European
Digital
UniverCity

University of Potsdam
Am Neuen Palais 10
14469 Potsdam
Germany

DELIVERABLE D4.8 – SECURITY AUDIT REPORT

www.educalliance.eu

This Project, EDUC Grant Agreement n.612442 has received funding from the Erasmus + Programme.
This document reflects only the authors' view and the Agency is not responsible for any use that may be made of the information it contains.

Project Acronym	EDUC
Project Full Name	European Digital UniverCity
Grant Agreement No.	612442-EPP-1-2019-1-DE-EPPKA2-EUR-UNIV
Programme	Erasmus +
Instrument	European Universities
Start date of Project	01/10/2019
Duration	36 months
Deliverable No.	D4.8
Document name	Deliverable D4.8 - EDUC Security Audit Report
Work Package	WP4
Associated Task	4.6
Dissemination Level	Restricted (Working group members, EDUC SC + EACEA, Commission services and project reviewers, if requested)
Contractual Submission Date	M36 (September 2022)
Actual Submission Date	February 2023[1]
Main Author	Alexander Kiy
Institution	University of Potsdam
E-mail	giovanni.fonseca@uni-potsdam.de
Abstract	At the end of the project, a security audit by external experts will be done. The goal consists in the analysis of whether data protection measures are meeting required standards.
Keywords	security, audit, certificates, vulnerabilities, CVS, dependencies

[1] For the reasons explained in D4.5, the portal was not available until December 2022, so the security audit by an external auditor was not possible until that date.

Table of contents

This Project, EDUC Grant Agreement n.612442 has received funding from the Erasmus + Programme.
This document reflects only the authors' view and the Agency is not responsible for any use that may be made of the information it contains.

1 Introduction

1.1 Purpose of the document

This security audit of the EDUC infrastructure is the deliverable (D4.8) attached to the EDUC work package 4 (WP4) Task 4.8. This security audit consists of a document and an excel sheet. The main document holds information according to the EDUC IT components. The excel sheet is a risk evaluation. Starting from risk scenarios (description of the damage, description of the vulnerability and the description of the thread) a classification of the amount of damage and the probability of occurrence are derived. The explanation of the existing measures lead to a risk score. This excel sheet is a starting point for collecting and maintaining the technical and organizational measures in form of an organized risk management for the EDUC IT infrastructure.

1.2 Structure of the document

The focus of the document is to go through all relevant components of the current EDUC IT infrastructure:

- IT component 1: Identity & Access Management
- IT component 2: Webpage of the EDUC alliance
- IT component 3: Portal
- IT component 4: Course catalogue of EDUC course offers (virtual and physical)
- IT component 5: Learning Management System

First the validity of the accounts is assessed for the EDUC IT components, which have a user and role management in section 2. In section 3 as far as possible the runtime environments are reviewed. In Section 4 an SSL-Certificate check is performed. Section 5 uses external tools to conduct a security scan of the components. Section 6 does a review of the current development before in section 7 suggestions are proposed.

2 Validity of the accounts

2.1 Virtual machines

On 9th February 2023 the last update of the login accounts for the five virtual machines was checked.

2.2 Access to EDUC infrastructure components

The access to the central EDUC IT infrastructure components was last ensured on 9th February 2023. The check included the following systems, which have an own role and right management system implemented: LMS and Course Catalogue. Only the following people have advanced administration rights:

Person	Position in EDUC	Role EDUC LMS	Role Course Catalogue
Giovanni Fonseca	Pedagogical Engineer UP	Admin, Pedagogical Engineer	Super Admin
Frank-Ringo Gutacker	IT Specialist UP	Admin	None
Gaële Flatley	Pedagogical Engineer UPN	Pedagogical Engineer	Admin
Krisztina Fodorné Dr. Tóth	Pedagogical Engineer Pécs	Pedagogical Engineer	Admin

Kristýna Hutová	Pedagogical Engineer MU	Pedagogical Engineer	Admin
Rozenn Joufflineau	Pedagogical Engineer UR1	Pedagogical Engineer	Admin
Pascal Kienast	IT Student Assistant UP	Pedagogical Engineer	Admin
Krisztián Simon	Pedagogical Engineer Pécs	Pedagogical Engineer	Admin
Fabio Sorrentino	Pedagogical Engineer UNICA	Pedagogical Engineer	Admin
Ádám Tibold	Pedagogical Engineer Pécs	Pedagogical Engineer	Admin
Péter Uherkovich	Developer Pécs	none	Super Admin
Theodora Papageorgiou	Project Manager UPN	none	Admin
Kinga Rippl	Community Manager Pécs	none	Admin
Erin Anna Smith	Summer School Manager MU	none	Admin
Wiebke Giese	Mobility Manager UP	none	Admin
Poree Coline	Porject Manager UPN	none	Admin

3 Validity of the runtime environments

3.1 Docker

The docker compose specification is based on version 3.3, which supports the Docker Engine releases 17.06.0 onward. The current docker engine version is 20.10.23 from the 19th of January 2023. The docker runtime should be up to date to avoid already known and closed CVE' .

