Zeplin - Web + API Penetration Test Report - November 2024

Report generated on May 9 2025

Targets

zeplin.io
api.zeplin.io
omlet.dev
app.zeplin.io
api.zeplin.dev
feta.omlet.dev
public.zeplin.io
scene.zeplin.io
jira-cloud.zeplin.io
msteams-app.zeplin.io

Test period

Nov 13, 2024 Nov 27, 2024

Status

Final

Test performed by

 Herane Malhotra **Lead**

 Kadri Raghavendra Rao **Pentester**

Executive Summary

Cobalt conducted a pentest of the Zeplin - Web + API application and API to assess the risk posture and identify security issues that could negatively affect Zeplin's data, systems, or reputation. The scope of the assessment covered Zeplin - Web + API and included credentials for various levels of privilege within the scope. A Cobalt pentest team of 2 conducted this engagement between Nov 13, 2024, and Nov 27, 2024.

This pentest was a manual assessment of the security of the application's functionality, business logic, and vulnerabilities, such as those cataloged in the Open Web Application Security Project (OWASP) Top 10. The assessment also included a review of security controls and requirements listed in the OWASP Application Security Verification Standard (ASVS). The pentesters leveraged tools to facilitate their work. However, the majority of the assessment involved manual analysis.

During this engagement, Cobalt's testers reported their findings and rated them based on the following severities:

	CRITICAL	HIGH	MEDIUM	LOW	INFO
Open	0	0	2	3	0
Resolved	0	0	1	10	1
Total	0	0	3	13	1

During the assessment, Cobalt identified several vulnerabilities in the application, including a Medium-risk finding related to the disclosure of Personally Identifiable Information (PII) and a Medium-risk finding related to a Stored Cross-Site Scripting (XSS) vulnerability.

It was discovered that any user could identify the PII of any other user of the application, including

their full name and username. This information leakage could happen through multiple vectors, such as improper error handling, web responses, default pages, and source code.

The application's "Add Link" functionality within the Section/Project feature was found to be vulnerable to Stored XSS. An attacker could exploit this vulnerability by submitting a compromised link containing JavaScript code, which would then be stored within the application's database and subsequently displayed to other users. This could allow the attacker to gain unauthorized access to user accounts, steal sensitive information, or perform other malicious actions.

It was also found that the application does not properly limit the number or frequency of interactions with an actor, such as the number of incoming requests. This could allow an attacker to perform actions more frequently than expected, potentially causing a denial of service or compromising program logic.

The application was found to be missing several recommended HTTP security headers, such as Content-Security-Policy (CSP) and HTTP Strict-Transport-Security (HSTS). Implementing these headers is recommended to strengthen the application's overall security posture by mitigating certain types of attacks, such as protocol downgrade attacks and cookie hijacking.

The application was also found to be sending the session token as part of the URL, which could allow an attacker to intercept and steal the token.

The following findings were reported:

- PII disclosure of any user of the application
- Stored XSS via the 'Add Link' functionality in Section/Project
- Lock arbitrary account
- No Rate Limiting On the 'Change Email' functionality
- Unauthenticated User Enumeration
- Missing HTTPOnly Flag
- User enumeration on the Forgot password page
- CSV / Formula Injection

- Username Leakage in Application Response
- Concurrent user logins allowed
- Cookie Missing Security Flags
- Cross-origin resource sharing (CORS) misconfigured
- CSP Header Misconfiguration
- Session token in URL - JWT
- Outdated JQuery usage
- Weak Cipher Suites In Use [SSL/TLS Misconfiguration]
- Registration doesn't require email verification
- Application Redirecting from HTTP to HTTPS over Insecure Channel
- External Service Interaction (DNS)

Specific recommendations were provided for each finding. As a whole, the recommendations indicate gaps that Zeplin could address by making improvements to the identified misconfigurations and access control on the web application.
These improvements include recommendations and security best practices that the Zeplin team should address to increase the overall security posture of the organization.

Approach

The engagement was done according to industry best practices. The following outlines the process from start to finish.

Pre Engagement

- Scoping
- Customer documentation
- Access

Engagement

- Reconnaissance
- Tool assisted assessment
- Manual assessment
- Vulnerability identification and/or exploitation
- Risk analysis
- Reporting

Post Engagement

- Prioritized remediation
- Recommendations
- Retesting (if applicable)

Risk Factors

Each finding is assigned two factors to measure its risk. Factors are measured on a scale of 1 (very low) through 5 (very high).

Impact

This indicates the finding's effect on technical and business operations. It covers aspects such as the confidentiality, integrity, and availability of data or systems; and financial or reputational loss.

Likelihood

This indicates the finding's potential for exploitation. It takes into account aspects such as skill level required of an attacker and relative ease of exploitation.

Severity Definitions

When our pentesters find vulnerabilities, they use the standard OWASP Risk Rating Methodology, and then classify them into one of the following risk levels, based on their business impact and likelihood: `risk = impact * likelihood`

CRITICAL

Includes vulnerabilities that require immediate attention. Risk score of 25.

HIGH

Impacts the security of your application/platform/hardware, including supported systems. Includes high probability vulnerabilities with a high business impact. Risk score range: 16 through 24.

MEDIUM

Includes vulnerabilities that are: medium risk, medium impact; low risk, high impact; high risk, low impact. Risk score range: 5 through 15.

LOW

Specifies common vulnerabilities with minimal impact. Risk score range: 2 through 4.

INFORMATIONAL

Notes vulnerabilities of minimal risk to your business. Risk score of 1.

Terms

PLEASE NOTE: It is impossible to test networks, information systems, and people for every potential security vulnerability. This report does not form a guarantee that your assets/targets are secured from any and all threats. All assessments performed, and their results, are only from the point-of-view of Cobalt, at the time of the engagement. Cobalt is unable to ensure or guarantee that your assets/targets are or will be completely safe from every form of attack now or in the future. With the ever-changing environment of information technology, any assessment performed by Cobalt will necessarily exclude vulnerabilities in software or systems that are unknown at the time of the engagement. For a full list of terms governing the services of Cobalt, this report, and the usage thereof, please consult the Terms of your Agreement with Cobalt or www.cobalt.io/terms.