Cure53 Security Assessment of SonarQube Data Center Edition, Management Summary, 04.2021

Cure53, Dr.-Ing. M. Heiderich, N. Hippert, BSc. J. Hector, BSc. C. Kean

Cure53, which is a Berlin-based IT security consultancy, completed a security assessment of the SonarQube DataCenter Edition Software in early 2021. The core aim of the project was to thoroughly examine and evaluate the security posture exposed by the SonarQube DataCenter Edition Software web UI, backend and API, with key focus on several specifically chosen features.

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. In addition, in final phase of the project, the testing team verified fixes that the SonarSource team crafted in response to the identified shortcomings and recommendations proposed by Cure53.

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 fifteen person-days on the scope, investing time into testing during Calendar Week 14, that is in early April 2021. It has been agreed that a so-called grey-box methodology fitted best with the objectives that the SonarSource team wished to achieve with this engagement. 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.

In order to make sure that all aspects of the scope receive proper attention, the work was split into two Work Packages (WPs). In WP1, Cure53 completed grey-box penetration tests against the SonarQube Data Center Web UI and frontend, whereas WP2 was dedicated to the backend and API endpoints of the SonarQube Data Center API & Setup, with the same methodologies deployed.

The test started on time and moved forward at a speedy pace, thanks in part to all preparations comprehensively completed by SonarSource in CW13. The relevant members of the SonarSource and the Cure53 teams were 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 five security-relevant issues have been spotted and documented, it is important to underline that only one was confirmed as an actual security vulnerability of low severity. The remaining items - four of them to be precise - belong to the array of general weaknesses with lower exploitation potential. In fact, the highest risk-score ascribed to a problem during this project stood at "Low" and the findings – also given their low scores and total number - do not point to any anti-patterns. Further of note is the fact that several issues, including the one spotted vulnerability, have already been addressed and verified as fixed by Cure53 in the weeks following the project.

In Cure53's expert opinion, this project confirmed a very solid security premise at SonarSource for the SonarQube DataCenter Edition Software. 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 were detected.

Cure53 would like to thank Belén Pruvost, Christophe Levis, Malena Ebert, Andrea Malagodi, Tobias Trabelsi and Nicolas Peru from the SonarQube team for their excellent project coordination, support and assistance, both before and during this assignment.