Penetration Test Report
Psono web application

for

esaqa GmbH

Trovent Security GmbH
Lise-Meitner-Allee 4 | 44801 Bochum

Revision 2
2023-03-06
Classification: public

Contents

1 Introduction

Trovent Security GmbH conducted a penetration test on the Psono web application Enterprise Edition of esaqa GmbH between 2022-12-06 and 2022-12-12.

The assessment was performed by Karima Hebbal, Sergey Makarov and Gianmarco Wahrig. Our contact on side of esaqa GmbH was Sascha Pfeiffer.

The purpose of this document is to describe the scope and the methodology of the penetration test, to provide details about the findings and to give recommendations to esaqa GmbH.

2 Executive summary

2.1 Penetration test result

Trovent Security GmbH tested the **Psono web application** Enterprise Edition of esaqa GmbH. The penetration test was performed in a combination of automated and manual testing.

The **Psono web application** was checked for typical web application security weaknesses like the following:

- SQL injection
- Broken authentication
- Broken access control
- Sensitive data exposure
- Cross-site-scripting (XSS)
- File inclusion
- Insecure direct object references (IDOR)
- Cross-site request forgery (CSRF)

More information is available in the OWASP Web Security Testing Guide.[1]

During the penetration test of the **Psono web application** Trovent Security GmbH found two security vulnerabilities. These vulnerabilities are not related to those mentioned above. Both vulnerabilities affect the configuration of the web application or the web server.

The estimated risk of one vulnerability was rated MEDIUM and the risk of one vulnerability was rated NONE.

No vulnerabilities were found in the Psono web application itself.

[1] https://owasp.org/www-project-web-security-testing-guide/stable/

The vulnerability that is rated as MEDIUM is:

- **Weak password policy** (TRPT-2212-PSONO-001)

The vulnerability TRPT-2212-PSONO-001 carries the risk that application users set a weak password that is easy to guess by possible attackers.

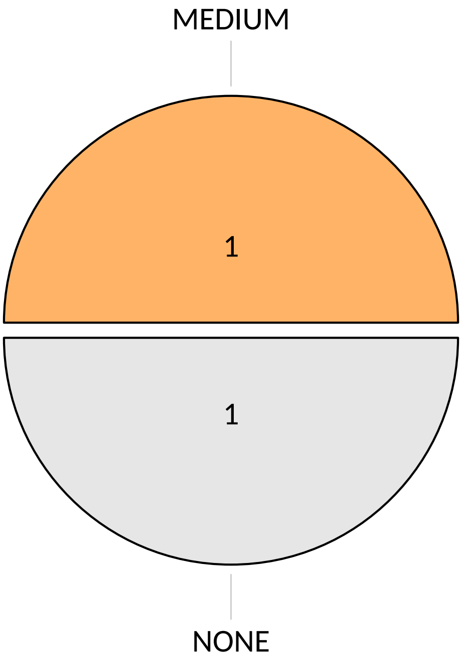


Figure 1: All findings by estimated risk rating

2.2 Findings overview table

Chapter	Trovent vulnerability ID	Technical severity	Estimated risk
5.1	TRPT-2212-PSONO-001	MEDIUM	MEDIUM
5.2	TRPT-2212-PSONO-002	INFORMATIONAL	NONE

2.3 Conclusion and recommendations

Looking at the results of the penetration test, we conclude that the security of the web application is at an acceptable level.

No vulnerabilities with CRITICAL or HIGH risk ratings were found. The remaining vulnerabilities should be mitigated by setting more secure default values in the configuration.

We advise to remediate all findings of this penetration test.

Furthermore we recommend security testing at regular intervals as new attacks are developed and vulnerabilities in software components are published. We consider a cycle of 6 months to be regular.

3 Scope

The test setup was hosted on an internal server where multiple Docker containers for the application were used.