3.2 PHP

The PHP runtime version 7.4.14 is from 7th January 2021 and the version 7.4.26 from 18th November 2021. The latest version is 7.4.33 from 3rd November 2022. The version used has some reported CVE. For current use they seem to be not relevant. When using SOAP-Request or XML-Parsing an upgrade to a newer version should be considered.

3.3 Nginx

The Nginx version used seems to be the version 1.18.0 from 21 April 2020. The current version is the mainline version 1.23.3 from 13 December 2022. The Nginx version 1.18.0 allows an HTTP request smuggling attack that can lead to cache poisoning, credential hijacking, or security bypass. The weakness was disclosed 05/14/2020. This vulnerability is handled as CVE-2020-12440 since 04/28/2020.

3.4 SimpleSAML

The PHP dependency used for the SimpleSAMLphp is still up to date. The current stable version is 1.19.7 and is covered by the dependency specification of the composer files: ^1.19.5 or ^1.19.6.

3.5 Moodle

The Moodle version used is Moodle 3.11.6 (Build: 20220314). The current stable release is 4.1 and the last security release 3.11.12 is from 16th January 2023. As listed in section 5.4 an update is recommended due to open high CVEs.

3.6 Ubuntu 18.04

A rough check for necessary security updated for the virtual machines was conducted by executing the following command /usr/lib/update-notifier/apt-check --human-readable
For the following virtual machines security updates are outstanding:

- Virtual Machine I:	7 additional security updates
- Virtual Machine II:	Error possibly to misconfiguration of third-party repository
- Virtual Machine III:	1 additional security updates
- Virtual Machine IV:	3 additional security updates
- Virtual Machine V:	7 additional security updates

It seems all virtual machines have a different patch status and are not centrally maintained or managed. It is recommended to establish automatic jobs for updates or to establish processes and definitions.

4 SSL-Certificate Check

Used SSL Labs[2] for scanning the following four domains:

- Webpage:	educalliance.eu
- Portal:	portal.educalliance.eu
- Course Catalogue:	courses.educalliance.eu
- LMS:	learning.educalliance.eu

SSL Labs gives an overall rating for the domain educalliance.eu a grade **B**. The server configuration supports TLS 1.0 and TLS 1.1 with weak cipher suites. Furthermore, the server currently does not support Forward Secrecy with the reference browsers.

For the domain portal.educalliance.eu the overall rating is also grade **B**. There are some weak cipher suites for TLS 1.2 available. The certificate chain seems to be broken, not all necessary certificates are sent by the server.

SSL Labs give for the domain courses.educalliance.eu also an **A** rating, with the same limitations as for learning.educalliance.eu.

For learning.educalliance.eu SSL Labs gives an overall rating of **A**. Some weak ciphers for TLS 1.2 are currently available. Due to some reason a second invalid certificate for the domain courses.educalliance.eu is available, which is already expired.

The results can be seen in the appendix.

[2] https://www.ssllabs.com/

5 Security scan of EDUC IT components

The scans were conducted with two providers HostedScan[3] and ImmuniWeb[4]. HostedScan supports:

- Nmap TCP Port Scan (range 0 to 65535),
- Nmap UDP Port Scan,
- OpenVAS[5] Network Vulnerability Scan (based on Common Vulnerabilities and Exposures (CVEs))
- OWASP ZAP Passive Web Application Scan (e. g. cross-domain misconfigurations, insecure cookies, vulnerable js dependencies),
- OWASP ZAP Active Web Application Scan (e. g. tests for SQL Injections, remote command execution, XSS) and
- Sslyze TLS/SSL Security Scan (e. g. bad certificates, weak ciphers, Heartbleed, ROBOT).

ImmuniWeb supports the following scans:

- Web Server Security Tests
- GDPR Compliance Tests
- PCI DSS Compliance Tests
- HTTP Header Security
- Content Security Policy Test
- Cookies Privacy and Security Analysis and
- External Content Privacy and Security Analysis.

5.1 Webpage

According to the Nmap TCP port scan the ports 22 (ssh), 80 (http) and 443 (https) are publicly available. No UDP ports are publicly available.

OpenVAS returned for the Webpage 2 high risks (CVSS 7.5, CVSS 7.5), 2 medium risks (CVSS 4.3, CVSS 4.3) and 1 low risk (CVSS 2.6). The high risks are related to vulnerable Cipher Suites for the HTTPS.

The passive and active OWASP Scans resulted in 4 medium and 7 low risks.

