Security-Report Meisterplan Application 04.2018

Cure53, Dr.-Ing. M. Heiderich, Dipl.-Ing. A. Inführ, N. Hippert, T.-C. “Filedescriptor” Hong

About Cure53

Cure53 was founded in February 2007 and has since grown to include a small and highly dedicated team of experts versed in solving multifaceted technical challenges in the information security field.

As of 2018, Cure53 works with a total of eighteen consulting researchers, who boast considerable expertise in web security, browser security, cryptography, server security and application security, thus covering a wide yet carefully scoped portfolio of services presented in more detail below.

Introduction

This report summarizes the results of a penetration test against the Meisterplan web application and connected services. The project was carried out by Cure53 in April 2018 and yielded nine security-relevant discoveries.

It should be noted that this is a second security-centered collaboration between the Meisterplan maintainers and Cure53. Specifically, the first investigations of the Meisterplan application was carried out by Cure53 in May 2016 and unveiled fourteen issues relevant from a security-standpoint. Nearly two years later, four testers from the Cure53 team were again tasked with having a detailed look at the Meisterplan application. In terms of other resources, the time budget allocated to the completion of this 2018 project entailed a total of six days, dedicated primarily to remote testing.

Perhaps in part thanks to previous experience of working together, the tests proceeded smoothly and right on schedule. The communications between Cure53 and the in-house Meisterplan team was done via email. The testers had all that they needed to reach good coverage and the email support from the maintainers was nothing short of excellent, prompt and professional. Over the course of the assessment, more relevant vulnerabilities were live-reported to enable quicker responses and good reaction time. Moreover, this strategy was conducive to having Cure53 take a second look at the scope during the testing time frame. In other words, the fix could be verified after being crafted and deployed.

As noted above, all in all nine findings stemmed from this assessment. Compared with the results gathered in 2016, this evidences a much better security posture of the Meisterplan scope in 2018. Nevertheless, five among them were classified as vulnerabilities and three of them were deemed to have rather "*High"* impact on the security of the broader Meisterplan web application. The remaining four issues grouped under the category of general weaknesses were non-exploitable in the current state of the project. Note that one issue was classified to be a false alert after the test was finished.

The closing section of this report contains broader conclusions, offering insights into Cure53's impressions about the tested application as regards the general state of security matters, robustness and presence of threats.

Test Subject

- **Meisterplan Web Application & API**
  - A Meisterplan Test-Server has been made available.
  - Test-Users were made available to Cure53.
  - Test-Accounts for OAuth Login were made available to Cure53.

Test Methodology

The project has followed a classic "black-box testing" methodology, meaning that no access to sources was given to the Cure53 testers, who thus closely resembled hostile attackers operating in real-life scenarios.

The Meisterplan maintainers have made one instance of the web application available to the testers. In addition, several user-accounts were set up, so the Cure53 team did not have to create additional users to facilitate further testing. The administrative area of the application was taken out of scope for this project and no admin user-account was supplied.

Test Plan

The following list of items and attacks were incorporated into the test process and covered by the Cure53 team to assess the security of the Meisterplan platform.

- **Tests against classic web-vulnerabilities and injections**
  - This test iteration was targeted against common web vulnerabilities and injection flaws through GET, POST and other user-controlled parameters and fields.
- **OWASP Top 10 2017 tests, SSRF tests, SOME tests, Mass-Assignment tests**

  - The entire range of OWASP Top 10 tests were performed against the Meisterplan web application to determine, whether the application is appropriately hardened against common and well known web attacks.
- **Strong focus on critical issues such as RCE, LFI and SQLI**
  - A strong focus was put on the tests regarding Remote Code Execution and SQL Injection. Given the nature of the framework in use, it was mandatory to check if the de-serialization of incoming objects is performed in a safe manner.
- **Tests against cryptographic designs and implementations**
  - This test was performed to determine, whether the use of cryptography and randomness employed by the Meisterplan application is flawless. This includes session IDs, password reset tokens, as well as the SSL implementation.
- **Tests against logic bugs and problems regarding authentication**
  - This test aimed towards determining whether the Meisterplan application deals correctly with logic flows such as user authentication and authorization. This also involved interaction between several user accounts.
- **Tests against utilized SQL/NoSQL databases and storage facilities**
  - Additional focus was put on analyzing how secure the server side storage mechanisms of the Meisterplan application are. This primarily included databases, in this test but also the import of data from external sources such as XLS files.
- **Tests against Java-specific vulnerabilities and attacks**
  - The Meisterplan application is run by the Java-driven framework GWT, so several tests were conducted to see if the implementation is secure and if application and runtime-specific issues could be abused.
- **Tests against Privilege Escalation / Privilege Confusion**
  - Similar to the test against logic bugs, the application was checked in depth for behaviors that allow illegitimate interaction between different registered users, password reset processes, privilege assignments and other specifics.
- **Tests against JavaScript- / Framework-specfic security issues and attacks**
  - This test focused on analyzing the JavaScript code deployed by GWT and other frameworks. The goal of such test was mostly to analyze the client side control flows and spot DOMXSS vulnerabilities.
- **Tests against exposed SOAP/JSON APIs and end-points**
  - Finally, the tests involved an analysis of the used REST and RPC APIs that come shipped with GWT to determine if there is any injection or privilege escalation attack potential.

Conclusion

The results of this Cure53 assessment of the Meisterplan web applications are positive. Acting as somewhat of a follow-up to the project carried out by Cure53 on this scope back in 2016, the findings testify to a continued dedication to security and a pervasive climate of security awareness characterizing the Meisterplan entities. From a black-box perspective, four Cure53 testers shared an overall good impression about the security posture of the Meisterplan project.

The uncovered issues were much less severe and significantly more complicated to evoke than their counterpart unveiled two years prior. Both the low number of nine findings (including one false alert), and their types, make it very much noticeable that security assessments have since taken place on the scope. Hardly any classic web vulnerabilities were noted and the vast majority of typical pitfalls seem to be avoided in a reasonably well-working manner.

On the latter, some points need to be raised as regards the discoveries made during this 2018 tests. Noteworthy is, for instance, the problem in the data source feature. In one finding, it was shown that an attacker could craft an XML file capable of stealing files from the Meisterplan server. On the plus side, the vulnerability was live-reported and fixed almost immediately. Less positive, however, was the fact that a variation of the issue was noted despite the deployed repairs. A new variant emerged and could cause a temporary Denial of Service. It is also worth mentioning that an XSS problem in the *Weblink Report* feature was spotted. Sadly, an almost identical vulnerability was exposed during the previous assessment two years ago and reported back in 2016. Once again, a fix was deployed in the present instance soon after the issue has been reported.

Besides testing for standard web vulnerabilities, Cure53 assessed the deployed *GWT* configuration as well. In essence no vulnerability was discovered in this realm but it must be noted that given the complexity of *GWT*, it was difficult to fully test it. A black box approach and a limited time budget should be seen as barriers to achieving a full coverage with reference to the *GWT* issues. Lastly, the deployed OAuth configuration was verified. The Cure53 testing team concluded that the OAuth Login flow appears to be implemented correctly and no security issues were uncovered as far as this aspect was concerned.

To sum up, the Meisterplan team has made tremendous progress with reference to security over the last two years.

Cure53 would like to thank Sebastian Kolb and Jakob Jarosch from the itdesign GmbH team for their excellent project coordination, support and assistance, both before and during this assignment.

Dr.-Ing. Mario Heiderich