



Ethical Hacking Services – www.vaadata.com

Security Audit Report

SEMANA

Blackbox pentest report

January 2023

CONFIDENTIAL – DO NOT SHARE

Renaud CAYOL
31 January 2023
Version 1.0
15 pages

Client: SEMANA

1 Scope

This document has been created following the security audit performed on the targets listed below:

- app.semana.io

2 Contacts

Company	Contact
SEMANA	Nicolas COSME – CTO & Co-founder
SEMANA	Paul MOUROT
VAADATA	Renaud CAYOL – Pentester
VAADATA	Aloïs THÉVENOT – CTO / Pentester
VAADATA	Nicolas BONNEFOUS – COO

3 Document history

Version	Date	Author	Comment
1.0	27/01/2023	Renaud CAYOL	Document creation

4 Referenced documents

Title	Version	Author

1	Scope.....	2
2	Contacts	2
3	Document history.....	2
4	Referenced documents.....	2
5	Executive summary	4
5.1	Objectives and methodology.....	4
5.2	Findings.....	4
5.3	General comments and recommendations	4
6	Overview table.....	5
6.1	Reconnaissance.....	5
6.2	Accessible systems and services	5
6.3	Web server.....	5
6.4	Application tests.....	5
7	Finding – Reconnaissance phase.....	7
7.1	Human elements.....	7
7.2	Technical elements.....	8
8	Findings – Application app.semana.io.....	9
8.1	V234-01 - Cross Origin Resource Sharing – Multiple endpoints.....	9
9	Logging and Monitoring	11
10	Tested items.....	12
11	Items not tested	12
12	Elements to delete.....	12
13	Annexes	13
13.1	Audit methodology.....	13
13.2	Risk rating.....	14

5 Executive summary

5.1 Objectives and methodology

This security audit has been commissioned by **SEMANA**, and conducted by VAADATA the 25th and 26th of January, 2023 over 2 man-days.

This was a blackbox / greybox audit. The main phase of the audit was blackbox and, once all blackbox tests were done, we switched to a greybox approach, with the two users provided.

The objective was to perform a global security audit of the platform, looking for both technical and logical flaws.

Social engineering was not used in this audit (except for message and emails sent via the audited platform).

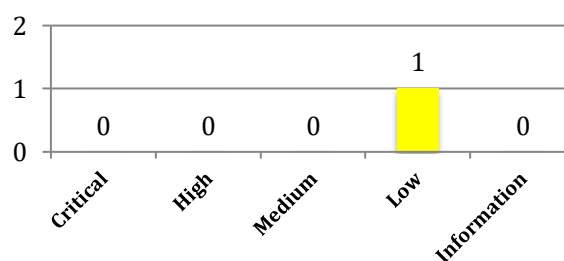
Our security testing methodology follows the OWASP's best practices and is composed of different phases, from open-source information research (Reconnaissance) to the exploitation of discovered vulnerabilities.

5.2 Findings

We found some endpoints misconfiguration that allowed CORS attacks.

All flaws have been manually tested, verified and are classified as Critical, High, Medium, Low or Information.

The following chart enumerates the technical vulnerabilities found during this audit.



5.3 General comments and recommendations

The only vulnerability found is of little impact and requires social engineering to be exploited, which severely limit its criticality.

From the point of view of an external attacker, the platform seems to be secure. The use of (properly implemented) mainstream, high-profile technologies such as Firebase and OAuth add a significant layer of security that is unlikely to be threatened as long as the configuration of those remains up to date.

Concerning the graybox (logged) part of the application, our tests have only been superficial and we recommend a more in-depth audit to ensure the security of the application in itself.

6 Overview table

6.1 Reconnaissance

Tests performed	Status	Severity
Content research according to known existent vulnerabilities	✓	NA
Search of technical information on job offers	✓	NA
Search of technical information on online databases (Shodan, Censys...)	✓	NA
Search of subdomains on indexed content (Search engine, SSL/TLS configuration...)	✓	NA
Search of data leakage	✓	NA

6.2 Accessible systems and services

Tests performed	Status	Severity
Search of accessible services through DNS enumerations	✓	NA
Scan of accessible services	✓	NA

6.3 Web server

Tests performed	Status	Severity
Scan of potential vulnerabilities on the web services	✓	NA
Verification of the versions of the component used by the server	✓	NA
Security configuration of the web servers	✓	NA

6.4 Application tests

Tests performed	Status	Severity
Injects (SQL, NoSQL, OS command, LDAP, code...)	✓	NA
Authentication system and user rights management	✓	NA
Sensitive data exposure	✓	NA

Banking data exposure	✓	NA
Rights control	✓	NA
Security configuration on the application layer	✗	Low
Cross Site Scripting (XSS)	✓	NA
Usage of components with known vulnerabilities	✓	NA
File path traversal	✓	NA
Client-side template injection	✓	NA
Clear text password submission	✓	NA
External service interaction (DNS, HTTP, SMTP)	✓	NA
Technical information disclosure	✓	NA
Open redirection	✓	NA
Security of session cookies	✓	NA
Security of upload functionalities	✓	NA
Application layer denial of services	✓	NA
HTTP parameter pollution	✓	NA
Source code disclosure	✓	NA
Directory listing	✓	NA
Search of available content with dictionary attack	✓	NA

7 Finding – Reconnaissance phase

That section describes information found during our Reconnaissance phase. It includes both human and technical elements related to the scope of the audit.

