Zeplin - Web + API - May 2021 Penetration Test Report

TARGET(S)

zeplin.io

app.zeplin.io

api.zeplin.dev

TEST PERIOD

May 4, 2021 → May 18, 2021

STATUS

Final

TEST PERFORMED BY


[redacted] Lead


[redacted] Pentester

Contents

Executive Summary

A gray box penetration test of the Zeplin - Web + API application was conducted in order 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 Web and API. The pentest was conducted by 2 pentesters between May 4, 2021 and May 18, 2021.

This penetration test was a manual assessment of the security of the application's functionality, business logic, and vulnerabilities such as those catalogued in the 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 involves manual analysis.

The pentesters identified 0 High, 5 Medium, and 5 Low risk vulnerabilities.

The application's overall risk is Medium. However, it is recommended to review the reported vulnerabilities for mitigation procedures, since new vulnerabilities introduced through future updates can represent chaining possibilities and increase the overall risk of the application.

After analysis of the identified vulnerabilities, the following should be taken into consideration: The application should avoid user enumeration vulnerabilities and weak password policy. Combined together, the likelihood of a successful account takeover is high.

The testers identified a few issues related to rate limiting that could allow an attacker to bruteforce coupon code and lock users' accounts.

The registration process doesn't require to verify the email address before allowing access to the account which could lead to social engineering attacks and various other attack vectors.

It was also found that the Content Security Policy is in "report-only" mode and need to be implemented.

Finally, the testers found that the users' sessions are sent in GET parameter and are not invalidated upon an email change operation.

Significant findings from this penetration test include:

- Weak password policy
- Multiple username and email enumeration
- Coupon code bruteforcable
- Lock arbitrary account
- Registration doesn't require email verification

Specific recommendations are provided for each finding. As a whole, the recommendations indicate gaps that can be addressed by improvements to authentication, rate limiting and misconfiguration.

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, `risk = impact * 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.