Fine penetration tests for fine websites

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

Cure53 Security Assessment of SonarQube v9.8 & v9.9, Management Summary, 12.2022

Cure53, Dr.-Ing. M. Heiderich, M. Pedhapati, H. Jaiswal

Cure53, a Berlin-based IT security consultancy, completed a security assessment against the SonarQube 9.8 and 9.9 Web UI and backend API, all in winter 2022 (namely in CW50) under the report entitled *SOQ-05*. The engagement's primary objective was to obtain a comprehensive understanding of both the security posture and potential exposure of the software items in scope.

Cure53 previously investigated the SonarQube web application and the findings from these examinations can be found in the reports headlined *SOQ-01*, *SOQ-02, SOQ-03* and *SOQ-04*.

For optimal structuring and tracking of tasks, the work was structured using one dedicated work package (WP):

- **WP1**: White-box pentests against SonarQube 9.8 & 9.9 Web UI and API

It can be derived from above that white-box methodology was utilized. Cure53 was provided with a staging environment, URLs, source codes as well as all other means of access required to complete the tests. Additional documentation was also provided to make sure the project can be executed in line with the agreed-upon framework.

The project progressed effectively on the whole. Sonar's excellent CW49 preparations facilitated a fluid working environment for the testing team. Slack provided an effective platform for cross-team communications during the previous audits, and, as such, was once again utilized to connect all participatory personnel from Sonar and Cure53. The testing team was able to relay regular status updates when necessary, allowing the Sonar team to swiftly and proactively implement mitigation strategies.

Generally speaking, Cure53 achieved very good coverage over all scope items throughout testing. Four security-relevant issues were detected and documented, though positively only one was confirmed as tangible security vulnerability, rated as Low, and the remaining three as general weaknesses with very low impact factors.

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

It needs to further be noted that all of the relevant issues reported by Cure53 have already been addressed and mitigated successfully by the Sonar development team while the test was still ongoing, making sure that the tested versions would not expose any customers to the connected risks.

To provide a conclusory note, this fifth collaborative engagement has resoundingly strengthened the impression gained of Sonar's security implementation. The development team can again be content regarding its accomplishments in providing a soundly-composed SonarQube web UI and backend API. That the application compound was deemed optimally protected against a plethora of web-application attack vectors only corroborates this judgment.

The development team's commitment to not only maintaining security features with due diligence, but also adhering to wider industry best practices, is worthy of praise. Following the mitigation of the remaining three findings offered in the *SOQ-05* report, Cure53 would take great pleasure in confirming that a first-class security posture has been reached for the components in scope.

Cure53 would like to thank Mark Clements, Christophe Levis, Aurélien Poscia, Léo Geoffroy, Damien Urruty, Mathieu Suen, and Emanuele Buda from the SonarSource SA team for their excellent project coordination, support, and assistance, both before and during this assignment.