The SSLyzer Scans did not indicate any anomalies.

ImmuniWeb gives an overall rating of C for the webpage (scale A-F). Especially the dependencies for vue.js, nuxt.js and core-js are outdated and need an update. Some HTTP Headers seems to be missing or misconfigured and the Content-Security-Header Policy is not set.

5.2 Portal

According to the Nmap TCP port scan the ports 22 (ssh), 80 (http) and 443 (https) are publicly available. No UDP ports are publicly available.

[3] https://hostedscan.com/
[4] https://immuniweb.com/
[5] https://openvas.org/

OpenVAS returned for the Portal 2 medium risks (CVSS 6.4, CVSS 5.0) and 1 low risk (CVSS 2.6). The medium risks are related to missing HTTP-attributes for cookies.

The passive and active OWASP Scans resulted in 2 high, 3 medium and 5 low risks. Especially the two 2 high risks related to Cross Site Scripting should be considered in a future release.

The SSLyzer Scans verifies the finding already indicated in the previous section. The certification chain should be checked.

ImmuniWeb gives an overall rating of C for the webpage (scale A-F). Especially the dependencies for jQuery and Showdown are outdated and need an update. Some HTTP Headers seems to be missing or misconfigured and the Content-Security-Header Policy is not set. Due to misconfiguration some versions (e. g. nginx/1.18.0 (Ubuntu) or PHP/7.4.26) are publicly available and may facilitate further attacks. The site does not meet the EU GDPR compliance tests (e. g. Cookie Protection, Cookie Disclaimer or Privacy Policy).

5.3 Course Catalogue

According to the Nmap TCP port scan the ports 80 (http) and 443 (https) are publicly available. No UDP ports are publicly available.

OpenVAS returned for the Course Catalogue 3 medium risks (CVSS 6.4, CVSS 5.0, CVSS 5.0) and 2 low risk (CVSS 2.6, CVSS 2.1). The medium risks are related to missing HTTP-attributes for cookies. The third risk seems to be related to an expired SSL certificate.

The passive and active OWASP Scans resulted in 2 medium and 6 low risks.

The SSLyzer Scans did not indicate any anomalies.

ImmuniWeb gives an overall rating of C for the webpage (scale A-F). Especially the dependencies for Core-js, Bootstrap and Showdown are outdated and need an update. Some HTTP Headers seems to be missing or misconfigured and the Content-Security-Header Policy is not set. Due to misconfiguration some versions (e. g. nginx/1.18.0 (Ubuntu) or PHP/7.4.26) are publicly available and may facilitate further attacks. The site does not meet the EU GDPR compliance tests (e. g. Cookie Protection, Cookie Disclaimer or Privacy Policy).

5.4 Learning Management System

According to the Nmap TCP port scan the ports 80 (http) and 443 (https) are publicly available. No UDP ports are publicly available.

OpenVAS returned for the Learning Management System 3 medium risks (CVSS 6.4, CVSS 5.0, CVSS 5.0) and 2 low risk (CVSS 2.6, CVSS 2.1). The medium risks are related to missing HTTP-attributes for cookies. The third risk seems to be related to an expired SSL certificate.

The passive and active OWASP Scans resulted in 1 high, 3 medium and 4 low risks.

The SSLyzer Scans did not indicate any anomalies.

ImmuniWeb gives an overall rating of F for the webpage (scale A-F). Moodle with the version 3.11.6 has already 3 high reported CVE risks and several outdated dependencies. Some HTTP Headers seems to be missing or misconfigured and the Content-Security-Header Policy is not set. Due to misconfiguration some versions (e. g. nginx/1.18.0 (Ubuntu) or PHP/7.4.14) are publicly available and may facilitate further attacks.

6 Review of self-developed EDUC IT components

A rough audit of the current stand of the self-developed EDUC IT components allow the conclusion of the necessity to update some dependencies. It would be good to have regular tasks for scanning for dependency updates and to generate automatic pull requests with updated dependencies (cp. section Security in Github for debendabot). The following necessary updates could be identified.

6.1 Webpage (npm audit am 2023/02/04 at 17:43)

For the webpage overall 319 vulnerabilities could be identified. The 28 critical and 190 high vulnerabilities should be fixed on time.

```
$ npm audit
found 319 vulnerabilities (11 low, 90 moderate, 190 high, 28 critical) in 2011 scanned packages
  run `npm audit fix` to fix 254 of them.
  31 vulnerabilities require semver-major dependency updates.
  34 vulnerabilities require manual review. See the full report for details.
```

