Zeplin - Web + API Penetration Test Report - July 2022

TARGET(S)

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

TEST PERIOD

Jun 20, 2022 ⟶ Jul 4, 2022

STATUS

Final

Executive Summary

Cobalt conducted a gray box 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 applications. The pentest was conducted by 2 pentesters between Jun 20, 2022 and Jul 4, 2022.

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 testing, Cobalt's pentesters tested for vulnerabilities and rated them based on the following categories:

Critical	High	Medium	Low	Informational
0	0	1	8	1

Cobalt rated the scoped applications' overall risk as Low. We recommend reviewing the reported vulnerabilities for mitigation procedures, as new vulnerabilities introduced through future updates could present chaining possibilities and increase the overall risk to the application.

The most severe finding that pentesters were able to discover was related to the lack of an anti-scripting mechanism on the "user log-on" functionality, which allowed us to automatically send enough requests to lock an account. Pentesters rated this vulnerability as Medium, because an attacker could exploit this lock arbitrary application accounts and keep them

locked.

Testers rated the remaining findings as Low-risk or Informational, as they did not pose any direct security impact to the application and were deviations from security best practices. These included username enumeration vulnerabilities, misconfigured headers and cookie flags, external service interactions, and a lack of antivirus scanning on uploads. However, Cobalt recommends remediating this to strengthen the applications overall security posture.

Testers reported the following significant findings:

- Ability to Lock Arbitrary Account
- Username enuimeration
- Cookies missing `HttpOnly` flag
- External Service Interaction via Domain Name Service (DNS)
- No Antivirus Scanning on Uploaded Files

Cobalt provided specific recommendations for each finding. As a whole, the recommendations indicate gaps that can be addressed by making improvements to the identified Server Security 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.

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 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.