP]...
```

23.41. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:19:54 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; 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
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/onv.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
```

```
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:19:56 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: 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://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 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"><img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"></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"><img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"></div></div></footer></body>
...[SNIP]...
```

23.42. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363557512
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:18:36 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: 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
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/brvl.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363557512
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:18:38 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: 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://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 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"><img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"></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><footer class="zal-footer"><div class="container-fluid"><div class="text-center p-md-5"><img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"></div></div></footer></body>
...[SNIP]...
```

23.43. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:18:52 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
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
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/ricpswg.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:18:54 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; 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://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 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"><img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"></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><footer class="zal-footer"><div class="container-fluid"><div
class="text-center p-md-5"><img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"></div></div></footer></body>
...[SNIP]...
```

23.44. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

```
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363557512
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:18:22 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: 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
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/mctb.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363557512
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:18:24 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: 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://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 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"> <img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"> 404 Not found <h1 class="mb-3 bd-text-purple-bright">Page not found</h1> Sorry, but it looks like that the page you are looking for is not available. Try too search again or go back to the previous page. Go back </main><footer class="zal-footer"> <img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"> </footer></body>
...[SNIP]...

23.45. https://testportal.zalaris.com/neptune/native/neptune_login_ping.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.bz2 HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:20:08 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; 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
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/aawi.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:20:10 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: 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://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 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"><img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"></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><footer class="zal-footer"><div class="container-fluid"><div
class="text-center p-md-5"><img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"></div></div></footer></body>
...[SNIP]...
```

23.46. https://testportal.zalaris.com/neptune/native/neptune_login_ping.cbz

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.cbz HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:20:23 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; 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
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/eucp.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:20:25 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: 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://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 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"><img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"></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><footer class="zal-footer"><div class="container-fluid"><div
class="text-center p-md-5"><img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"></div></div></footer></body>
...[SNIP]...
```

23.47. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:23:58 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
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/ncqd.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:24:00 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-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://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 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"><img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"></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><footer class="zal-footer"><div class="container-fluid"><div
class="text-center p-md-5"><img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"></div></div></footer></body>
...[SNIP]...
```

23.48. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:20:36 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
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
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/rqtx.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:20:37 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: 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://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 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"><img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"></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><footer class="zal-footer"><div class="container-fluid"><div
class="text-center p-md-5"><img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"></div></div></footer></body>
...[SNIP]...
```

23.49. https://testportal.zalaris.com/neptune/native/neptune_login_ping.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.gz HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:20:49 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; 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
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/gvu.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:20:51 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: 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://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 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"> <img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"> 404 Not found <h1 class="mb-3 bd-text-purple-bright">Page not found</h1> Sorry, but it looks like that the page you are looking for is not available. Try too search again or go back to the previous page. Go back </main><footer class="zal-footer"> <img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"> </footer></body>
...[SNIP]...

23.50. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:24:14 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: 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
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/icvu.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:24:16 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; 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://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 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"><img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"></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><footer class="zal-footer"><div class="container-fluid"><div
class="text-center p-md-5"><img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"></div></div></footer></body>
...[SNIP]...
```

23.51. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:24:28 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://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


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

Request 2

```
GET /neptune/native/wkemksii.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:24:30 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: 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://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 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"> <img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"> 404 Not found <h1 class="mb-3 bd-text-purple-bright">Page not found</h1> Sorry, but it looks like that the page you are looking for is not available. Try too search again or go back to the previous page. Go back </main><footer class="zal-footer"> <img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"> </footer></body>
...[SNIP]...

23.52. https://testportal.zalaris.com/neptune/native/neptune_login_ping.jar

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.jar HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842

Response 1

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:21:02 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: 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
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/ulne.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:21:04 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: 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://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 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"><img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"></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><footer class="zal-footer"><div class="container-fluid"><div
class="text-center p-md-5"><img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"></div></div></footer></body>
...[SNIP]...
```

23.53. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:21:16 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; 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
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/kkdly.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:21:17 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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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 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"> <img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"> 404 Not found <h1 class="mb-3 bd-text-purple-bright">Page not found</h1> Sorry, but it looks like that the page you are looking for is not available. Try too search again or go back to the previous page. Go back </main><footer class="zal-footer"> <img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"> </footer></body>
...[SNIP]...

