Fine penetration tests for fine websites

Dr.-Ing. Mario Heiderich, Cure53
Rudolf Reusch Str. 33
D 10367 Berlin
cure53.de · mario@cure53.de

Security Summary-Report WoSign CA 06.2017

Cure53, Dr.-Ing. M. Heiderich, M. Wege, M. Kinugawa, BSc. D. Weißer, J. Larsson, MSc. N. Krein, N. Hippert, BSc. F. Fäßler

Test Summary

This summary report documents the results of a large-scale penetration test and source code audit of the WoSign suite. The project was carried out by Cure53 in June 2017 and yielded a total of twenty-one security-relevant discoveries. A team of eight senior penetration testers from the Cure53 team performed this assignment, which took an entirety of 40 days to complete.

As for the main scope and rationale of this assessment, it should be emphasized that the test targeted the newly written code base and infrastructure created by the WoSign team. The reasons behind an overhaul of the code base and establishing new infrastructure pertained to a certificate distrust imposed by browser vendors on the WoSign suite in recent past. The main issues raised by the vendors reflected the process of issuing new certificates and suboptimal security within configuration aspects. For the product to be able to regain trust of the key browser vendors, a sequence of steps and procedures needed to be completed. This Cure53 security test constitutes one of the envisaged necessary measures for moving forward.

Particular items placed in scope of this test included four primary objects, namely the Login system, the Buyer system, the WoSign Certificate Management System (CMS), and the related infrastructure. The approach relied on remote-testing with the use of VPNs, which allowed the Cure53 testers significant insights into the relevant parts of the system in scope. The timing of the test was carefully selected as the tested version was basically "one click away" from being turned into a production version. This means that the tested system examined by Cure53 will constitute the core production system. Additional elements of the scope encompassed sources and tarballs made available by WoSign for a thorough and detailed code audit. Finally, some items found in scope were the public websites, the CMS, as well as several tools running in the background (i.e. CA Proxy, CT Proxy and validation system).

All issues that were spotted during the test were live-reported upon discovery via S/MIME encrypted email messages. This way the WoSign had the ability to fix the issues right away and discuss any doubts they might have with the testing team. This logic turned out to be successful, as the WoSign in-house team crafted and deployed fixes for all relevant issues when the test was still ongoing. What is more, by the time of the final

Dr.-Ing. Mario Heiderich, Cure53
Rudolf Reusch Str. 33
D 10367 Berlin
cure53.de · mario@cure53.de

report's rollout, it was also possible for the Cure53 team to engage in re-testing and verify that the issues have been resolved and tackled correctly. This suggests impressive dedication as some issues certainly required major changes in the code base and server setup. For instance the problems with the handling of uploaded files posed one great area of vulnerability patterns, yet have been addressed correctly by now.

Scope & Test Parameters

- **WoSign CMS/Buyer Application, Server & related Infrastructure (~91kLoC)**
- **WoSign CA Proxy System, Server & related Infrastructure (~8kLoC)**
- **WoSign CT Proxy System, Server & related Infrastructure (~3kLoC)**
- **WoSign Validation System (~11kLoC)**
- **WoSign OCSP System (~27kLoC)**

Test Conclusion

The results of this June 2017 Cure53 penetration test and source code audit first and foremost suggest that the security has been moved into the very front and center of the development and priorities at the WoSign entity. Eight senior testers from the Cure53 team were involved in this project's completion over the course of 40 days. Given the recent complete overhaul of both the code base and the infrastructure, bringing in external auditors to assess the WoSign product was a well-thought out business and development strategy. Nevertheless, in spite of how many steps needed to be taken for the WoSign suite to arrive at the current stage, it must be underscored that the current security situation warrants a positive rating.

Even though the number of twenty-two issues discovered during tests may indicate that there is still more work to be done, the complexity and extent of the scope must be taken into account as alleviating factors. What is more, it has to be mentioned that the majority of the unveiled issues did not constitute actual security vulnerabilities.

The WoSign platform could still benefit for enhanced hardening by means of incorporating some novel technologies. The in-house team is encouraged to review and become familiar with the proposals and advantages of, among others, CSP headers, SameSite cookies, Cache Control headers and other browser-based technologies that make the application's users safer.

Dr.-Ing. Mario Heiderich, Cure53
Rudolf Reusch Str. 33
D 10367 Berlin
cure53.de · mario@cure53.de

Returning to the test proceedings, further notable is the fast-paced yet appropriate tackling of the findings. More specifically, WoSign tried and - in most cases - succeeded to fix all reported issues as quickly as possible. Therefore, it had been possible for the Cure53 team to perform a comprehensive fix verification. Only several minor fixes needed to be refined to work as expected as a result of this heightened exchange and considerable efforts. The report would not give a complete picture without mentioning that some infrastructure tests were hard to carry out given the slow connection to the servers in China. However, it must be reiterated that the WoSign Team did all that they could to make the test experience as productive and efficient as possible for the external team.

To conclude, it is clear that security is now a priority at the WoSign entity. The Cure53 team has no doubts that that WoSign has taken the first steps on the correct path of creating a secure web application and backend. Now it is time to make sure that this impression lasts. This requires a shift in the understanding of security as a process rather than a state and entails defense mechanisms that are truly refined. More importantly, it should be underlined that the new security technologies will not be beneficial without being embedded and integrated into the everyday development processes correctly. While some aspects call for further optimization, the baseline is established at an appropriate level.

The WoSign team can now embark on the next stages of the journey towards high-level security of all web-facing features and backend process. Being a CA, it is paramount for WoSign to keep the security and privacy at the forefront of the project’s ultimate goals.

Cure53 would like to thank Richard Wang of WoSign and his team for their excellent project coordination, support and assistance, both before and during this assignment.