Report
Security Assessment

Ultimate Web Tool

August - October 2018
Updated: April 2019

WhiteHats
ethical hackers

Management Summary

WhiteHats performed a security assessment in week 33 - 40 (2018) for GSoftware to identify potential vulnerabilities in the application platform *Ultimate Web Tool* and to suggest remediations. In week 14 - 16 (2019) several findings were reassessed to confirm their resolution.

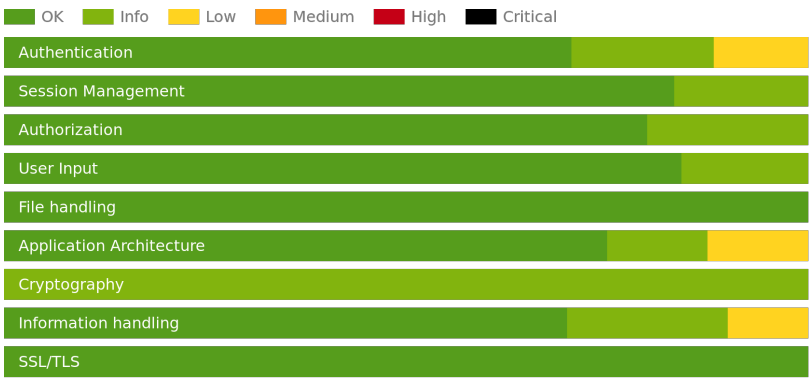
The assessments have been conducted on a local test environment. User credentials for an administrative account were provided and source code was made available for review: a typical whitebox setup. The security assessment covered WhiteHats' standard test protocol, which is based on the OWASP Testing Guide v4. This report details the findings of these assessments.

Result

Ultimate Web Tool is a highly flexible platform for rapid development of applications based on Java and Google Web Toolkit (GWT). GWT facilitates a solid software architecture by allowing both front- and back-end to be developed in the same language which enables code re-use. The codebase is rather extensive and complex because of the generic nature of the platform and due to custom implementations of standard functionality, such as encryption and the database layer.

Initially, multiple vulnerabilities were identified. However, the total number of identified weaknesses was low and it was assumed that most issues could be resolved with limited development effort. The security of the application is partly dependent on a correct configuration of the hosting environment (which was not part of the scope for this assessment). The reassessment confirmed that all but the low priority issues were addressed effectively, resulting in a versatile application with a solid security posture.

The chart below visualizes the security posture after reassessment:



Advice

Implement the remaining suggestions in this report to maximize the resilience of the application against attacks.

Advice third-parties using on-premise installations to conduct a security assessment of their deployments to ensure no vulnerabilities arise from incorrect configuration.

New weaknesses might be introduced when new functionality is developed or issues are addressed. Execute frequent security assessments and deploy automated vulnerability scans to ensure that the application remains as safe as possible.