Secure App

More and more providers release apps in order to offer a clear and simplified use of their services via mobile applications. Many consumers are finding it increasingly difficult to identify trusted apps they know handle their data is securely.

We Make Your App Secure

To make the security of your app visible to your users, our security experts check your application manually or tool-based for several factors and provide you with a comprehensive test report including a catalogue of measures, a personal certificate and the usd seal.

Certification of Your App

The certification of your app is based on and in accordance with NIST SP800-163. The requirements of the international security standard of the credit card industry (PCI DSS) and the recommendations of the German Federal Office for Information Security (BSI) and the Open Web Application Security Project (OWASP) are fully considered in the review of your application.

Our Methods

The majority of security problems are caused by critical vulnerabilities in the applications. Especially in the field of mobile applications, security risks are often underestimated, as the possibilities of input appear to be limited. We combine static and dynamic analysis methods in a so-called “whitebox“ approach for your Android or iOS app. Our security experts identify the vulnerabilities while running your application, using the application data as well as the source code of the application provided to them. We check compliance with recognised Secure Coding Guidelines and Best Practices. Our procedures support applications for the Android and iOS platform and thus for Java, Objective-C and Swift.

Mobile App Pentest

usd Pentests offer you the opportunity to have your application individually tested by one of our security experts. To obtain information, he uses professional tools and attempts to exploit vulnerabilities via the mobile application in a targeted, individual and inventive manner. This gives the security expert a deeper insight into the developer view and efficiently detects weaknesses in the application. With the help of the whitebox pentest we deliver reliable results, which we provide you along with concrete suggestions for improvement compiled in a report.

Code Analysis

The analysis of the source code is performed in addition to the Mobile App Pentest. We look at parts of your application and examine the code for vulnerabilities. The review is carried out on the basis of the recognised OWASP procedure model.

How We Proceed

Kick-Off

The preparation of the review takes place in the context of a kick-off meeting remotely by telephone or web conference or, if desired, on your premises with your company's responsible technical and administrative staff. The application to be tested is specified, the necessary access channels are coordinated, contact persons and escalation paths are defined, and the course of the review is discussed in detail.

Manual Research

The application and source code provided in advance are examined for potential weaknesses using static and dynamic analysis methods. Different facets of a mobile application, such as the application server, the data stored locally on the device and side-channel attacks, are considered.

Exploitation

During this phase, our experts attempt to exploit the identified vulnerabilities in order to develop real attack scenarios or access sensitive data. A potential vulnerability can turn out to be false-positive - i.e. upon reexamination, no vulnerability can be detected. Only verified vulnerabilities are included in the final report and classified according to their criticality.

Report

You will receive a comprehensive report comprising an executive summary and a technical report. Criticality of findings and entry risks are evaluated and the vulnerabilities are explained by means of an attack example or code excerpts. A corresponding recommendation for action is also given.

Remediation

In this phase, the identified deviations or weaknesses are eliminated by your company. If required, you will be supported by our experienced consultants.

Optional Verification

You have the option of having us carry out a re-examination after the remediation. We check the effectiveness of your measures and adjust the report accordingly.

Price/Scope

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

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.

Your Personal Certificate

When evaluating your pentest results, we follow the security requirements of the Open Web Application Security Project (OWASP). If your pentest results meet the requirements, we will gladly confirm this in a personal certificate. This way, you can demonstrate your security standards to third parties.

This Product sheet will be valid until a new version is released. *Creation Date: 14.01.2020*

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