Executive Summary: Cure53 Security Assessment of Small Improvements, November 2021

Cure53, Dr.-Ing. M. Heiderich, MSc. N. Krein, BSc. J. Hector, M. Garrett, Dipl.-Ing. A. Inführ

Cure53, which is a Berlin-based IT security consultancy, completed a comprehensive security assessment of the Small Improvements Web UI & API complex (labeled as *SI-01*).

To give some details, this project marks the first security-centered cooperation between Cure53 and Small Improvements. The project was requested by Small Improvements Software GmbH in early July 2021 and then scheduled for autumn of the same year, with ample time for preparations on both ends of the requesting and executing parties. Cure53 completed the examination in late September 2021, namely in CW39.

A team of five Cure53 testers, all with expertise matching the project's goals, invested a total of twenty person-days into this assignment. For optimal structuring and tracking of tasks, the work was split 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, alongside test-user-accounts, as well as all relevant sources. Additionally, extensive test-supporting documentation was provided to make sure the project can be executed in line with the agreed-upon framework. It can be derived from above that white-box methodology was utilized during this inspection.

This methodology was particularly advantageous since the testers could access the source code of the platform. As is often the case with the white-box methods, communication channels between the testers and the in-house teams remained open. For this project, a Shared Slack Channel was used and Cure53 also delivered live-reports on the spotted issues to the Small Improvements team.

The tested Small Improvements project represents a multi-functional platform with a correspondingly large and complex codebase. It is therefore worth mentioning that Cure53 only managed to identify eight security-relevant issues affecting the Small Improvements website UI and API components.

Notably, a very good coverage of the scope has been accomplished, thus strengthening the validity of the overall verdict. Among the discoveries, five items were classified as security vulnerabilities and three should be seen as general weaknesses.

Importantly, the testers managed to confirm two issues carrying High-scored risks and three issues with Medium-severity levels. Other findings were less prominent in terms of severity and Cure53 must underscore that the codebase an deployment made a rather solid impression.

The list of findings did not really include too many of the so-called 'low-hanging fruit' or obvious to spot problems. Instead, nearly all findings required substantial testing depth and efforts to be identified. The usual bug patterns such as XSS, SQL injection and the OWASP Top Ten flaws were not overly prominent or present. This again hints at the development team having many security best practices in place.

As a final stage of this project in late November 2021, Cure53 engaged in and completed a phase of fix verification, inspecting how the Small Improvements scope has improved over time and in relation to the communicated findings. In this realm, the testing team is happy to report that *all* reported vulnerabilities and miscellaneous issues have been properly addressed, with recommendations stemming from the assessment followed correctly.

To conclude, this late September 2021 assessment combined with the November 2021 fix verification confirm that the Small Improvements complex is now perceivable as strong and stable regarding security posture. From the Cure53 team's perspective, appropriate steps were taken to ensure that good fixes got crafted and now take effect on the Small Improvements Website UI and backend API.

The measures proposed and largely implemented as a result of this Cure53 assessment represented necessary steps towards improving the overall security standing of the Small Improvements web application UI & API.

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