mnemonic

TLP: CLEAR

# Assessment Summary
# Web Application Security Assessment
# Orgbrain AS

| | |
|---|---|
| Place | **Oslo** |
| Date | **2026-02-05** |
| Version | **1.0** |
| Author | **Peder Grundvold** |

# Assessment Summary

In October 2025, mnemonic performed a security assessment of the Orgbrain platform. The application was also previously tested by mnemonic in 2020.

Orgbrain is a Norwegian SaaS company offering a governance portal for boards and general assemblies. Their platform consolidates features like meeting planning, document management, secure communication, digital signatures, shareholder registry (aksjeeierbok), board evaluations, due-diligence dataroom, and AI-assisted drafting.

The project resulted in a technical report, describing the findings and observations made during the assessment, as well as recommendations and potential improvements. Following the initial report, Orgbrain proceeded to implement fixes for discovered issues according to mnemonic's recommendations.

In February 2026, 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 the previously discovered vulnerabilities, and that they 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.

## Test Execution

Testing was carried out from mnemonic's dedicated testing environment in Oslo, by an experienced cyber security consultant. Dedicated test accounts and test organisations were utilized in order to avoid exposure of customer data.

mnemonic tested for standard web application vulnerabilities, such as those listed in the OWASP Top 10 Application Security Risks (2025).

The main goal of the test was to identify concrete vulnerabilities and provide recommendations on how they can be fixed or mitigated. Additionally, the assessment aimed to provide deeper insight into the application's overall security posture and assist in selecting and prioritizing remediation activities to effectively manage overall risk exposure.

## 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 practices*", together with our own experience accumulated over the last 25 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 Security testing procedure*" 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.