MOBILE APP TESTING

Secura

Secura delivers world-class security testing services. One of our most valued services, and the service with the longest history within Secura, is Vulnerability Analysis and Penetration Testing. Secura started testing for customers in the year 2000, meaning that we have nearly two decades of experience. This service includes security assessments of mobile apps.

IN CONTROL WITH SECURA

Secura has worked in information security and privacy for over 18 years. This is why we uniquely understand the challenges that you face like no one else and would be delighted to help you address your information security matters efficiently and thoroughly. We work in the areas of people, processes and technology. For mobile app developers and users, we offer a security assessment of the app's security functionalities and of the relevant parts of the back-end.

MOBILE APP TESTING

Whether our customers are banks, software businesses or government institutions, they all require some form of security testing of their mobile apps. Secura offers professional testing services on all mobile platforms. With over 18 years of working for our clients, our team is equipped with all the knowledge and hands-on experience you would expect.

Mobile applications have an increasingly large impact on our personal lives. The smartphones they run on, have become a trusted companion to most people, and the close proximity to our personal lives mean that vast amounts of personal and private data are processed by these apps.

In contrast to web applications, most mobile applications run in a hybrid environment: part of the application runs on the phone, and another part runs on a back-end server (but not always). On top of that, the user has less control over the data connection that is used, and security functions are an integral part of the device (such as fingerprint or facial scanners). Devices are easily lost and stolen, exposing data on them to attackers.

These factors all contribute to the fact that mobile apps, despite their contained environment, can carry risks to both the user and the app owner (and their back-end). It is therefore important that mobile apps, whether iOS or Android based, are tested for security weaknesses and vulnerabilities before being made available on the market, at every important change and at regular intervals as part of continuous security testing cycles.

The following diagram provides an overview of the various parts that we test during a mobile app testing project.
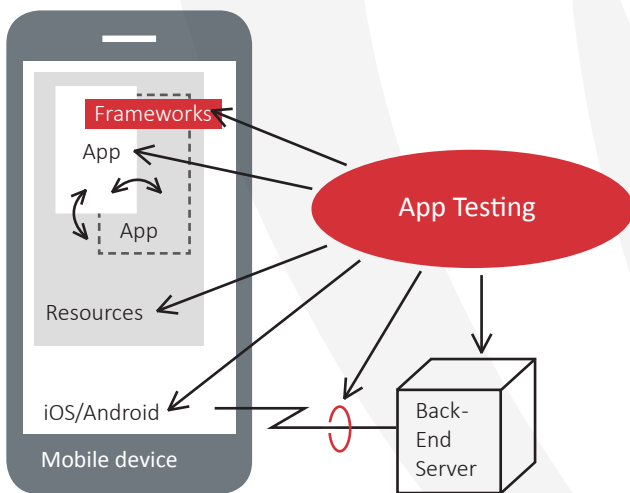
Secura offers her expertise in testing of mobile applications, both on the Android and the iOS platform. Unlike static or behavioral analysis of apps, Secura usually also performs vulnerability analysis and penetration testing on the back-end server. This provides a complete picture of all security weaknesses in the application. Amongst others, we test for issues in:

- App-to-App isolation: can other apps see your data?
- App resource usage: are the correct functions used to secure data locally?
- App functions: passwords, sessions, certificate checks, jailbroken/rooted devices etc.

- Frameworks: what frameworks are used, and how? Do they contain vulnerabilities?
- Communications: how secure is the transport layer to the back-end?
- Back-end functions: how vulnerable is the back-end to traditional attacks, such as business logic failures, authorization bypasses, injection attacks and many others?

In our testing process, we can also investigate the source code of the app, if available. It is worth noting that due to the inherently more closed iOS platform, testing of iOS apps is greatly improved when the source code is available.

Our testing methodology follows the OWASP Mobile Security Testing Guide. This methodology ensures that all relevant topics are tested thoroughly and that all platforms are tested consistently and equally. Secura can test on all currently supported versions of iOS and Android.

All our Vulnerability Analysis and Penetration testing services, including mobile app testing, result in a written report. This report contains an introduction, a management summary describing all the important risks we identified, and a technical section describing the steps we took to identify the risks. This means that in contrast to many other providers, your developers and engineers will be able to repeat our actions using the information in the report, and validate for themselves what we found. As we have dedicated teams running mobile application security assessments all the time, you also have assurance that the major risks are known to you and can now be improved. In our report we tell you what to fix, and with what priority. Our recommendations are actionable and scored: you will know exactly what to do first.