Zeplin - Web + API Penetration Test Report - October 2025

Report generated on Dec 1 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

Oct 13, 2025 Oct 27, 2025

Status

Final

Test performed by

 Fatih Egbatan **Pentester**

 Ahmet Can Karaağaçlı **Lead**

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 Oct 13, 2025 and Oct 27, 2025.

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	0	1	0
Resolved	0	1	0	2	1
Total	0	1	0	3	1

During the assessment, several vulnerabilities were identified that could pose significant risks to the application and its users. A high-severity account takeover vulnerability was discovered via open redirection on feta.omlet.dev, potentially allowing attackers to craft phishing links that appear legitimate, leading to unauthorized account access.

Additionally, the application was susceptible to email flooding due to IP-based rate limit bypass on email verification requests, which could overwhelm the Zeplin email server or user inboxes, creating a denial-of-service condition. The application was found to be transmitting session tokens in the URL, which could lead to exposure of these tokens through caching or browser history. Finally, the application exhibits detailed error messages on scan deletion, potentially revealing sensitive information about the backend technology.

Cobalt's team reported the following findings during the pentest:

Account Takeover via Open Redirection
Email Flood - Lack of Rate Limit on Email Verification Requests
Session Token in URL - JWT
Detailed Error Message on Scan Deletion
Insecure URL Shortening

Cobalt provided specific recommendations for each finding. As a whole, the recommendations indicate gaps that Zeplin could address by making improvements to input validation, rate limiting, session management, and secure coding practices.

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.