23.54. https://testportal.zalaris.com/neptune/native/neptune_login_ping.old

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.old HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363557512

Response 1

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:18:07 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; 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
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/uwbg.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363557512
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:18:09 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: 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://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 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"><img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"></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><footer class="zal-footer"><div class="container-fluid"><div
class="text-center p-md-5"><img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"></div></div></footer></body>
...[SNIP]...
```

23.55. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:23:13 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
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
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/gbcm.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:23:15 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: 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://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 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"><img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"></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><footer class="zal-footer"><div class="container-fluid"><div
class="text-center p-md-5"><img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"></div></div></footer></body>
...[SNIP]...
```

23.56. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:21:29 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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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


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

Request 2

```
GET /neptune/native/alqg.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:21:31 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://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 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"> <img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"> 404 Not found <h1 class="mb-3 bd-text-purple-bright">Page not found</h1> Sorry, but it looks like that the page you are looking for is not available. Try too search again or go back to the previous page. Go back </main><footer class="zal-footer"> <img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"> </footer></body>
...[SNIP]...

23.57. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:21:42 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; 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
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/cbgtymz.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:21:44 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: 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://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 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"><img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"></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><footer class="zal-footer"><div class="container-fluid"><div
class="text-center p-md-5"><img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"></div></div></footer></body>
...[SNIP]...
```

23.58. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:21:55 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: 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
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/hbcaejpp.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:21:57 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
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://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 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"> <img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"> 404 Not found <h1 class="mb-3 bd-text-purple-bright">Page not found</h1> Sorry, but it looks like that the page you are looking for is not available. Try too search again or go back to the previous page. Go back </main><footer class="zal-footer"> <img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"> </footer></body>
...[SNIP]...

23.59. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:22:08 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; 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
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/mclqifz.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:22:10 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: 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://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 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"><img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"></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><footer class="zal-footer"><div class="container-fluid"><div
class="text-center p-md-5"><img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"></div></div></footer></body>
...[SNIP]...
```

23.60. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:22:22 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: 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
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/jiwpnptek.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:22:23 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; 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://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 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"> <img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"> 404 Not found <h1 class="mb-3 bd-text-purple-bright">Page not found</h1> Sorry, but it looks like that the page you are looking for is not available. Try too search again or go back to the previous page. Go back </main><footer class="zal-footer"> <img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"> </footer></body>
...[SNIP]...

23.61. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842

Response 1

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:22:34 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
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
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/nghmvpu.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:22:36 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: 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://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 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"><img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"></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><footer class="zal-footer"><div class="container-fluid"><div
class="text-center p-md-5"><img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"></div></div></footer></body>
...[SNIP]...
```

23.62. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:23:44 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
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
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/hnau.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:23:45 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
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://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 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"><img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"></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><footer class="zal-footer"><div class="container-fluid"><div
class="text-center p-md-5"><img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"></div></div></footer></body>
...[SNIP]...
```

23.63. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:23:27 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: 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
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/adue.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:23:29 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: 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://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 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"> <img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"> 404 Not found <h1 class="mb-3 bd-text-purple-bright">Page not found</h1> Sorry, but it looks like that the page you are looking for is not available. Try too search again or go back to the previous page. Go back </main><footer class="zal-footer"> <img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"> </footer></body>
...[SNIP]...

23.64. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842

Response 1

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:22:47 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: 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
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close

<body >
</body>
</html>

Request 2

```
GET /neptune/native/emz.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:22:49 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; 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://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 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"><img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"></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><footer class="zal-footer"><div class="container-fluid"><div
class="text-center p-md-5"><img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"></div></div></footer></body>
...[SNIP]...
```

23.65. 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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 07:23:00 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
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
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/gvud.html HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; SAPWP_active=1;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655363917842
```

Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 16 Jun 2022 07:23:02 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://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 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"> <img class="img-fluid mb-3 mb-md-0" src="/assets/img/404.jpg" alt="" width="683" height="512"> 404 Not found <h1 class="mb-3 bd-text-purple-bright">Page not found</h1> Sorry, but it looks like that the page you are looking for is not available. Try too search again or go back to the previous page. Go back </main><footer class="zal-footer"> <img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"> </footer></body>
...[SNIP]...

