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 Perdoo
Management Summary October 2020

Cure53, Dr.-Ing. M. Heiderich, MSc. N. Krein, BSc. T.-C. “Filedescriptor” Hong, MSc. R. Peraglie

Cure53, which is a Berlin-based IT security consultancy, completed a security assessment of the Perdoo complex in April 2020. The work was specifically requested by Perdoo and entailed both a penetration test and a dedicated audit of the Perdoo source code. Featured as the main test targets were the Perdoo web application, as well as its API and admin backend.

Notably, Cure53 performed a similar examination of the Perdoo scope back in May 2019, which indicates that the project falls into a broader plan of external security assessments. In 2020, core testing was enacted by four members of the Cure53 team selected on the basis of skills and expertise best matching the technical goals set for this project. They investigated the Perdoo scope over the course of twelve person-days. In addition, a fix verification phase occurred later in 2020, with the same personnel involved.

To optimally meet the goals set by Perdoo, Cure53 leveraged white-box methodology during this assignment. The testers had access to the Perdoo application deployed on a staging server. Moreover, all relevant sources were provided alongside documentation. Cure53 was further given an invite URL for admin users, which meant the testers had the capacity to create and invite subsequent users in the frames of ACL testing. An explicit focus was placed on the topic of web, server and API security premise, namely in relation to the main application’s backend API, super-admin panel, as well as GraphQL interface at the actual corporate homepage of Perdoo.

The project started on time and progressed efficiently. The communications during this test were done using Slack; a shared channel was set up between the Perdoo and the Cure53 workspaces, in doing so connecting all involved team members. Cure53 was able to ask questions and deliver status updates to the Perdoo team, enabling good tracking of findings through the requested live-reporting into the GitHub bug tracker established in the private Perdoo API repository.

Eight security-relevant issues negatively affecting the scope of Perdoo were spotted. Six items were classified to be security vulnerabilities of varying risk levels and two problems represented general weaknesses with generally lower exploitation potential. Two discoveries were given

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

High severity ratings due to their possible impact on the Perdoo users. More broadly, the Cure53 team noticed both strengths and weaknesses, yet it needs to be underlined that a substantial portion of the testing budget has been spent on deep-dives and crafting nuanced or creative approaches to bug-hunting. In that sense, the Perdoo team managed to successfully eradicate low-hanging fruit and easily exploitable problems in their compound.

Positive security indicators further related to the exceptionally well-handled input-validation and the chosen language and framework taking care of nearly all issues related to user-controlled input. The Perdoo team has largely averted risks in the realms of SQL injection, Cross-Site Scripting (XSS) and Remote Code Execution. As for the areas that needed improvement, Cure53 observed that mistakes seemed to be driven by oversight. For example, shortcomings in ACL presented attractive ways for attackers wishing to take control over companies, while a faulty request permitted logging of plain-text passwords. Another issue exposed a mistake linked to the incorrect usage of a sanitization function, which ultimately led to a stored XSS vulnerability.

However, the results of a fix verification phase are more than satisfactory. In fact, all but one issue received proper security attention. The remaining problem will be tackled in due course, albeit its limited implications make it an acceptable risk. While great outcome of this phase does not mean that all problems have been fully eliminated, it demonstrates skills and dedication of the Perdoo team in terms of introducing the necessary changes to fend off attacks.

To conclude, the results of this spring 2020 assessment of the Perdoo complex generally indicate a stable and robust state of the security premise, with the developments observed over time evidencing a good direction. Since Cure53 found several exceptions concerning areas that received lower marks overall, the ensuing fix verification made the test clearly beneficial and successful in elevating the overall security premise of Perdoo. Cure53 positively views the achieved result and sees Perdoo as having a lot of potential as a well-designed and largely secure platform.

Dr.-Ing. Mario Heiderich, Cure53, Director, October 15, 2020