

LYYTI WEB APPLICATION

PENETRATION TEST SUMMARY

Issued by Fraktal on 18 March 2024

INTRODUCTION

Fraktal has performed a penetration test of Lyyti Oy's Lyyti web application. The objective for the test was to verify the current security posture. This testing phase of the engagement took place in April 2023 with additional fix verification testing in November 2023 and March 2024.

SCOPE

In scope for the testing was the web application. The testing was focused on the following areas:

- Login brute force
- CSRF
- XSS
- File handling (upload/download)
- Broken authentication
- Sensitive data exposure
- Broken access control
- Invalid input/output

METHOD

Method for testing was grey box with architecture diagrams, documentation, and developers' support available for review and test planning. Testing was performed by following best practices, OWASP Web Security Testing Guide, and by using Burp Suite Pro.

CONCLUSION

The testing concluded that the overall security posture is very good against most attack vectors relevant to the service.

During the fix verification testing performed in March 2024, Fraktal verified that Lyyti has effectively solved and mitigated the security issues encountered in previous assessments, strengthening the solution's security.

As web security and attacks evolve, a similar penetration test should be performed regularly to verify continued security posture.

ABOUT FRAKTAL

Fraktal Oy/Ltd is a cyber security company focusing on advising and testing software security and cloud implementations.