6.2 Portal

For the Portal 1 security vulnerability could be found. This vulnerability is the same as for the Course Catalogue.

```
$ composer audit
Found 1 security vulnerability advisory affecting 1 package:
+-------------------+----------------------------------------------------------------------------------+
| Package           | symfony/http-kernel                                                              |
| CVE               | CVE-2022-24894                                                                   |
| Title             | CVE-2022-24894: Prevent storing cookie headers in HttpCache                      |
| URL               | https://symfony.com/cve-2022-24894                                               |
| Affected versions | >=2.0.0,<2.1.0|>=2.1.0,<2.2.0|>=2.2.0,<2.3.0|>=2.3.0,<2.4.0|>=2.4.0,<2.5.0|>=2.5 |
|                   | .0,<2.6.0|>=2.6.0,<2.7.0|>=2.7.0,<2.8.0|>=2.8.0,<3.0.0|>=3.0.0,<3.1.0|>=3.1.0,<3 |
|                   | .2.0|>=3.2.0,<3.3.0|>=3.3.0,<3.4.0|>=3.4.0,<4.0.0|>=4.0.0,<4.1.0|>=4.1.0,<4.2.0| |
|                   | >=4.2.0,<4.3.0|>=4.3.0,<4.4.0|>=4.4.0,<4.4.50|>=5.0.0,<5.1.0|>=5.1.0,<5.2.0|>=5. |
|                   | 2.0,<5.3.0|>=5.3.0,<5.4.0|>=5.4.0,<5.4.20|>=6.0.0,<6.0.20|>=6.1.0,<6.1.12|>=6.2. |
|                   | 0,<6.2.6                                                                         |
| Reported at       | 2023-02-01T08:00:00+00:00                                                        |
+-------------------+----------------------------------------------------------------------------------+
```

6.3 Course Catalogue (composer audit 2023/02/04 at 17:45)

The Course Catalogue has 2 security vulnerabilities, one already reported in September 2022. Both should be fixed on time.

```
$ composer audit
Found 2 security vulnerability advisories affecting 2 packages:
+-------------------+----------------------------------------------------------------------------------+
| Package           | symfony/http-kernel                                                              |
| CVE               | CVE-2022-24894                                                                   |
| Title             | CVE-2022-24894: Prevent storing cookie headers in HttpCache                      |
| URL               | https://symfony.com/cve-2022-24894                                               |
| Affected versions | >=2.0.0,<2.1.0|>=2.1.0,<2.2.0|>=2.2.0,<2.3.0|>=2.3.0,<2.4.0|>=2.4.0,<2.5.0|>=2.5 |
|                   | .0,<2.6.0|>=2.6.0,<2.7.0|>=2.7.0,<2.8.0|>=2.8.0,<3.0.0|>=3.0.0,<3.1.0|>=3.1.0,<3 |
|                   | .2.0|>=3.2.0,<3.3.0|>=3.3.0,<3.4.0|>=3.4.0,<4.0.0|>=4.0.0,<4.1.0|>=4.1.0,<4.2.0| |
|                   | >=4.2.0,<4.3.0|>=4.3.0,<4.4.0|>=4.4.0,<4.4.50|>=5.0.0,<5.1.0|>=5.1.0,<5.2.0|>=5. |
|                   | 2.0,<5.3.0|>=5.3.0,<5.4.0|>=5.4.0,<5.4.20|>=6.0.0,<6.0.20|>=6.1.0,<6.1.12|>=6.2. |
|                   | 0,<6.2.6                                                                         |
| Reported at       | 2023-02-01T08:00:00+00:00                                                        |
+-------------------+----------------------------------------------------------------------------------+
+-------------------+----------------------------------------------------------------------------------+
| Package           | twig/twig                                                                        |
| CVE               | CVE-2022-39261                                                                   |
| Title             | Possibility to load a template outside a configured directory when using the fil |
|                   | esystem loader                                                                   |
| URL               | https://symfony.com/blog/twig-security-release-possibility-to-load-a-template-ou |
|                   | tside-a-configured-directory-when-using-the-filesystem-loader                    |
| Affected versions | >=1.0.0,<1.44.7|>=2.0.0,<2.15.3|>=3.0.0,<3.4.3                                   |
| Reported at       | 2022-09-28T10:36:08+00:00                                                        |
+-------------------+----------------------------------------------------------------------------------+
```

7 Suggestion and Conclusion

The synoptic security check suggests that most EDUC IT components are in a good state. As most components are self-developed IT components it must be considered to update the necessary dependencies as soon as possible to prevent security or data leaks. The security vulnerabilities found above, especially the ones ranked high or the security vulnerabilities, should be fixed as soon as possible.

Some EDUC IT components are still not GDPR compliant. At the current state neither for the webpage or the course catalogue the imprint seems to be applicable. Here a critical review should happen.

In the appendix a risk analysis was started. This analysis should be finalized and continuously updated and critically reviewed in the next funding phase and during daily operation. The risk analysis is a valid basis for an organizational risk assessment and management.