The following Docker containers were deployed for the penetration test:

- psono/psono-server-enterprise:3.1.5
- psono/psono-client:2.1.0
- psono/psono-admin-client:1.6.4
- psono/psono-fileserver:1.0.5
- psono/psono-postgres:latest (PostgreSQL 9.6.2)
- psono-proxy (nginx 1.21.4)

The user accounts for the web application were self-registered.

4 Methodology

This chapter explains the rating methodology used by Trovent Security GmbH.

4.1 Severity and risk rating

All findings that are discovered during a penetration test are evaluated and categorized.

The **Technical severity rating** is based on the Common Vulnerability Scoring System (CVSS) score of the vulnerability. The CVSS score ranges between 0.0 and 10.0.

CVSS score	Technical severity rating
9.0 - 10.0	CRITICAL
7.0 - 8.9	HIGH
4.0 - 6.9	MEDIUM
0.1 - 3.9	LOW
0.0	INFORMATIONAL

See also the CVSS specification document. [2]

The **CVSS vector string** represents the values of each CVSS base metric. [3]

The following CVSS metrics are used to calculate the final CVSS score:

- Attack Vector (AV)
- Attack Complexity (AC)
- Privileges Required (PR)
- User Interaction (UI)
- Scope (S)
- Confidentiality (C)
- Integrity (I)
- Availability (A)

[2] https://www.first.org/cvss/v3.1/specification-document#Qualitative-Severity-Rating-Scale

[3] https://www.first.org/cvss/v3.1/specification-document#Base-Metrics

The **Likelihood of exploitation rating** depends on the probability that a vulnerability is exploited. This rating is subjective to a certain degree.

Likelihood of exploitation rating	Description
HIGH	High probability of being exploited (e.g. system is reachable publicly on the Internet or ready-to-use exploit exists, easy for any attacker)
MEDIUM	Exploitation is likely to happen (e.g. system is reachable within an enterprise network, some experience is needed to exploit the vulnerability)
LOW	Low probability of being exploited (e.g. system is only reachable from defined internal hosts or attacker has to be very skilled)

The following table shows the **Estimated risk rating** that is based on the technical severity rating and the likelihood of exploitation rating.

	Likelihood of exploitation		
Technical severity	LOW	MEDIUM	HIGH
CRITICAL	HIGH	CRITICAL	CRITICAL
HIGH	MEDIUM	HIGH	CRITICAL
MEDIUM	LOW	MEDIUM	HIGH
LOW	LOW	LOW	MEDIUM
INFORMATIONAL	NONE	NONE	NONE

The **Estimated risk rating** is a better indicator which vulnerabilities should be handled with priority.

Findings are also categorized by type. Trovent Security GmbH uses **Common Weakness Enumeration (CWE)** to perform this task. More information and a list of all known CWE IDs can be found here: https://cwe.mitre.org

5 Findings

5.1 Weak password policy

Trovent vulnerability ID: **TRPT-2212-PSONO-001**

Technical severity and risk rating

CWE	CVSS v3.1 vector string	CVSS v3.1 base score
521	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	5.3

Technical severity	MEDIUM
Likelihood of exploitation	MEDIUM
Estimated risk	MEDIUM

