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 Web & API, Management Summary, 03.2022

Cure53, Dr.-Ing. M. Heiderich, M. Rupp, M. Kinugawa

Cure53, a Berlin-based IT security consultancy, completed a security assessment against the SonarQube Web UI and backend API in spring 2022 (namely CW11) under the report entitled SOQ-03. This engagement's primary objective was to obtain a comprehensive understanding of both the security posture and potential exposure of the SonarQube Web UI, backend, and API. Here, several features were identified and preassigned by the SonarSource development for elevated testing scrutiny.

Following the audit's conclusion, the majority of proposed features were implemented between October 2021 and March 2022. Notably, the previous penetration test conducted by the Cure53 testing team against this scope was held in October 2021 and documented via report SOQ-02. As a result, this assessment primarily focused on the *feature-delta*. In order to issue a reliable verdict regarding the components in scope, the Cure53 team initiated a penetration test and broader security assessment following a white-box methodology, since additional access was granted to all sources for this audit iteration.

Concerning the overall strategy and timeline of this audit, three Cure53 team members were selected to conduct testing based on their individual skill sets, experience, and compatibility with this specific scope. Ten working days were allocated to complete testing; these were held throughout CW11 in March 2022. A dedicated instance rolled out for security testing was utilized for these purposes, and complementary audit support was facilitated via test-user accounts, selected source code-access, and pertinent test-assisting documentation.

Typically, all work for engagements of this nature is divided into work packages (WPs) for optimal structuring and ease of tracking. However, only one work package was deemed necessary for SOQ-03, which reads as follows: *WP1: White-box penetration tests against SonarQube Web UI & API*.

SonarSource's excellent CW10 preparations facilitated a fluid working environment for the testing team. Slack provided an effective platform for cross-team communications during the previous audit held in October 2021, and as such was once again utilized to connect all participatory personnel from SonarSource and Cure53. Here, the testing team was able to relay regular status updates when necessary, allowing the SonarSource team to swiftly and proactively implement mitigation strategies.

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

Generally speaking, Cure53 achieved complete coverage reach over all scope items throughout testing. Six security-relevant issues were detected and documented, though positively only five were confirmed as tangible security vulnerabilities. Furthermore, these findings were not deemed significantly impactful and were only assigned Informational, Low, and Medium severity ratings - the latter of which constituted the highest rating assigned for any issue unearthed during this audit. Considering that the yield of findings has approximately halved since the October review, one can only argue that considerable progress has been made towards bolstering SonarQube's security posture.

The sole remaining item exhibited an almost trivially low exploitation potential and was therefore only categorized as a general weakness. The fact that two of the detected issues reported have already been addressed and mitigated by the SonarSource development team during testing represents the cherry on top of an already superb result.

To provide a conclusory note, this third collaborative engagement has resoundingly strengthened the impression gained of SonarSource's security implementation. The development team should be proud of 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. The fact that Cure53's expertise and rigorous deep-dive techniques could only unearth a maximum Medium severity-rated issue provides irrefutable evidence of a secure framework foundation. Following the mitigation of the findings offered in this report, Cure53 would take great pleasure in confirming that a first-class security posture has been reached for these components in scope.

Cure53 would like to thank Zipeng Wu, Christophe Levis, Tobias Trabelsi, and Mark Clements from the SonarSource SA team for their excellent project coordination, support and assistance, both before and during this assignment.