RECIPIENT

Esaqa GmbHG
Tiergartenstr. 13, 91247 Vorra, Germany

PSONO

Penetration Testing Report

Analysis report on intrusive cybersecurity activity

Linkspirit Sicurezza Informatica
Viale Venezia 100 – 33100 UD
+39 0432 309 903 – info@linkspirit.it

Document: PSONO2201-T01A.odt (20 dec 2021)
Author: Moreno Versolatto
Class: [ ] Public – [ ] Restricted – [**X**] Confidential

Document notes

Classification and diffusion

The following document is classified as confidential.

Its diffusion by Linkspirit is limited to the following people:

Company	Recipient	Role
esaqa GmbH	Sascha Pfeiffer	CEO
Linkspirit	Andrea Zwirner	Information security strategist
Linkspirit	Moreno Versolatto	Cybersecurity operation manager
Linkspirit	Alessandro Zancani	Penetration tester

Revisions

Data	Rev	Autor	Notes
19 January 2022	T01A	ALZ	Report started
24 January 2022	T01A	MV	Report closed

Index

Introduction

This report contains information about potential vulnerabilities of the psono.com web solution.

Linkspirit recommends that special precautions be taken to protect the confidentiality of this document.

Linkspirit conducted the penetration testing during the period of December 6, 2021 – 10 January 2022.

All testing activities were performed in testing environment.

Scope

The scope of analysis consider the following aspects:

- Web application (unauthenticated users)
- Web application (authenticated users)

Our testing included both unauthenticated as well and authenticated testing. For the purpose of our testing we used only demo provided users.

Any risk assessments have been made in a synthetic way, through the qualitative assessment of the vulnerabilities detected, taking into account of

- complexity (constraints, skills) of their exploitation;
- potential impact, on a technical and business level.

The results are classified as follow:

- 0 – [INFO]
- 1 – [LOW]
- 2 – [MODERATE]
- 3 – [MODERATE] / [HIGH]
- 4 – [HIGH]
- 5 – [VERY HIGH]

It should be noted that the risk values resulting from the analysis are affected by the limited visibility of the value of the assets at a corporate strategic level and therefore must be considered as indicative.

Vulnerabilities detected

This section report the vulnerabilities detected and the relative risk level calculated on the basis of the method described up to now.

None of the vulnerabilities identified are critical, however, it is not excluded that a motivated attacker can exploit these vulnerabilities to carry out targeted attacks.

For each vulnerability refer to appendix A in which all affected pages are indicated.

RP.1 – CSP: Wildcard Directive

Affected Asset: psono.com

Risk Level : [INFO]

Description

The vulnerability is present on multiple pages.

The wild card "*" inside the CSP header at the * .s3.amazonaws.com * .digitaloceanspaces.com domains, can allow communication, loading and execution of scripts from these domains. This configuration in case of an XSS or other type attack can allow the loading of malicious payloads, rendering the CSP ineffective.

The low risk is given by a low chance of being able to exploit this vulnerability via XSS, since no injection points have been detected

Potential impact

It is very easy to register a subdomain in .amazonaws.com .digitaloceanspaces.com.

In the context of a complex attack and exploiting other vulnerabilities that may be present in the system, but currently not detected, this could present a possible fattening point for the execution of malicious scripts, evading the CSP.

Mitigation and corrective action

Mitigation: --

Corrective action: Configure the specific CSP according to the context. If you trust all of the subdomains of this domain there is no impact.

RP.2 – CSP: style-src unsafe-inline

Affected Asset: -

Risk Level : [LOW]

Description

If an attacker manages to compromise the site by injecting code, this vulnerability could lead to XSS attacks, ranging from simply changing the style of the page to replacing some elements in it and sending information to external domains, made possible by the vulnerability to point RP.1.

However, having not found any injection points, the probability of this attack remains remote with a low risk level.

Potential impact

Complex XSS attack, information leakage.

Mitigation and corrective action

Mitigation: --

Corrective action: when possible do not allow inline style-src in CSP

RP.3 – Incomplete or No Cache-control Header Set

Affected Asset: -

Risk Level : [LOW]

Description

The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content.

Potential impact

Given the lack of the cache-control header, browsers could store the content of the page visited, thus also recording user and session information. This could allow the use of this information by a compromised browser or by users accessing the same browser. There does not seem to be any evidence of actually being able to compromise passwords, in any case we recommend a further verification and use of this header where possible-

Mitigation and corrective action

Mitigation: --

Corrective action: Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate.

RP.4 – Lack of CSFR tokens

The lack of CSFR tokens is also reported in some pages that use forms, from what has been verified the forms should not display relevant information, and auto-completion is in any case disabled, an additional check on your part is recommended. See the appendix for the list of affected pages.

Final notes

The application is well structured and with a high degree of security, fixing the reported vulnerabilities even if not significant can lead to a general increase in security.

Security vulnerabilities can exist in the OSS (open source software) libraries that we import as much as in the code we write and therefore it is necessary that the guidelines, tests and checks (including automated) of the code are an integral part in the development of the application. It is also important that these libraries are periodically updated.

In general, it is recommended to put in place a remediation and patch management strategy and also to keep the security of the infrastructure monitored through timed vulnerability assessments.

Nothing to report about the infrastructure.