7.1 Human elements

It is relatively common for a pirated platform to have its users' credentials published, like for Adobe, LinkedIn, Dropbox, etc.

This information (generally: email address and password) is collected and compiled in files available on the Internet.

No leaks were found for your domain in this audit.

It is recommended to monitor data leaks related to customer domains. This can be done by using a service such as HaveIBeenPwned: <https://haveibeenpwned.com/DomainSearch>

7.2 Technical elements

Subdomains:

```
app-dev.semana.io
image.app.semana.io
auth-demo.semana.io
auth-staging.semana.io
es.semana.io
auth-dev.semana.io
api-staging.semana.io
app.semana.io
trail.semana.io
api.semana.io
metabase.semana.io
it.semana.io
app-demo.semana.io
fr.semana.io
www.semana.io
image.app-staging.semana.io
en.semana.io
blog.semana.io
de.semana.io
app-staging.semana.io
auth.semana.io
```

Services:

```
Nmap scan report for app.semana.io (34.120.162.159)
Host is up (0.012s latency).
rDNS record for 34.120.162.159: 159.162.120.34.bc.googleusercontent.com
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE  SERVICE  VERSION
80/tcp    open   http
113/tcp   closed  ident
443/tcp   open   ssl/https UploadServer
```

8 Findings – Application app.semana.io

8.1 V234-01 - Cross Origin Resource Sharing – Multiple endpoints

Severity	OWASP Top 10	Exploitation probability
Low	YES – A5 – 2021	Low

Vulnerability type description:

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.

Contextual elements:

Some endpoints allows query from arbitrary domains.

URL: <https://app.semana.io/api/people/collaborators/?ids=54287>

Request:

```
GET /api/people/collaborators/?ids=54287 HTTP/2
Host: app.semana.io
Cookie: sid=s%3A5bkBbjbnEdzetmegTqaGug466NCAdL9-.niangxfU2f0locyKF3HUcmjAZ%2B3rr0o9pwUxpsFqmBE;
_zlcmid=1E6lYI4KxWL1Uh4;
mp_c65af14e417fc90c4193b745402ed273_mixpanel=%7B%22distinct_id%22%3A%20%22185e9281105249-0912b41a3f3845-c5c5429-144000-185e928110624b%22%2C%22%24device_id%22%3A%20%22185e9281105249-0912b41a3f3845-c5c5429-144000-185e928110624b%22%2C%22%24initial_referrer%22%3A%20%22%24direct%22%2C%22%24initial_referring_domain%22%3A%20%22%24direct%22%7D; _gcl_au=1.1.1359201575.1674663951;
mp_f5e4b189fc0f1e82556c45eccee35c84_mixpanel=%7B%22distinct_id%22%3A%20%2254286%22%2C%22%24device_id%22%3A%20%22185e81ce8337b-0465c18ff00d748-c5c5429-144000-185e81ce8348cc%22%2C%22%24initial_referrer%22%3A%20%22%24direct%22%2C%22%24initial_referring_domain%22%3A%20%22%24direct%22%2C%22%24user_id%22%3A%20%2254286%22%7D
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0
Accept: */*
Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://app.semana.io/vaadata/home?d=2023-01-26
Content-Type: application/json
X-Client-Version: 2.34.1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Origin: https://ontqpyzszfin.com
```

Response:

```
HTTP/2 200 OK
Access-Control-Allow-Origin: *
X-App-Version: 0
Content-Type: application/json; charset=utf-8
Etag: W/"80-lFjlmcd0Mg+Nw96ijF7TfkWpWTo"
Set-Cookie: sid=s%3A5bkBbjbnEdzetmegTqaGug466NCAdL9-
.niangxfU2f0locyKF3HUcmjAZ%2B3rr0o9pwUxpsFqmBE; Domain=app.semana.io; Path=/; Expires=Sun, 05 Feb 2023
13:36:25 GMT; HttpOnly; Secure; SameSite=None
X-Cloud-Trace-Context: f040adb21f17c40a78edd7202293b38b
Date: Thu, 26 Jan 2023 13:36:25 GMT
Server: Google Frontend
Content-Length: 128
Via: 1.1 google
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

{"ok":true,"data":[{"id":54287,"peopleId":"collaborator-54287","name":"Dummy
9","email":"dummy9@vaadata.eu","color":"#313141"}]}
```

The two endpoints we found with this problem are :

- <https://app.semana.io/api/groups/search>
- <https://app.semana.io/api/people/collaborators>

It's probable that other endpoints are also vulnerable.