---

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/analyticgrid/Grid.js
- /neptune/public/application/zalaris_common_used/js/jspdf.js
- /neptune/zmfp_personal_profile
- /neptune/zmfp_setup_wizard

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/analyticgrid/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/analyticgrid/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/analyticgrid/Grid.js
HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349919451; 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, 16 Jun 2022 03:26:22 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
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://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
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 = functio
...[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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349718611
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: 20220616 052218 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
dxp-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: 00163EDC07D11ED9B88BF57517ABF213
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://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

!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]...
<james@parall.ax>
...[SNIP]...
rdo.morais@usp.br
* 2013 Lee Driscoll, https://github.com/lsdriscoll
* 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349578618
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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.d1920a3ecc4043ff
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-d1920a3ecc4043ff-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, 16 Jun 2022 03:20:00 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: 85750
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://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

{"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","ORG_TEXT":"","POS_TEXT":"Project Manager ICT","MAN_NAME":"Tommy Andersen","MAN_NAME_VIS":true,"ICON":"","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","USRTY","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/neptune/zmfp_setup_wizard

Summary

Severity: **Information**

Confidence: **Certain**

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

Path: **/neptune/zmfp_setup_wizard**

Issue detail

The following email address was disclosed in the response:

- noreply@zalaris.com

Request 1

```
POST /neptune/zmfp_setup_wizard?ajax_id=GET_DATA&ajax_applid=ZMFP_SETUP_WIZARD&sap-client=650&dxp=21100006&field_id=00012 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650;
ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454;
ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655350119630; 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: FpYmClnd+RtLTtE3bzKaoOnTed8qWdro3ky0XweNI/Q=1696260A59DDF91B4B4ED1376F329AA0E9D379DF2A59
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |40a05d456dfc4d6999abcff0b7c296be.83f15385e45045b1
Traceparent: 00-40a05d456dfc4d6999abcff0b7c296be-83f15385e45045b1-01
Content-Length: 14
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_DATA":{}}
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:29:24 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: 26664
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://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

{"modeloPageData":{"ROLE":"","ROLEID":"1FA","ROLETYPE":"","WIZTYPE":"1","SYSID":"ZEQ","SHOW_OTP":"","STEP1_OPT2_TXT":"Via Zalaris HR Portal: download the app by
scanning the QR-code which you can find
...[SNIP]...
your phone and the relevant appstore will open where you can easily install the app. For iOS / iPhone the app will install instantly upon scanning the QR code.","ID_ITEXT":" Note:
Possibly email from noreply@zalaris.com will be determined as Junk.\\n So if you are not getting the e-mail please check your \"Junk\" folder as well.","FIN_ITEXT":" The first time
you log in to Zalaris HR app with username and password, yo
...[SNIP]...
your phone and the relevant appstore will open where you can easily install the app. For iOS / iPhone the app will install instantly upon scanning the QR code.","ID_ITEXT":" Note:
Possibly email from noreply@zalaris.com will be determined as Junk.\\n So if you are not getting the e-mail please check your \"Junk\" folder as well.","FIN_ITEXT":" The first time
you log in to Zalaris HR app with username and password, yo
...[SNIP]...
```

