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 SonarCloud Web UI & API - Management Summary 11.-12.2021

Cure53, Dr.-Ing. M. Heiderich, MSc. S. Moritz, MSc. D. Weißer, M. Garrett

Cure53, a Berlin-based IT security consultancy, completed a penetration test and security assessment of the SonarCloud complex, spanning the SonarCloud web UI and API, as well as placing an explicit focus on the newly built and integrated SonarCloud features. The work was requested by SonarSource SA and all testing was executed by Cure53 in November 2021, precisely in CW45.

Cure53 has looked at the SonarCloud Web UI and API scope before. Two examinations that happened to date took place in November 2020 (see SOC-01) and May 2021 (see SOC-02). It can be derived that the current project, SOC-03, fits into the longer series of security engagements Cure53 has been commissioned to perform for the SonarSource team.

A team of four Cure53 team-members with skills and expertise matching the technical goals of SonarCloud's scope spent a total of sixteen days on this examination. The so-called white-box methodology was deployed, which means that Cure53 had access to various insights ranging from several environments with the API rolled-out, to test-users, source code and supporting materials about the API documents as well as similar items pertinent to the SonarCloud Web UI & API components.

The project progressed effectively on the whole. All preparations were done in CW44 to foster a smooth transition into the testing phase. Over the course of the engagement, the communications were done using a private, dedicated and shared Slack channel which has already been in place since the former tests. The discussions throughout the test were very good and productive and not many questions had to be asked. The scope was well-prepared and clear, greatly contributing to the fact that no noteworthy roadblocks were encountered during the test.

A total of six findings were spotted, three were classified to be security vulnerabilities and three to be general weaknesses with lower exploitation potential. It needs to be noted that the total number of issues is not overly high, making up for a good result on the whole. Similarly, most of the spotted problems do not appear concerning, but rather reside in the realm of *Medium* or even less threatening finds. This is in line with the outcomes gathered during past projects.

Note however that one Critical flaw was discovered in the third-party *Userback.io* service that is used by SonarCloud to collect feedback, from customers, about beta functions. This is an unexpected and important exception and the problem essentially describes a Blind XSS. This issue was live-reported by the Cure53 team while the test was still in progress. The SonarSource SA team switched off the service and reached out to *Userback.io* immediately to request an assessment and fix to be developed. Shortly after the test was finished, the issue was confirmed by *Userback.io*, a fix was deployed and the Cure53 team was able to verify the successful remediation of the problem.

Another finding was verified as property mitigated by the Cure53 team in mid December 2021, where malicious user input might have lead to a second-order injection and a possible command execution as a result. Similarly to the fix described before, Cure53 was able to have a look at a freshly deployed environment and confirm, that the issue was addressed successfully and can no longer be abused.

To conclude, this assessment of the SonarCloud Web UI & API and their periphery confirmed that the examined application compound is now in a good shape from a security perspective. Following the successful fix verification for the two most relevant issues, the investigated items should be seen as production-ready.