Remediation:

Rather than using a wildcard or programmatically verifying supplied origins, use a whitelist of trusted domains.

9 Logging and Monitoring

Monitoring and tracking key functionalities on a platform allows for early detection of abnormal behaviors and therefore makes it possible to promptly react after an attack (incident response).

Logging and monitoring are thus essential elements in terms of security.

The table below provides a list of important actions (from a business context) on which abusive use have been performed during the audit. The logging/monitoring system linked to the platform should have detected these behaviors:

#	Description	Date and time*
01	Scan of https://app.semana.io/api/people/collaborators/?ids=54287	26/01/2023 From 14h35 to 14h36
02		
03		
04		
05		
06		

- Time is in UTC +1

These elements need to be monitored (logs) and trigger alerts in an automated fashion.

For more information about best practices with logging and monitoring:

- <https://www.vaadata.com/blog/logging-monitoring-definitions-and-best-practices/>

IP addresses source of the tests:

- 81.250.174.11 (Orange)
- From 5.50.80.193 to 5.50.80.197 (Bouygues)

10 Tested items

- Login/logout
- Firebase implementation
- OAuth implementation
- Add/remove users to favorites
- Book/unbook a seat
- Edit user profile
- Change profile picture

11 Items not tested

Anything not listed previously.

12 Elements to delete

(Email) accounts used during the tests:

- dummyX@vaadata.eu (Renaud CAYOL)

13 Annexes

13.1 Audit methodology

The methodology we use is recognized as the most efficient, and based on years of testing experience, from many organizations acting in the field of information security. It relies on a series of four main steps, conducted on a cyclical basis.

Reconnaissance: Information research around the target, outside the application itself.

Mapping: Study of the application and of its environment.

Discovery: Vulnerabilities research, on both server side and client-side aspects.

Exploitation: Vulnerabilities exploitation, to push the analysis further and determine the potential impact.



Main tools used during the test, in addition to manual tests:

- BurpSuite Pro
- nMap, dig, Subfinder, Amass
- Open source information research, including Maltego
- Sqlmap
- Internally developed tools and scripts
- Metasploit

13.2 Risk rating

Risks related to vulnerabilities listed in this report have been rated so as to take probability and impact aspects into consideration.

Probability:

Considering the vulnerability within an attack scenario, several aspects are taken into account, to estimate the “probability”.

First, the “threat actor” performing the attack: their skills, motivation, attack opportunity and magnitude of the actor (number of attackers).

In second place, the vulnerability itself: easy of discovery, exploitation, awareness (is it well known), and then detection mechanisms.

Impact:

The technical impact in terms of confidentiality, integrity and availability is estimated, as well as the possibility to trace the threat agent.

On the other hand, the “business” impact regarding financial, reputational, compliance and privacy violation aspects also enter the calculation.

A tool developed internally allows us to perform this risk evaluation, in a reliable and repeatable manner.

Overall risk severity

IMPACT	HIGH	MEDIUM	HIGH	CRITICAL
	MEDIUM	LOW	MEDIUM	HIGH
	LOW	INFORMATION	LOW	MEDIUM
		LOW	MEDIUM	HIGH
		PROBABILITY		

Following the evaluation of the risk, the severity appears as either Information, Low, Medium, High or Critical.

How to interpret the vulnerability in these various cases?

LEVEL	APPRECIATION
CRITICAL	The vulnerability must be fixed as soon as possible.
	The potential impact for the company is very high, and there is a high probability that an attacker (not necessarily experienced) spots the vulnerability. In some cases, the vulnerability might be exploited by mistake.
HIGH	The vulnerability requires a very specific attention.
	Remediating (or mitigating) the flaw must be a priority, so as to eliminate or reduce the risk. Exploitation and potential impact probabilities are medium or high depending on the case.
MEDIUM	Though rated as « medium », the vulnerability identified here might cause a lot of damage if detected and exploited by an attacker.
	The threat is significant and must be taken into account, at least to reduce the impact of a potential exploitation.
LOW	Considering the low or medium probability of exploitation and potential impact, the vulnerability identified can be considered as low (but should not be ignored).
	It is recommended to solve the vulnerability. As a minimum, its evolution must be monitored and documented.
INFORMATION	The vulnerability does not imply a particular danger and is given here as information.