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, 10.2021

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

Cure53, which is a Berlin-based IT security consultancy, completed another security assessment of the SonarQube Web UI and backend API in autumn 2021 (SOQ-02, CW40). The core aim of the project was to thoroughly examine and evaluate the security posture exposed by the SonarQube Web UI, backend and API, with key focus on several specifically chosen features that have been moved into spotlight by the SonarSource development team.

The majority of those features have been implemented between April and October 2021. Note that the last penetration test executed by Cure53 against this scope (SOQ-01) was performed in April 2021, so this assessment mainly focused on the feature-delta. To be able to issue a reliable verdict about the components in scope, the Cure53 team carried out a penetration test and broader security assessment which followed the grey-box methodology.

In terms of resources, methods and timeline, it should be clarified that four members of the Cure53 team were tasked with this project, based on their skills and expertise matching the examination's goals. They spent ten person-days on the scope, investing time into testing during Calendar Week 40, that is in October 2021. The Cure53 testing team investigated a dedicated instance rolled out for security testing, as well as benefitted from dedicated test-user accounts and additional test-supporting documentation.

For optimal structuring and tracking of tasks, the work was split into just one work package, which reads as follows: Grey-box penetration tests against SonarQube Web UI & API.

The test started on time and moved forward at a speedy pace, thanks in part to all preparations comprehensively completed by SonarSource in CW39. The relevant members of the SonarSource and the Cure53 teams were, just as in April 2021, connected through a shared Slack channel, which had been created by connecting workspaces of the two entities. Cure53 issued regular status updates, therefore making it possible for the SonarSource team to consult on the optimal mitigation strategies.

The coverage reached in this test was very good. While ten security-relevant issues have been spotted and documented, it is important to underline that only three were confirmed as actual security vulnerabilities of medium, low and informational severity.

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

The remaining items - seven of them to be precise – all belong to the array of general weaknesses with very low exploitation potential. In fact, the highest risk-score ascribed to a problem during this project stood at “Info” and the findings – also given their low scores and total number - do not point to any anti-patterns. Further of note is the fact one of the issues has already been been reported as addressed and fixed by the SonarSource development team.

In Cure53’s expert opinion, this project confirmed a very solid security premise at SonarSource for the SonarQube Web UI & backend API. The application compound is currently well-protected against a broad number of web application attack vectors. One can argue that the outcome highlights the development team’s commitment to maintaining security features with due diligence and adherence to best practices.

Despite extensive deep-dives and exemplary coverage toward a plethora of application features by the Cure53 testers, no serious issues beyond “Medium” severity levels were detected.

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