Fine penetration tests for fine websites

Dr.-Ing. Mario Heiderich, Cure53
Wilmersdorfer Str. 106
D 10629 Berlin
cure53.de · mario@cure53.de

Cure53 Security Assessment of Ente Platform, Cryptography & Infra, Management Summary, 10.2025

Cure53, Dr.-Ing. M. Heiderich, Y. Yuan, Dr. N. Kobeissi, S. Rajbhar

Cure53, a Berlin-based IT security consulting firm, was engaged to conduct a comprehensive security assessment of the Ente platform. This project, commissioned by Ente in August 2025, involved both a penetration test and a source code audit targeting the platform, its server cryptography, the underlying Compute Instances infrastructure, and selected feature sets.

The engagement (ENT-02) was conducted in October 2025 (CW42) by a four-person review team, comprising a total of fourteen days.

The work was divided into four distinct Work Packages (WPs) for test execution efficiency. These were defined as follows:

- **WP1:** White-box code audits & reviews against Ente server crypto functions
- **WP2:** White-box pen.-tests & code audits against Ente authn & authz, ACL
- **WP3:** White-box pen.-tests & code audits against Ente specific functionalities
- **WP4:** Gray-box pen.-tests & assessments against Ente compute instances

This assessment builds upon a previous review from March 2023 (*ENT-01*), where Cure53 vetted the Ente platform's crypto designs. For this engagement, a dual white- and gray-box methodology was adopted, with the Ente team providing Cure53 testers with full access to source code, documentation, and other assets to ensure comprehensive test coverage.

A dedicated Discord server was used for all communication, enabling Cure53 to provide frequent status updates and live reporting. This collaborative process proved highly efficient, with minimal queries and no significant blockers.

The Cure53 team achieved satisfactory coverage, identifying a total of fifteen security issues. These findings were categorized as ten security vulnerabilities and five general weaknesses.

In summary, the Ente platform exhibits multiple security vulnerabilities spanning authentication, email management, file handling, and infrastructure components. While the system benefits from solid foundations - including robust server-side access control list (ACL) enforcement and generally secure coding practices - several critical issues were identified that require immediate attention, such as cross-site scripting (XSS) vulnerabilities and a counterfeit session mechanism, which introduce avoidable risks to the environment.

Dr.-Ing. Mario Heiderich, Cure53
Wilmersdorfer Str. 106
D 10629 Berlin
cure53.de · mario@cure53.de

That said, the Ente team's prompt action in addressing the discovered issues deserves recognition, having fixed twelve of the fifteen identified issues, including all *Critical* and *High* impact findings along with all but one *Medium* impact issue, which were subsequently verified by Cure53. Combined with the platform's well-designed architecture, this reflects a strong dedication to security and is commendable.

Additionally, certain identified issues, including for instance a desktop client remote code execution (RCE), were deemed out of scope for this assessment.

Cure53 would like to thank Vishnu Mohandas, Manav Rathi, and Neeraj Gupta from the Ente team for their excellent project coordination, support, and assistance, both before and during this assignment.