



Zeplin - Web + API - March 2020 Penetration Test Report

zeplin.io
app.zeplin.io
api.zeplin.io
img.zeplin.io
scene.zeplin.io
scene-api.zeplin.io
figma-api.zeplin.io
api.zeplin.dev
zpl.io
cdn.zeplin.io
jira-cloud.zeplin.io

TEST PERIOD

Mar 14, 2020 → Mar 28, 2020

STATUS

Final

TEST PERFORMED BY



Lead

Pentester

Contents

Executive Summary	3
Methodology	5
Pre Engagement 1 Week	5
Penetration Testing 2~3 Weeks	5
Post Engagement On-demand	5
Risk Factors	6
Criticality Definitions	7
Terms	8

Executive Summary

A gray box penetration test of the Zeplin - Web + API application was conducted to assess its risk posture and identify security issues that could negatively affect Zeplin's data, systems, or reputation. The scope of the assessment covered **zeplin.io, app.zeplin.io, api.zeplin.io, img.zeplin.io, scene.zeplin.io, scene-api.zeplin.io, figma-api.zeplin.io, api.zeplin.dev, zpl.io, cdn.zeplin.io, jira-cloud.zeplin.io**, and included credentials for various levels of privilege within the application(s). The pentest was conducted by 2 pentester(s) between Mar 14, 2020 and Mar 28, 2020.

This penetration test was a manual assessment of the security of the application's functionality, business logic, and vulnerabilities, such as those cataloged in the OWASP Top 10. The evaluation 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 involves manual analysis.

The pentesters identified 4 Low-risk vulnerabilities.

The assessment results show that the application was developed from a security-in-depth perspective. The vulnerabilities identified don't signify a direct risk to Zeplin's server, which is an indication of the security maturity of the Zeplin web application & API and the continuous work behind its development.

The low-risk issues identified were related to rate-limiting, session management, and misconfiguration/best practices, which can improve the security posture of the Zeplin web application even more.

Specific recommendations are provided for each finding. As a whole, the recommendations indicate gaps that can be addressed by improvements to rate-limiting, session management, misconfigurations.

Methodology

The test was done according to penetration testing best practices. The flow from start to finish is listed below.

Pre Engagement

- Scoping
- Customer
- Documentation
- Information
- Discovery

Penetration Testing

- Tool assisted assessment
- Manual assessment
- Exploitation
- Risk analysis
- Reporting

Post Engagement

- Prioritized remediation
- Best practice support
- Re-testing

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.

Criticality Definitions

Findings are grouped into three criticality levels based on their risk as calculated by their business impact and likelihood of occurrence, $\text{risk} = \text{impact} * \text{likelihood}$. This follows the [OWASP Risk Rating Methodology](#).

High

Vulnerabilities with a high or greater business impact and high or greater likelihood are considered High severity. Risk score minimum 16.

Medium

Vulnerabilities with a medium business impact and likelihood are considered Medium severity. This also includes vulnerabilities that have either very high business impact combined with a low likelihood or have a low business impact combined with a very high likelihood. Risk score between 5 and 15.

Low

Vulnerabilities that have either a very low business impact, maximum high likelihood, or very low likelihood, maximum high business impact, are considered Low severity. Also, vulnerabilities where both business impact and likelihood are low are considered Low severity. Risk score 1 through 4.

Terms

Please note that 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 are secure from all threats. The tests performed and their resulting issues are only from the point of view of Cobalt Labs. Cobalt Labs is unable to ensure or guarantee that your assets are completely safe from every form of attack. With the ever-changing environment of information technology, tests performed will exclude vulnerabilities in software or systems that are unknown at the time of the penetration test.

