Lyyti web application

Executive summary

Introduction

Second Nature Security Oy was contracted by Lyyti Oy to assess the security of the Lyyti web application.

The audit was conducted in November 2024 for Lyyti Core and in February 2025 for Lyyti Modules. Verification audits of the fixes and other work for Lyyti Core were done during February and March 2025.

Scope

The audit scope included web application and APIs for both Lyyti Core and Lyyti Modules technology stacks and review of infrastructure code and workflows for Lyyti Modules.

The workload for Lyyti Core audit was 5 person-days, and workload of the verifications was 3 person-days for Lyyti Core.

The workload for Lyyti Modules was 5 person-days for audit, and 3 person-days for review of infrastructure code and workflows.

Method

The audit methodology was based on the OWASP Testing Guide documentation and the OSSTMM standard and by following best practices.

Infrastructure code and workflows review was based on documentation review.

Conclusion

The audit confirmed that Lyyti's application has strong security controls in place, with no critical vulnerabilities found. In total, the Lyyti Core audit revealed 0 critical, 1 high, 2 moderate and 0 low level vulnerabilities. In addition, 9 weakness level findings were found. All vulnerabilities and one weakness in Lyyti Core were confirmed as properly fixed after the verifications.

The audit for Lyyti Modules revealed 0 critical, 0 high, 0 moderate and 2 low level vulnerabilities. In addition, 3 weakness level findings were found.

During the infrastructure code and workflows review it was evident, that information security has been considered and well implemented during the development. Suggested actions have been discussed separately with Lyyti development team.