mnemonic

CONFIDENTIAL

REPORT

WEB APPLICATION SECURITY ASSESSMENT: EXTENDED SUMMARY

Orgbrain AS

Place	Oslo, Norway
Date	2021-05-03
Version	1.0
Author	Kaspar Papli

Executive Summary

In December 2020 and January 2021, mnemonic performed a security assessment of the Orgbrain platform, consisting of a web application and backing APIs. The main goal of the assessment was to provide an independent security review of the web application, identifying concrete vulnerabilities and providing advice about how these vulnerabilities can be fixed or mitigated.

The platform is built as a progressive web app that communicates with backend services via an HTTP API and WebSockets. This assessment covered the frontend web application along with the backend web services.

Following the initial report, Orgbrain applied fixes and mitigations to discovered security issues according to mnemonic's recommendations. In March 2021, mnemonic conducted a retest of the Orgbrain platform. The goal of the retest was to verify that the implemented fixes and mitigations were effective against discovered vulnerabilities and did not introduce any additional security issues.

During the retest, all reported security issues were confirmed to be appropriately fixed or mitigated following mnemonic's recommendations. No new security issues arising from the applied fixes or mitigations were identified.

Test Execution

mnemonic tested for standard web application vulnerabilities, such as those listed in the OWASP Top 10 Application Security Risks (2017 and 2013).

The security assessment simulated a knowledgeable and skilled threat actor attempting to explore the system, bypass the security controls present, or otherwise cause undefined or unexpected behavior.

Testing was conducted remotely from mnemonic's headquarters in Oslo, Norway.

Testing Methodology

mnemonic has conducted security and penetration testing, source code audits, and related services, ever since the company was founded in 2000. Our security testing methodology is based on the combination of open standards and collections of "industry best practice", together with our own experience accumulated over the last 20 years. In addition to this, testing is supported by an extensive knowledge base, as well as internally developed tools and scripts.

Our methodology is supported by the processes "*P3003 Procedure for security testing*" and "*P3006 Use and maintenance of testing platform*" in mnemonic's ISO 9001 / ISO 27001 certified quality and security management system, as well as associated templates and documentation.