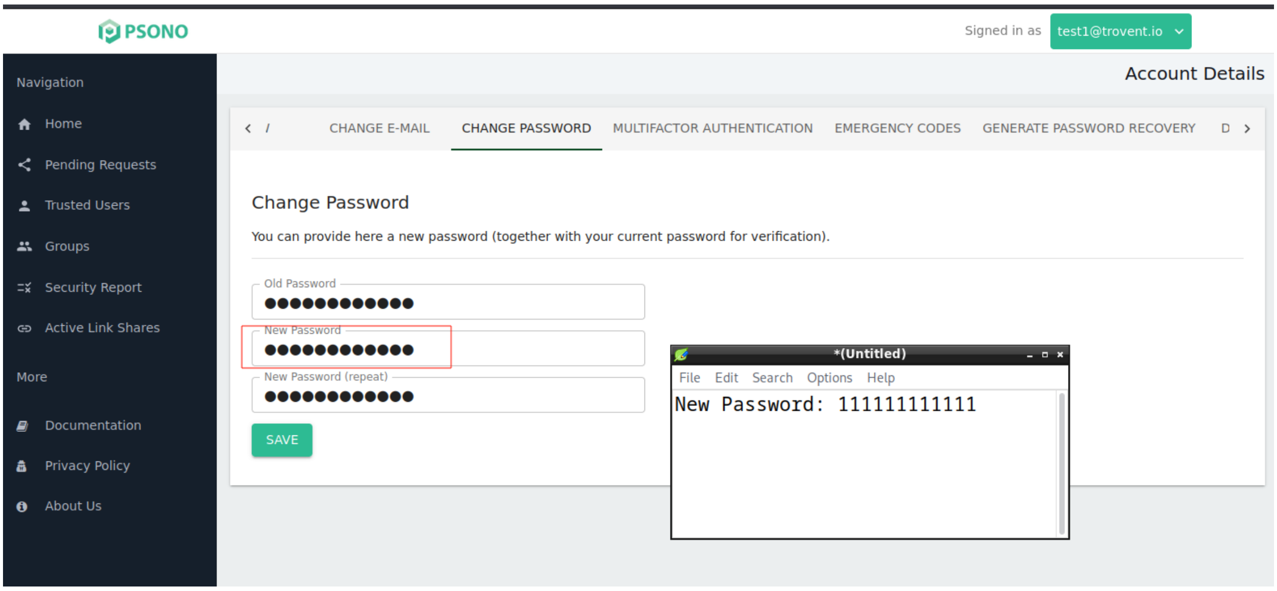
5.1.1 Description

When performing a password change, the Psono web application allows setting a weak user password like **111111111111**. While the configured default minimum password length is 12, there are no complexity requirements by default.

A possible attacker is able to guess weak passwords of user accounts with ease.

5.1.2 Proof of concept

The Psono web application allows setting a simple password that consists of 12 digits.



Change Password

You can provide here a new password (together with your current password for verification).

