Cobalt

Zeplin - Web + API Penetration Test Report - October 2023

TARGET(S)

zeplin.io

app.zeplin.io

omlet.dev

feta.omlet.dev

api.zeplin.dev

api.zeplin.io

TEST PERIOD

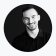
Oct 4, 2023 → Oct 18, 2023

STATUS

Final

Prepared for Zeplin. For informational purposes only and may not be relied upon for any other purpose. To be shared only with permission from Zeplin. Cobalt disclaims all liability to any third party arising from this letter. Subject to Cobalt terms of use on https://cobalt.io.

TEST PERFORMED BY

	Saad Nasir	Lead
	Ryne Hanson	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 Oct 4, 2023 and Oct 18, 2023.

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	1	0	3	2

- All high severity findings have been fixed and retested
- 1 low severity finding has been fixed and retested

During the assessment, pentesters found issues related to input validation, including an instance of Cross-Site Scripting (XSS) vulnerabilities and an HTML 5 Storage Manipulation vulnerability. An attacker could leverage these vulnerabilities to fully take over an account in the application. All users are vulnerable to this stored attack, and the legitimate Zeplin URL would make this a powerful vector for phishing-style attacks.

The testers also found that the application did not properly implement the cookies flags and security headers. This could allow an attacker who can access the token to take over the victim's session and perform actions on their behalf.

Additionally, pentesters found that applications redirected from HTTP to HTTPS over insecure channels. An attacker suitably positioned to view a legitimate user's network traffic could record and monitor their interactions with these resources, which may indirectly disclose information about the user's activity on the application itself.

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

- Stored Cross-Site Scripting in Image Uploads
- Application Redirecting from HTTP to HTTPS over Insecure Channel
- HTML 5 Storage Manipulation (DOM Based)
- Host Header Poisoning
- Application Revealing Backend Technologies

Cobalt provided specific recommendations for each finding. As a whole, the recommendations indicate gaps that Zeplin can address by making improvements to such as input validation, authorization, or identified misconfigurations

Prepared for Zeplin. For informational purposes only and may not be relied upon for any other purpose. To be shared only with permission from Zeplin. Cobalt disclaims all liability to any third party arising from this letter. Subject to Cobalt terms of use on https://cobalt.io.

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
- Retesting

Prepared for Zeplin. For informational purposes only and may not be relied upon for any other purpose. To be shared only with permission from Zeplin. Cobalt disclaims all liability to any third party arising from this letter. Subject to Cobalt terms of use on https://cobalt.io.

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.

Info

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

Prepared for Zeplin. For informational purposes only and may not be relied upon for any other purpose. To be shared only with permission from Zeplin. Cobalt disclaims all liability to any third party arising from this letter. Subject to Cobalt terms of use on https://cobalt.io.

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.