Code Review

Most security problems are caused by critical vulnerabilities in applications. Code reviews identify security gaps in the source code thus minimizing potential risks.

A code review is something you should seriously consider, especially for security-relevant applications that provide access to sensitive data. The result of this code review is a report that we send you specifying the vulnerabilities analyzed in the source code according to their criticality, as well as detailed suggestions on how to eliminate them.

Our procedures

Depending on the kind of application, we use static or manual analysis methods. In doing so, we either look at a section or at your complete application. We check compliance with recognized secure coding guidelines and best practices. Our methods support PHP, Java, C/C++, Bash, Perl, SQL, JavaScript and Python.

Static analysis

Automated tools are applied in static analysis methods to identify vulnerabilities. The source code of the application is checked without running it. We send you the results in the form of a report generated by the analysis tool.

Manual analysis

Purely static analysis methods reach their limits if errors stem from business logic. This is where the dynamic analysis method is applied by one of our experts.

The tool-based manual analysis identifies the critical areas and is conducted, as far as possible, during the running of the application. After that our expert performs a manual check and an evaluation of the detected vulnerabilities.

Price/Scope

The scope of this service is determined individually. It depends, for example, on the object of the assessment. Please contact us! We would be happy to make you an individual offer.

Our recommendation

A complete code review includes both the static and the manual analysis. Checking of the results by an expert is indispensable to be able to provide a real assessment. We test specifically for errors in the application and business logic by focusing on typical vulnerabilities such as injection, directory traversal, buffer overflow, privilege escalation, etc. Furthermore, we analyze the cryptographic methods used and check the exception handling. This comprehensive testing also enables us to detect errors in the application of control structures.

Code review according to PCI DSS

The PCI Security Standards Council defines a code review requirement. According to requirement 6.3.2 an internally and externally accessible user-defined code is to be checked for vulnerabilities within the context of a code review.

usd - A Strong Partner

Experts know usd AG as one of the leading providers of technical security analyses in Germany. The usd AG security team performs thousands of automated vulnerability scans and hundreds of manual pentests of IT systems and applications every year. usd security experts are committed to the Code of Ethics of the EC Council and have numerous security certifications and extensive experience with international projects. usd AG is one of the few German companies authorised by the PCI Security Standards Council (PCI SSC) to conduct security audits according to the standards PCI DSS, PCI PA-DSS, PCI P2PE and PCI 3DS Europe-wide.

This product sheet will be valid until a new version is released. *Product sheet creation date: 25/05/2018*

usd AG
Frankfurter Straße 233, Haus C1
63263 Neu-Isenburg, Germany | www.usd.de
Phone: +49 6102 8631-190 | E-mail: sales@usd.de
PGP or S/MIME for secure communication