Old Password: ●●●●●●●●●●●●

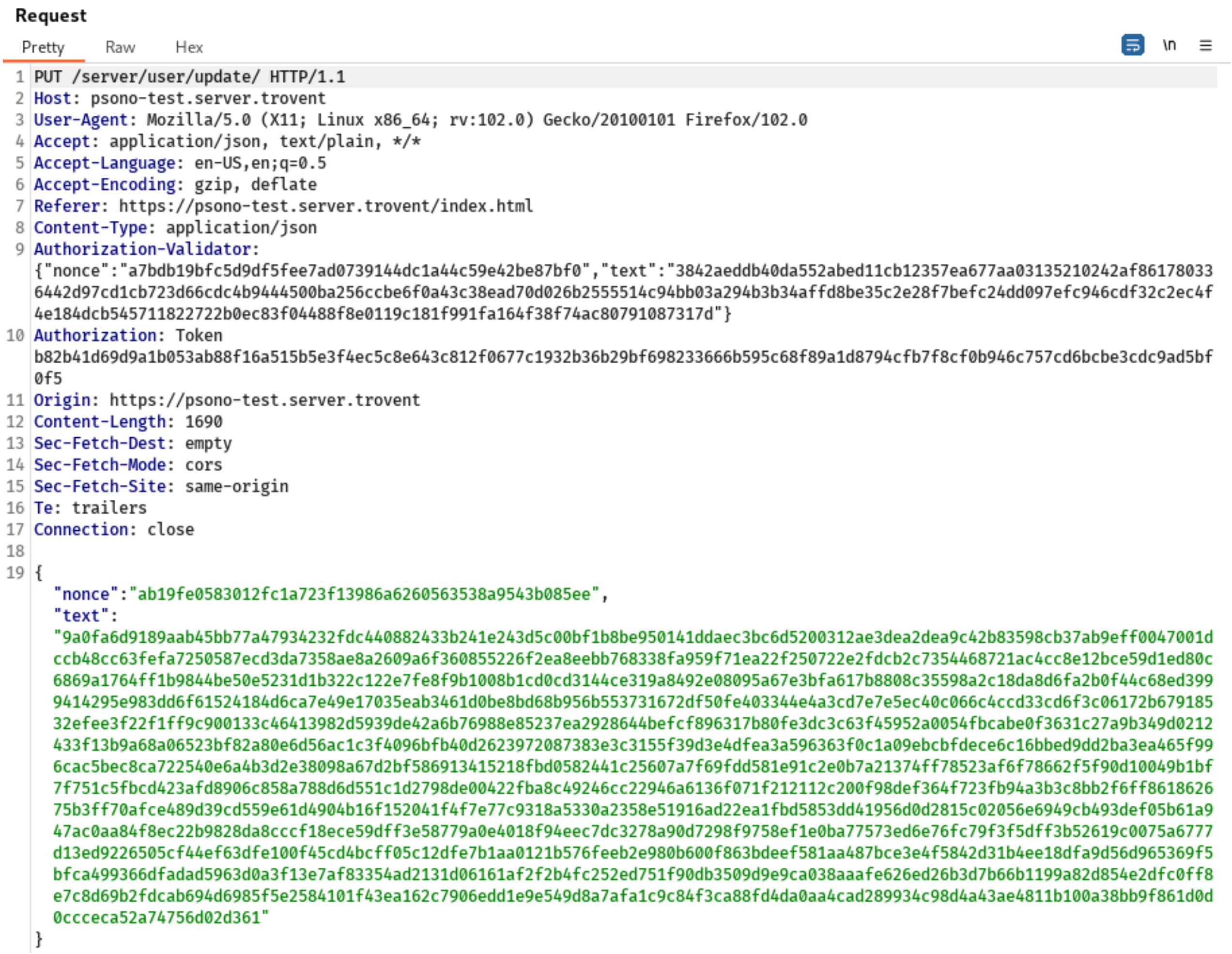
New Password: ●●●●●●●●●●●●

New Password (repeat): ●●●●●●●●●●●●

```
New Password: 111111111111
```

Figure 2: Setting the weak password **111111111111**

The Hypertext Transfer Protocol (HTTP) request shows that the new password is encrypted in the JavaScript client application before it is sent to the server.



```
PUT /server/user/update/ HTTP/1.1
Host: psono-test.server.trovent
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://psono-test.server.trovent/index.html
Content-Type: application/json
Authorization-Validator:
{"nonce":"a7bdb19bfc5d9df5fee7ad0739144dc1a44c59e42be87bf0","text":"3842aeddb40da552abed11cb12357ea677aa03135210242af86178033
6442d97cd1cb723d66cdc4b9444500ba256ccbe6f0a43c38ead70d026b2555514c94bb03a294b3b34affd8be35c2e28f7befc24dd097efc946cdf32c2ec4f
4e184dcb545711822722b0ec83f04488f8e0119c181f991fa164f38f74ac80791087317d"}
Authorization: Token
b82b41d69d9a1b053ab88f16a515b5e3f4ec5c8e643c812f0677c1932b36b29bf698233666b595c68f89a1d8794cfb7f8cf0b946c757cd6bcbe3cdc9ad5bf
0f5
Origin: https://psono-test.server.trovent
Content-Length: 1690
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{
  "nonce":"ab19fe0583012fc1a723f13986a6260563538a9543b085ee",
  "text":
  "9a0fa6d9189aab45bb77a47934232fdc440882433b241e243d5c00bf1b8be950141ddaec3bc6d5200312ae3dea2dea9c42b83598cb37ab9eff0047001d
  ccb48cc63fefa7250587ecd3da7358ae8a2609a6f360855226f2ea8eebb768338fa959f71ea22f250722e2fdcb2c7354468721ac4cc8e12bce59d1ed80c
  6869a1764ff1b9844be50e5231d1b322c122e7fe8f9b1008b1cd0cd3144ce319a8492e08095a67e3bfa617b8808c35598a2c18da8d6fa2b0f44c68ed399
  9414295e983dd6f61524184d6ca7e49e17035eab3461d0be8bd68b956b553731672df50fe403344e4a3cd7e7e5ec40c066c4ccd33cd6f3c06172b679185
  32efee3f22f1ff9c900133c46413982d5939de42a6b76988e85237ea2928644befcf896317b80fe3dc3c63f45952a0054fbcabe0f3631c27a9b349d0212
  433f13b9a68a06523bf82a80e6d56ac1c3f4096bfb40d2623972087383e3c3155f39d3e4dfea3a596363f0c1a09ebcbfdece6c16bbed9dd2ba3ea465f99
  6cac5bec8ca722540e6a4b3d2e38098a67d2bf586913415218fbd0582441c25607a7f69fdd581e91c2e0b7a21374ff78523af6f78662f5f90d10049b1bf
  7f751c5fbcd423afd8906c858a788d6d551c1d2798de00422fba8c49246cc22946a6136f071f212112c200f98def364f723fb94a3b3c8bb2f6ff8618626
