INFOSENTRY

Advisory Report

Pro Backup

Web Application Pentest - Pro Backup app

Advisory report for

Web Application Pentest - Pro Backup app

The Security Factory was tasked to perform a technical web application penetration test to provide Pro Backup with a clear view of how resilient Pro Backup is against a cyber-attack.

Name and registration no service provider: Infosentry NV - DV.A110056
Advisory report: Pro Backup needs advisory for Web Application Pentest - Pro Backup app.
Project no. KMOP: 2025KMO133947
Date Report: 17/12/2025

Assessment team: Krystian Dunikowski
Quality assurance: Jorden Deserrano
Subcontractor: the Security Factory

Target audience: This document is mainly intended for technical personnel involved in the remediation of the reported vulnerabilities.

Table of Contents

Project details

Analysis of the problem definition of Pro Backup

Pro Backup wants to get an understanding of and expert advisory on the security posture of its environment. Infosentry and its subcontractor The Security Factory were tasked with performing a number of vulnerability assessments on the environment of Pro Backup to give advice on the security posture and implementation plan. The purpose of this assessment was to verify the effectiveness of the security controls put in place by Pro Backup to secure business-critical information, and the extent to which an attacker can compromise systems and information should these controls fail.
This report represents the findings from the assessment and the associated remediation recommendations/implementation plan to help Pro Backup strengthen its security posture.

Scope

Start Date: 09/12/2025
End Date: 12/12/2025

Assets:

Asset	Type
API: https://api-staging.probackup.io [https://api-staging.probackup.io]	Web Application
Dev dashboard: https://api-staging.probackup.io/maintenance/v1/dashboard [https://api-staging.probackup.io/maintenance/v1/dashboard]	Web Application
Frontend: https://app-staging.probackup.io [https://app-staging.probackup.io]	Web Application

Performed from: 81.82.219.230 (the Security Factory HQ)
Accounts:

- pb.tsf.2025@gmail.com
- pb.tsf.2@gmail.com
- pentest1@thesecurityfactory.be (separately created account)
- tim.truyens@thesecurityfactory.be (separately created account)

Retest 09/01/2026:

Vulnerability	Status
No HTTP strict transport security header	Fixed
Vertical privilege escalation	Fixed

Not in Scope

The following items were not in scope during this security test:

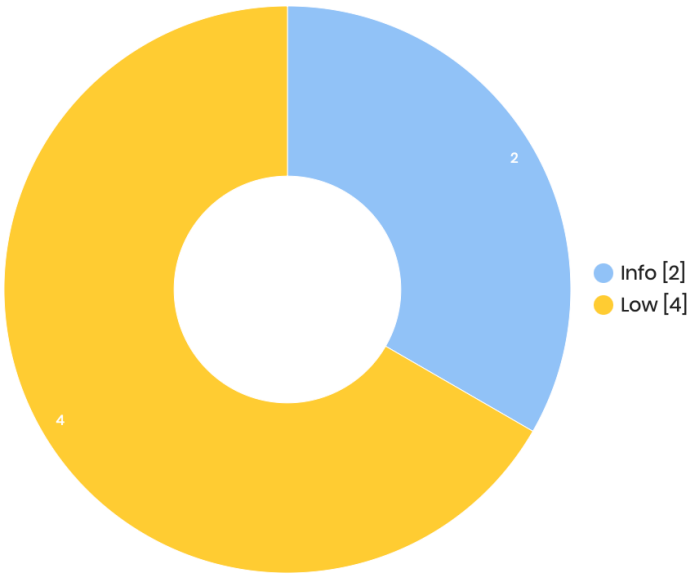
- Denial of Service or any other destructive techniques
- Functional testing

- Introduction of new vulnerabilities without the explicit permission of the customer

Advices

General findings

The testers of the Security Factory validated the application, where applicable, against an extensive list of more than 200 vulnerabilities. This list covers the OWASP Top 10 and many more vulnerabilities categorized within weak passwords, missing OS patches, outdated software, human errors, misconfiguration, incorrect use, vulnerable software, malware, excessive permissions, design flaws, legacy, and many more.



Observations

This section documents our positive and negative observations made during the infrastructure testing phase. This section serves as a keystone for defining the final security posture of the network.

Under "Positive observations" we highlight aspects that performed significantly better or were exceptionally good compared to other internal infrastructures typically tested by our team. On the other hand, "Negative observations" indicate areas where there is room for improvement, indicating the most significant risks currently present within your internal network.

Positive Observations

- No critical or high rated issues were found during the test.
- No IDOR or XSS vulnerabilites were found during the test.

Significant Issues

- The sessions aren't correctly managed.
- The session token is stored in local storage

Overall Security Posture

Comparing the security posture of the application tested at Pro Backup with our experience in the market, we rate this application as currently having a **High** security posture.

High Security Posture