CYREX

Penetration Test Report

Marketplace

Prepared for: Luxy.io

Prepared by: Tim De Wachter, CTO, Cyrex Ltd

2023-05-08

TABLE OF CONTENTS

1 Executive summary 2

2 About Cyrex 3

3 Scope of engagement 4

4 Risk analysis 5

5 Conclusion 8

1. EXECUTIVE SUMMARY

Cyrex was contracted by Luxy.io to conduct a penetration test to determine its exposure to a targeted attack. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against the scope with the goals of:

- Identifying if a remote attacker could penetrate the scope its defences.
- Determining the impact and possibility of a security breach.

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The attacks were conducted with all levels of access that a general internet user would have.

As Luxy.io provided Cyrex with source code concerning the scope, we can label this kind of test as a white box penetration test. Cyrex was granted access to the application with minimal user privileges.

What follows is a detailed explanation of all the different vulnerabilities, advised patches and an accompanying risk analysis. We are confident that the penetration test and this report helps the customer to raise its security regarding the web application and the API service to a higher level.

2. ABOUT CYREX

Cyrex is a native cybersecurity scale-up that specialises in penetration testing, load testing, and software development. Our focus is on online gaming, blockchain, and the SaaS world.

With more than 50 security engineers and 100 clients worldwide, Cyrex is known for its work on state-of-the-art technologies and innovation in multiple industries. With a constant drive for excellence, Cyrex has been recognized repeatedly for its quality of work, timely deliverables, and an outstanding operational performance.

Cyrex goes beyond the traditional penetration testing offering through a unique approach that integrates pair-hacking methodologies and manual security testing. As leaders in the industry for over 10 years, our teams are prepared for any type of project regardless of the technology stack, providing a full coverage of our partners' needs.

We are Cyrex, the gold standard in security, load testing and development.

3. SCOPE OF ENGAGEMENT

Cyrex performed a penetration test on Luxy.io his web application. The following tests were performed by Cyrex:

Initial assessment (2023-03-06 - 2023-03-14).

Retest (2023-04-17 - 2023-04-17).

Retest (2023-04-28 - 2023-04-28).

During the penetration test, strict protocols, guidelines and a unique workflow have been followed. Different frameworks were integrated into this process flow which are in line with the ethical hacking procedures. The process involved an active analysis of the application for any weaknesses, technical flaws or vulnerabilities.

The focus of the test was to determine whether the applications were prone to any technical vulnerabilities that could affect the confidentiality and integrity of the data of Luxy's customers, the availability of the platform and security of its users.

During the entire penetration testing life cycle, Cyrex performed the following actions in order to determine security issues within the application:

1. Analysis and testing of different endpoints
2. Tampering of different parameters within those requests
3. Identification of potential injection points, security flaws and vulnerabilities
4. Exploitation to provide Proof of Concept (PoC)

With the regression testing, we make sure the vulnerabilities discovered during the penetration test are patched in a correct manner and no other vulnerabilities have been introduced during the patching process.

The following hosts, IPs and components were part of the tested scope:

- Luxy Marketplace
- Luxy API
- Luxy Admin
- Project Source

We want to thank Luxy.io for putting trust in our know-how and expertise concerning ethical hacking specific to application security.

4. RISK ANALYSIS

The risk assessment conducted uses the 'Common Vulnerability Scoring System'. The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

CVSS is composed of three metric groups: Base, Temporal, and Environmental, each consisting of a set of metrics.

The Base metric group represents the intrinsic characteristics of a vulnerability that are constant over time and across user environments. It is composed of two sets of metrics: the Exploitability metrics and the Impact metrics.

- The Exploitability metrics reflect the ease and technical means by which the vulnerability can be exploited. That is, they represent characteristics of the thing that is vulnerable, which we refer to formally as the vulnerable component.
- The Impact metrics reflect the direct consequence of a successful exploit, and represent the consequence to the thing that suffers the impact, which we refer to formally as the impacted component.

The Temporal metric group reflects the characteristics of a vulnerability that may change over time but not across user environments. For example, the presence of a simple-to-use exploit kit would increase the CVSS score, while the creation of an official patch would decrease it.

The Environmental metric group represents the characteristics of a vulnerability that are relevant and unique to a particular user's environment. Considerations include the presence of security controls which may mitigate some or all consequences of a successful attack, and the relative importance of a vulnerable system within a technology infrastructure.

For more information:
https://www.first.org/cvss/

The risk assessment for a finding serves as an indication. It is intricate to estimate the exact (business) impact of a vulnerability. Ultimately, it is up to the client to determine the urgency of remedying a security weakness.

Additional report labels

Next to the risk classifications, several other indication labels are (possibly) used in the report:

- When there is no direct security impact related to the finding, but it is still recommended to follow the best practices as outlined in the recommendation section: INFO
- When a vulnerability found during the initial research has been retested, and is resolved correctly: ✓ RESOLVED
- When a vulnerability found during the initial research has not been resolved, but is marked as an acceptable risk by the client: ACCEPTED RISK

CRITICAL	HIGH	MEDIUM	LOW	INFO

No findings	No findings	No findings	No findings	3 findings

Table 4.1: Finding counts by severity.

Category	Findings
✓ **Access Control Flaws**	OK ✓ Resolved: 5 findings
✓ **Business Logic Flaws**	OK ✓ Resolved: 8 findings
✓ **Open Redirect Vulnerabilities**	No findings
✓ **Improper Input Validation**	OK ✓ Resolved: 2 findings
✗ **Improper Session Management**	INFO (0) ● Info: 1 finding of which 1 risk accepted by the client ✓ Resolved: 1 finding
✗ **Security Misconfiguration**	INFO (0) ● Info: 2 findings of which 2 risks accepted by the client ✓ Resolved: 5 findings
✓ **SQL Injection**	No findings
✓ **Denial of Service**	No findings
✓ **Information Disclosure**	FALSE POSITIVE ✓ Resolved: 8 findings
✓ **Brute Force Attacks**	OK ✓ Resolved: 1 finding

✓ **Remote Code Execution**	No findings
✓ **Path Traversal Attacks**	No findings
✓ **Unrestricted File Upload**	OK ✓ Resolved: 4 findings
✓ **CSS Injection**	No findings
✓ **Broken Authentication Flaws**	No findings
✓ **Cross Site Scripting**	No findings
✓ **Server-Side Request Forgery**	No findings
✓ **Prototype Pollution**	No findings
✓ **Local File Inclusion**	No findings
✓ **Privilege Escalation**	No findings

Table 4.2: An overview of findings listed by section.

5. CONCLUSION

Cyrex determined that the overall security maturity of this application is great and will meet the risk appetite of any end user. Most suggested patches were implemented in a correct manner but more importantly the web application was tested and validated thoroughly by Cyrex' application security experts.

We can also clearly see that Luxy has improved its base security level, and takes security and data privacy serious.

User input is one of the main injection points for malicious end-users for any application, Luxy has applied validations for the parameters used within the exposed endpoints. These validations are handled in an effective and secure manner whenever the methods are tampered with. In this way, malicious payloads are rendered useless and will not affect the system or its data.

Layered security is implemented in the application, which is the recommended security best-practice for any application, meaning whenever a new vulnerability would be exploited it will not impact the end-user as much as it potentially could, or it will be a lot harder for a malicious actor to determine a new vulnerability within the target scope.

We are confident that we tested the whole scope and all functionalities available to us as in-depth as possible.

A few lower risk vulnerabilities and recommendations are accepted as risk. But these are merely suggestions that don't have a big security impact on the application.