  75b3ff70afce489d39cd559e61d4904b16f152041f4f7e77c9318a5330a2358e51916ad22ea1fbd5853dd41956d0d2815c02056e6949cb493def05b61a9
  47ac0aa84f8ec22b9828da8cccf18ece59dff3e58779a0e4018f94eec7dc3278a90d7298f9758ef1e0ba77573ed6e76fc79f3f5dff3b52619c0075a6777
  d13ed9226505cf44ef63dfe100f45cd4bcff05c12dfe7b1aa0121b576feeb2e980b600f863bdeef581aa487bce3e4f5842d31b4ee18dfa9d56d965369f5
  bfca499366dfadad5963d0a3f13e7af83354ad2131d06161af2f2b4fc252ed751f90db3509d9e9ca038aaafe626ed26b3d7b66b1199a82d854e2dfc0ff8
  e7c8d69b2fdcab694d6985f5e2584101f43ea162c7906edd1e9e549d8a7afa1c9c84f3ca88fd4da0aa4cad289934c98d4a43ae4811b100a38bb9f861d0d
  0ccceca52a74756d02d361"
}
```

Figure 3: HTTP request when changing the password

5.1.3 Recommendation

We recommend to set a sane default configuration for password complexity. The configuration parameter **COMPLIANCE_MIN_MASTER_PASSWORD_COMPLEXITY** has to be configured in **settings.yml** according to the documentation.

More information:
https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html#implement-proper-password-strength-controls
https://doc.psono.com/admin/configuration/compliance-settings.html#enforce-minimum-password-complexity

5.2 Missing HTTP security header

Trovent vulnerability ID: **TRPT-2212-PSONO-002**

Technical severity and risk rating

CWE	CVSS v3.1 vector string	CVSS v3.1 base score
1349	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:N	0.0

Technical severity	INFORMATIONAL
Likelihood of exploitation	NONE
Estimated risk	NONE

5.2.1 Description

In the default demo configuration the Psono web application does not send the HTTP security header **Strict-Transport-Security**.

The HTTP header **Strict-Transport-Security** forces the browser to connect with Transport Layer Security (TLS) to the web server.

Note: The setup was done with the installation script from the **psono-quickstart** repository[4]. The script function **build_psono_proxy_configuration ()**[5] creates the Nginx proxy configuration file. The configuration line with the HTTP header **Strict-Transport-Security** is commented out.

As the documentation (**README.md**) clearly states the installation script is not meant for production use, we rate this finding as INFORMATIONAL.

