Fine penetration tests for fine websites

**Dr.-Ing. Mario Heiderich, Cure53**
Bielefelder Str. 14
D 10709 Berlin
cure53.de · mario@cure53.de

# Executive Summary: Cure53 Security Assessment of Small Improvements, 01.-05.2023

Cure53, Dr.-Ing. M. Heiderich, MSc. F. Fäßler, M. Elrod

Cure53, a Berlin-based IT security consultancy, has completed a comprehensive security assessment of the Small Improvements Web UI & API complex (referred to as *SI-02*). To give some details, this project is the second security-focused collaboration between Cure53 and Small Improvements, with the first (*SI-01*) having taken place in November 2021.

This *SI-02* project was requested by Small Improvements Software GmbH in September 2022 and then scheduled for early spring of the following year, with ample time for preparation on both sides of the requesting and performing parties. Cure53 completed the audit in early to mid January 2023, namely in CW02 and CW03.

A team of four Cure53 testers, all with expertise in line with the project objectives, invested a total of sixteen person-days in this task. For optimal structuring and tracking of tasks, the work was divided into three separate work packages (WPs):

- **WP1**: Penetration tests & code audits of the Small Improvements Web UI
- **WP2**: Penetration tests & code audits of the Small Improvements Backend API
- **WP3**: Penetration tests covering public Small Improvements servers & networks

Cure53 was given access to the application in scope, rolled out on a staging server, as well as test user accounts and all relevant sources. In addition, extensive test support documentation was provided to ensure that the project could be executed within the agreed framework. From the above, it can be concluded that the white-box methodology was used during this inspection.

This methodology was particularly advantageous as the testers had access to the source code of the platform. As is often the case with white-box methodologies, the communication channels between the testers and the internal teams remained open. For this project, a shared Slack channel was used, and Cure53 also provided live reports to the Small Improvements team on the issues found.

The Small Improvements project is a multi-functional platform with a correspondingly large and complex code base. It is worth noting that Cure53 identified only eight security issues affecting the UI and API components of the Small Improvements website.

**Dr.-Ing. Mario Heiderich, Cure53**
Bielefelder Str. 14
D 10709 Berlin
cure53.de · mario@cure53.de

In particular, a very good coverage of the scope was achieved, which strengthens the validity of the overall verdict. Of the seven findings, only three were classified as security vulnerabilities and the remaining four should be considered general weaknesses.

Importantly, the testers were able to confirm no critical severity findings, only *one* high severity issue and no medium severity issues. All of the other findings were in the Low and Informational severity ranges, and were therefore less prominent in terms of severity, and Cure53 must emphasize that the codebase and deployment made a fairly solid impression.

The list of findings did not really contain too many of the so-called 'low hanging fruit' or obvious to spot problems. Instead, almost all of the findings required considerable testing depth and effort to identify, especially the high severity XSS issue. The usual bug patterns, such as SQL injection and the OWASP Top Ten, were not overly prominent or present. Again, this suggests that the development team has many security best practices in place.

As the final stage of this project, in early May 2023, Cure53 undertook and completed a fix verification phase, examining how the scope of small improvements had improved over time and in relation to the communicated findings. In this area, the testing team is pleased to report that all reported vulnerabilities and almost all miscellaneous issues have been properly addressed, and that the recommendations resulting from the assessment have been properly followed.

In conclusion, this early to mid-January 2023 assessment combined with the May 2023 fix verification confirms that the Small Improvements complex is again perceived as strong and stable in terms of security posture. From the perspective of the Cure53 team, appropriate steps have been taken to ensure that good fixes have been developed and are now taking effect on the Small Improvements website UI and backend API.

The measures proposed and largely implemented as a result of this Cure53 assessment were necessary steps to improve the overall security posture of the Small Improvements web application UI & API.

Cure53 would like to thank Peter Crona, Jesper Oskarsson, Matthew Reid and Kolja Lange from the Small Improvements Software GmbH team for their excellent project coordination, support and assistance, both before and during this assignment.