your phone and the relevant appstore will open where you can easily install the app. For iOS / iPhone the app will install instantly upon scanning the QR code.","ID_ITEXT":" Note: Possibly email from noreply@zalaris.com will be determined as Junk.\\n So if you are not getting the e-mail please check your \"Junk\" folder as well.","FIN_ITEXT":" The first time you log in to Zalaris HR app with username and password, yo
...[SNIP]...
your phone and the relevant appstore will open where you can easily install the app. For iOS / iPhone the app will install instantly upon scanning the QR code.","ID_ITEXT":" Note: Possibly email from noreply@zalaris.com will be determined as Junk.\\n So if you are not getting the e-mail please check your \"Junk\" folder as well.","FIN_ITEXT":" The first time you log in to Zalaris HR app with username and password, yo
...[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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; 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: 20220616 051014 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: 2328807
dxp-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-cache-control: +86400
sap-isc-etag: C2C0DC5F147F0375E10000000ADC9967
sap-isc-uagent: 0
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://*.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

!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]...
.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.
9,5.9,0,0,0,4.17,10.06.51.51,0,0,1,.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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; 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: 20220616 051011 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/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-cache-control: +86400
sap-isc-etag: 0EE26F8F2C521EDCB684DC6601FF4CB5
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://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

{
  "_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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; 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: 20220616 051010 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/json
content-length: 977
dxp-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-cache-control: +86400
sap-isc-etag: 0EE26F8F2C521EDCB684DC15671A4CB5
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://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

{
  "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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; 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: 20220616 051009 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/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-cache-control: +86400
sap-isc-etag: 0EE26F8F2C521EDCB684DC3DF4B3ECB5
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://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

{
  "_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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; 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: 20220616 051006 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/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-cache-control: +86400
sap-isc-etag: 0EE26F8F2C521EDCB684DCAE2C188CB5
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://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

{
  "sapBrandColor": "#3079BF",
  "sapHighlightColor": "#265f96",
  "sapBaseColor": "#fff",
  "sapShellColor": "#fff",
  "sapBackgroundColor": "#f9f9fd",
  "sapFontFamily": "\"72full\", 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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; 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: 20220616 051007 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/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-cache-control: +86400
sap-isc-etag: 0EE26F8F2C521EDCB684DCAE2C1A0CB5
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://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

{
  "_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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; 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: 20220616 051009 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/json
Content-Length: 6448
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
ms-author-via: DAV
sap-cache-control: +86400
sap-isc-etag: 0EE26F8F2C521EDCB684DCD620878CB5
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://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

{
  "_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=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; 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: 20220616 051008 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/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
ms-author-via: DAV
sap-cache-control: +86400
sap-isc-etag: 0EE26F8F2C521EDCB684DCFE91B28CB5
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://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

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

27. Multiple content types specified

There are 8 instances of this issue:

- /neptune/ZMFP_DASH_ESS_LVREQ_OVERVIEW.view.js
- /neptune/ZMFP_DASH_ESS_NEXT_SALARY.view.js
- /neptune/ZMFP_DASH_ESS_OTHER_QUOTAS.view.js
- /neptune/ZMFP_DASH_ESS_PAID_VACATION.view.js
- /neptune/ZMFP_DASH_ESS_SICKNESS.view.js
- /neptune/ZMFP_DASH_ESS_TIME_REG.view.js
- /neptune/ZMFP_DASH_ESS_TRAVEL_PAID.view.js
- /neptune/ZMFP_DASH_ESS_TRVL_PROCESS.view.js

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)

27.1. https://testportal.zalaris.com/neptune/ZMFP_DASH_ESS_LVREQ_OVERVIEW.view.js

Summary

Severity: **Information**

Confidence: **Certain**

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

Path: **/neptune/ZMFP_DASH_ESS_LVREQ_OVERVIEW.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

Request 1

```
GET /neptune/ZMFP_DASH_ESS_LVREQ_OVERVIEW.view.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:40 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/javascript; charset=utf-8
Content-Length: 1010266
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220329183341
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://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

<!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]...
```

27.2. 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 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

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:40 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/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://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

<!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]...
```

27.3. https://testportal.zalaris.com/neptune/ZMFP_DASH_ESS_OTHER_QUOTAS.view.js

Summary

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

Request 1