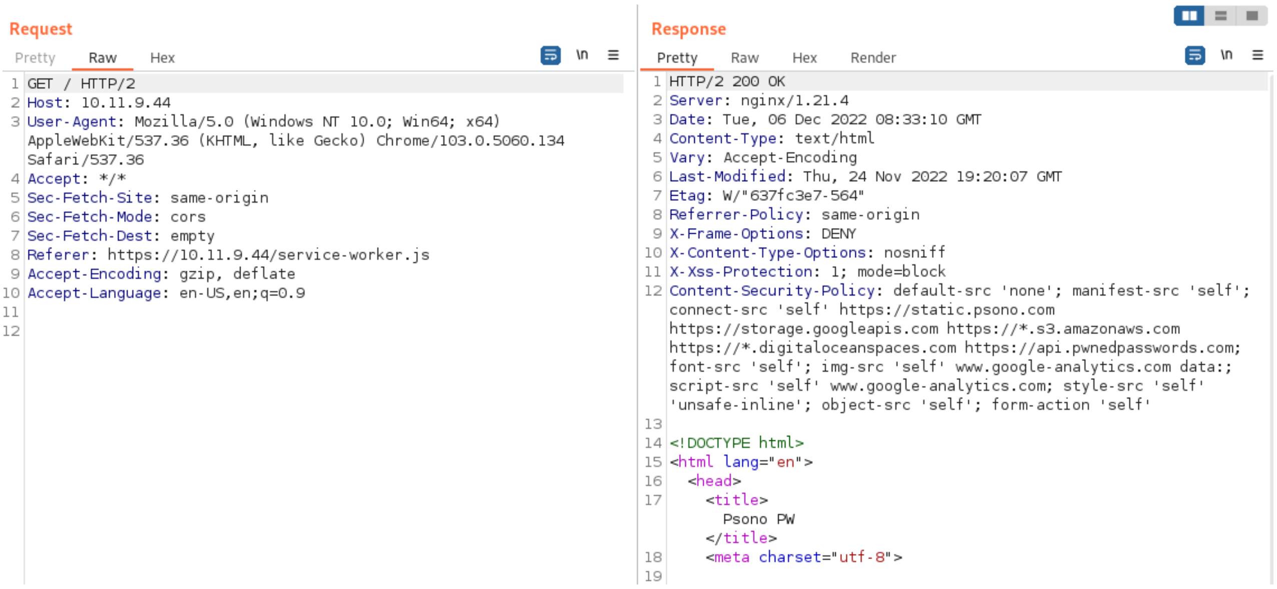
[4] https://gitlab.com/psono/psono-quickstart/-/tree/08545bbfd22667822b23f0f5f6e38e719d566e79

[5] https://gitlab.com/psono/psono-quickstart/-/blob/08545bbfd22667822b23f0f5f6e38e719d566e79/install.sh#L826

5.2.2 Proof of concept

Excerpt from **install.sh** (git commit `08545bbfd22667822b23f0f5f6e38e719d566e79`)

```
build_psono_proxy_configuration () {
    echo "Build psono proxy configuration"
    cat > ~/psono/psono_nginx.conf <<- "EOF"
worker_processes 1;

events { worker_connections 1024; }

http {

    sendfile on;

    server {
        listen 80;
        server_name _;
        return 301 https://$host$request_uri;
    }

    server {
        listen 443 ssl http2;

        ssl_protocols TLSv1.2 TLSv1.3;
        ssl_dhparam /etc/ssl/dhparam.pem;
        ssl_prefer_server_ciphers on;
        ssl_session_cache shared:SSL:10m;
        ssl_session_tickets off;
        ssl_stapling on;
        ssl_stapling_verify on;
        ssl_session_timeout 1d;
        resolver 8.8.8.8 8.8.4.4 valid=300s;
        resolver_timeout 5s;
        ssl_ciphers 'ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-

        # add_header Strict-Transport-Security "max-age=63072000; includeSubdomains; preload";

        add_header Referrer-Policy same-origin;
        add_header X-Frame-Options DENY;
        add_header X-Content-Type-Options nosniff;
        add_header X-XSS-Protection "1; mode=block";
        add_header Content-Security-Policy "default-src 'none'; manifest-src 'self'; connect-src 'self' https://static.psono.com https://storage.googleapis.com https://*.s3.amazonaws.com https://*.digitaloceanspaces.com https://api.pwnedpasswords.com; font-src 'self'; img-src 'self' www.google-analytics.com data:; script-src 'self' www.google-analytics.com; style-src 'self' 'unsafe-inline'; object-src 'self'; form-action 'self'";

        ssl_certificate /etc/ssl/public.crt;
        ssl_certificate_key /etc/ssl/private.key;
```



```
GET / HTTP/2
Host: 10.11.9.44
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134
Safari/537.36
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://10.11.9.44/service-worker.js
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9


