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 Small Improvements Web UI, API & Server, Management Summary, 01.-02.2025

Cure53, Dr.-Ing. M. Heiderich, BSc. D. Brinkrolf, MSc. J. Moritz, MSc. N. Krein

Cure53, a Berlin-based IT security consulting firm, has been contracted to conduct a security assessment of a number of newly-introduced Small Improvements features and authentication features. To give some context regarding the assignment's origination and composition, Small Improvements Software GmbH contacted Cure53 in October 2024. The test execution was scheduled for late January / early February 2025, namely in CW05. The project was completed with an investment of fourteen person-days to ensure the expected coverage was achieved. A team of four senior testers, leveraging their expertise, was assigned to the preparation, execution, and finalization of this project.

In line with a white-box testing methodology, the team was provided with complete transparency and comprehensive support to ensure thorough testing. This support encompassed access to source code, relevant URLs, documentation, test user credentials, and all other necessary means required to effectively conduct the tests.

The work was split into two separate work packages (WPs), defined as:

- **WP1**: White-box pen.-tests & audits against new Small Improvements features
- **WP2**: White-box pen.-tests & audits against Small Improvements Auth features

It should be noted that this security assessment is not the first engagement Cure53 has had with the Small Improvement web application; it has been the target of multiple prior audits. The two most recent of these engagements took place in January 2024 (see project SI-03) and January 2023 (see project SI-02).

The testing preparations were completed by both parties in CW04 of January 2025, ensuring a smooth start for Cure53. Communication throughout the test was managed via a dedicated and shared Slack channel, integrating the teams of both companies with full participation from relevant personnel. This facilitated efficient communication, with minimal clarification needed due to the clear and well-prepared scope. The test proceeded without significant issues, and Cure53 provided regular status updates and shared findings through the Slack channel. Live reporting was not specifically requested for this audit.

Demonstrating good coverage across the scope items, Cure53 identified nine findings, including five security vulnerabilities and four general weaknesses with lower exploitation potential. The moderate number of findings in this engagement is a positive indicator of the Small Improvements web application's security, highlighting continued progress and an overall improvement compared to previous assessments.

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

The absence of any critical vulnerabilities suggests a strong security focus within the development team. However, the testing team identified two High severity vulnerabilities, and unresolved findings from previous testing iterations were also observed. Cure53 emphasizes that all reported issues, even those with low severity ratings, should be appropriately remediated.

The Small Improvements team is to be commended for their swift action in addressing all of the identified vulnerabilities, as well as the majority of general weaknesses, as outlined below. Cure53 then reviewed the implemented fixes as part of their quality assurance process.

Identified Vulnerabilities

- SI-04-001 WP1: Lack of ACL for AI Copilot history (Low) **FIXED**
- SI-04-002 WP2: Login CSRF via improper OAuth state verification (Low) **FIXED**
- SI-04-005 WP1: HTML injection via Copilot bot response (Medium) **FIXED**
- SI-04-008 WP1: DoS in user import via Kallidus integration (High) **FIXED**
- SI-04-009 WP1: Stored XSS in company observer via Copilot bot response (High) **FIXED**

Miscellaneous Issues

- SI-04-003 WP2: Client-side directory traversal via Bamboo iframe (Low) **FIXED**
- SI-04-004 WP1: Permissive regular expressions used in richLinks (Info) **FIXED**
- SI-04-006 WP1: Several CSP bypasses via allow-listed domains (Low) **FIXED**
- SI-04-007 WP1: JavaScript source maps disclose unpacked source code (Info)

Cure53 would like to thank Jesper Carolan Oskarsson, Matt Reid, Laura Sochaczewski, and Sarah Burgess from the Small Improvements Software GmbH team for their excellent project coordination, support and assistance, both before and during this assignment.