```
GET /neptune/ZMFP_DASH_ESS_OTHER_QUOTAS.view.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:40 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/javascript; charset=utf-8
Content-Length: 1009909
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220329190925
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://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

<!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]...
```

27.4. https://testportal.zalaris.com/neptune/ZMFP_DASH_ESS_PAID_VACATION.view.js

Summary

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

Request 1

```
GET /neptune/ZMFP_DASH_ESS_PAID_VACATION.view.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
```

```
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:40 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/javascript; charset=utf-8
Content-Length: 1010521
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220329170542
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://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

<!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]...
```

27.5. https://testportal.zalaris.com/neptune/ZMFP_DASH_ESS_SICKNESS.view.js

Summary

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

Request 1

```
GET /neptune/ZMFP_DASH_ESS_SICKNESS.view.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:41 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/javascript; charset=utf-8
Content-Length: 1007896
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220329170846
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://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

<!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]...
```

27.6. https://testportal.zalaris.com/neptune/ZMFP_DASH_ESS_TIME_REG.view.js

Summary

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

Request 1

```
GET /neptune/ZMFP_DASH_ESS_TIME_REG.view.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:41 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/javascript; charset=utf-8
Content-Length: 1021208
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220329171112
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://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

<!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]...
```

27.7. https://testportal.zalaris.com/neptune/ZMFP_DASH_ESS_TRAVEL_PAID.view.js

Summary

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

Request 1

```
GET /neptune/ZMFP_DASH_ESS_TRAVEL_PAID.view.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:41 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/javascript; charset=utf-8
Content-Length: 1011115
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
```

```
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220329171528
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://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

<!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]...
```

27.8. https://testportal.zalaris.com/neptune/ZMFP_DASH_ESS_TRVL_PROCESS.view.js

Summary

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

Request 1

```
GET /neptune/ZMFP_DASH_ESS_TRVL_PROCESS.view.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:41 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/javascript; charset=utf-8
Content-Length: 1011427
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220329171618
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://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

<!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 3 instances of this issue:

- /com.sap.portal.design.urdesigndata/themes/portal/sap_tradeshow_plus/common/emptyhover.html
- /com.sap.portal.pagebuilder/html/EmptyDocument.html
- /htmlb/jslib/emptyhover.html

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_tradeshow_plus/common/emptyhover.html

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://testportal.zalaris.com**
Path:	**/com.sap.portal.design.urdesigndata/themes/portal/sap_tradeshow_plus/common/emptyhover.html**

Request 1

GET /com.sap.portal.design.urdesigndata/themes/portal/sap_tradeshow_plus/common/emptyhover.html HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE1289120)1289150; sap-webdisp-session=63-28601-AuJVeyp8EXhVmi3aBw1zkw; sap-usercontext=sap-client=650; ai_user=s4SfN06Q9atFoPwQQKB+PL|2022-06-16T03:10:14.013Z; ai_authUser=650-00034448%7C650; CSRF-Session=c6d8c0fe06e202dffb8a093ade331454; ai_session=Y36MblRdOCLc/kjOPX0D/p|1655349014046|1655349919451
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, 16 Jun 2022 03:26:06 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
cache-control: max-age=604800
last-modified: Fri, 10 Jun 2022 05:35:04 GMT
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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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

<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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:31 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
last-modified: Fri, 11 Mar 2022 05:02:11 GMT
cache-control: max-age=604800
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://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
Content-Length: 429
Connection: close

<html>
<head>
  <title>Untitled</title>
<script type="text/javascript">

function relax( input )
{
  if (input.search(/^\\d+\\.\\d+\\.\\d+\\.\\d+$/) >=0 )
  {
    return input;
  }
  var lnD
...[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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 03:30:32 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
last-modified: Tue, 30 Nov 2021 05:06:49 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://* data: blob: https://maps.googleapis.com:443 https://*.hana.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

<html>
<head>
  <title>Untitled</title>
  <link rel="stylesheet" type="text/css" />
</head>
<script language="JavaScript">
// --
...[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 v2021.12.1, at Fri Jun 17 10:24:36 IST 2022.