```

```
HTTP/2 200 OK
Server: nginx/1.21.4
Date: Tue, 06 Dec 2022 08:33:10 GMT
Content-Type: text/html
Vary: Accept-Encoding
Last-Modified: Thu, 24 Nov 2022 19:20:07 GMT
Etag: W/"637fc3e7-564"
Referrer-Policy: same-origin
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Content-Security-Policy: default-src 'none'; manifest-src 'self';
connect-src 'self' https://static.psono.com
https://storage.googleapis.com https://*.s3.amazonaws.com
https://*.digitaloceanspaces.com https://api.pwnedpasswords.com;
font-src 'self'; img-src 'self' www.google-analytics.com data:;
script-src 'self' www.google-analytics.com; style-src 'self'
'unsafe-inline'; object-src 'self'; form-action 'self'

<!DOCTYPE html>
<html lang="en">
  <head>
    <title>
      Psono PW
    </title>
    <meta charset="utf-8">

```

Figure 4: HTTP response without Strict-Transport-Security header

5.2.3 Recommendation

We recommend to implement the HTTP security header **Strict-Transport-Security** to increase the security level of the demo configuration.

More information:

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security

6 About Trovent

Trovent Security GmbH is a provider of cyber security solutions and services headquartered in Bochum (Germany). We have a cross-industry focus and our international team comprises a wide range of skill sets:

- Penetration testing
- Security and network operations
- Cyber security consultancy
- Certified IT / information security auditors
- Software development
- Data science

Our tried and tested service solutions, which can be flexibly adapted to an individual organisation's specific requirements, are seamlessly integrated into existing IT infrastructure and processes.

Trovent delivers solutions for real-world problems.

We understand the challenges that IT / cyber security organisations are confronted with on a daily basis, and our core objective is to support our customers in overcoming these challenges:

- Alarm flood – countless "events" originating from a wide range of systems. Which ones are relevant? Who has the capacity and skills to do something about it?
- Preoccupied with day-to-day operations – lack of time and resources to focus on improvement of IT security processes and underlying infrastructure.
- Reactive mode of operation – react to changing circumstances or full-blown crises as events unfold, instead of having clear strategies and response plans in place beforehand.
- Lack of visibility in IT infrastructure – no visibility of network traffic flows, no aggregrated views and analysis of logfile data and no comprehensive understanding of the organisation's attack surface.

Working for our customers, we deliver real, tangible value.

- Service-oriented solutions to facilitate rapid deployment and cyber resilience improvement.
- Skilled professionals for introduction of new security operations processes or detection capabilities.
- Minimised additional cost of building (new) internal team and/or infrastructure.
- Objective insight – assessment of cyber security maturity and risk profile of IT infrastructure.
- Productivity improvement – focus on truly actionable events, avoiding flood of log data and events/alarms.
- Leverage existing infrastructure and data sources.
- Full transparency – automation where possible or necessary, but no analytical results driven by cyber security "black boxes".

7 Changelog

Date	Revision	Changes	Author
2023-03-02	1	Create initial report	K. Hebbal, S. Makarov, S. Pietsch
2023-03-06	2	QA	M. Katmann, T. Nieberg

A Appendix

A.1 Acronyms

CVSS Common Vulnerability Scoring System

CWE Common Weakness Enumeration

HTTP Hypertext Transfer Protocol

TLS Transport Layer Security

A.2 CWE - Common Weakness Enumeration

CWE ID	Title
521	Weak Password Requirements
1349	OWASP Top Ten 2021 Category A05:2021 - Security Misconfiguration