Please note that as technologies and risks change over time, the vulnerabilities associated with the operation of systems described in this report, as well as the actions necessary to reduce the exposure to such vulnerabilities, will also change. This is the first time we have found such a low number of vulnerabilities and low severity, congratulations from the Linkspirit team.

Appendix A (Affected pages)

RP.1 – CSP: Wildcard Directive

- GET: https://pen.psono.com/
- GET: https://pen.psono.com/activate.html
- GET: https://pen.psono.com/css
- GET: https://pen.psono.com/css/lib
- GET: https://pen.psono.com/download-file.html
- GET: https://pen.psono.com/enforce-two-fa.html
- GET: https://pen.psono.com/fonts
- GET: https://pen.psono.com/img
- GET: https://pen.psono.com/index.html
- GET: https://pen.psono.com/js
- GET: https://pen.psono.com/js/lib
- GET: https://pen.psono.com/link-share-access.html
- GET: https://pen.psono.com/lost-password.html
- GET: https://pen.psono.com/open-secret.html
- GET: https://pen.psono.com/popup_pgp.html
- GET: https://pen.psono.com/privacy-policy-content.html
- GET: https://pen.psono.com/privacy-policy.html
- GET: https://pen.psono.com/register.html
- GET: https://pen.psono.com/server/authentication/activate-token
- GET: https://pen.psono.com/server/authentication/login
- GET: https://pen.psono.com/server/datastore
- GET: https://pen.psono.com/server/group
- GET: https://pen.psono.com/server/group/rights
- GET: https://pen.psono.com/server/info
- GET: https://pen.psono.com/server/link-share
- GET: https://pen.psono.com/server/secret
- GET: https://pen.psono.com/server/share

- GET: https://pen.psono.com/server/share/right
- GET: https://pen.psono.com/server/user/status
- GET: https://pen.psono.com/translations
- GET: https://pen.psono.com/view

RP.2 – CSP: style-src unsafe-inline

- GET: https://pen.psono.com/
- GET: https://pen.psono.com/activate.html
- GET: https://pen.psono.com/css
- GET: https://pen.psono.com/css/lib
- GET: https://pen.psono.com/download-file.html
- GET: https://pen.psono.com/enforce-two-fa.html
- GET: https://pen.psono.com/fonts
- GET: https://pen.psono.com/img
- GET: https://pen.psono.com/index.html
- GET: https://pen.psono.com/js
- GET: https://pen.psono.com/js/lib
- GET: https://pen.psono.com/link-share-access.html
- GET: https://pen.psono.com/lost-password.html
- GET: https://pen.psono.com/open-secret.html
- GET: https://pen.psono.com/popup_pgp.html
- GET: https://pen.psono.com/privacy-policy-content.html
- GET: https://pen.psono.com/privacy-policy.html
- GET: https://pen.psono.com/register.html
- GET: https://pen.psono.com/server/authentication/activate-token
- GET: https://pen.psono.com/server/authentication/login
- GET: https://pen.psono.com/server/datastore
- GET: https://pen.psono.com/server/group
- GET: https://pen.psono.com/server/group/rights
- GET: https://pen.psono.com/server/info
- GET: https://pen.psono.com/server/link-share
- GET: https://pen.psono.com/server/secret
- GET: https://pen.psono.com/server/share
- GET: https://pen.psono.com/server/share/right

- GET: https://pen.psono.com/server/user/status
- GET: https://pen.psono.com/translations
- GET: https://pen.psono.com/view

RP3 - Incomplete or No Cache-control Header Set

- GET: https://pen.psono.com/activate.html
- GET: https://pen.psono.com/
- GET: https://pen.psono.com/config.json
- GET: https://pen.psono.com/download-file.html
- GET: https://pen.psono.com/enforce-two-fa.html
- GET: https://pen.psono.com/img/browserconfig.xml
- GET: https://pen.psono.com/index.html
- GET: https://pen.psono.com/link-share-access.html
- GET: https://pen.psono.com/link-share-access.html?passphrase=
- GET: https://pen.psono.com/lost-password.html
- GET: https://pen.psono.com/open-secret.html
- GET: https://pen.psono.com/popup_pgp.html
- GET: https://pen.psono.com/privacy-policy-content.html
- GET: https://pen.psono.com/privacy-policy.html
- GET: https://pen.psono.com/register.html
- GET: https://pen.psono.com/search.xml
- GET: https://pen.psono.com/server/datastore/
- GET: https://pen.psono.com/server/group/
- GET: https://pen.psono.com/server/info/
- GET: https://pen.psono.com/server/link-share/
- GET: https://pen.psono.com/server/share/right/
- GET: https://pen.psono.com/server/user/status/
- GET: https://pen.psono.com/translations/datatables.*.json
- GET: https://pen.psono.com/translations/locale-*.json
- GET: https://pen.psono.com/VERSION.txt
- POST: https://pen.psono.com/server/authentication/activate-token/
- POST: https://pen.psono.com/server/authentication/login/
- POST: https://pen.psono.com/server/datastore/
- POST: https://pen.psono.com/server/user/search/

RP.4 – Lack of CSFR token

- GET: https://pen.psono.com/
- GET: https://pen.psono.com/activate.html
- GET: https://pen.psono.com/enforce-two-fa.html
- GET: https://pen.psono.com/index.html
- GET: https://pen.psono.com/link-share-access.html
- GET: https://pen.psono.com/popup_pgp.html
- GET: https://pen.psono.com/view/templates.js