Orange Cyberdefense

SensePost assessments

Mobile

Key benefits

Qualified real-world testing
The SensePost team have made many contributions to projects such as the OWASP Application Security Verification Standard (ASVS) and built custom open source tooling to facilitate mobile application hacking, many of which are referenced in the OWASP Mobile Security Testing Guide. This experience and track record puts us in the ideal position to test applications from a hacker's perspective.

Reduced risk
Comprehensive reviews increase the chance of finding security issues before a malicious actor does.

Systematic approach
We follow industry standard practises to allow for consistently reproducible results as well as custom experience-led activities to push it just a bit farther

Improved application resilience
Testing from an attacker's perspective identifies weaknesses malicious actors look for

Service description

Mobile devices are commonplace in our lives, and for many organisations, mobile applications are an integral part of their digital strategy. Further, with digitalization, organisations have seen a significant rise in mobile applications. A direct consequence of this is an increased attack surface. Attackers exploit vulnerabilities within mobile applications to gain access to backend infrastructure, databases and other related systems.

The SensePost team have presented some of their tooling at international conferences, such as BlackHat USA and DEF CON, and apply their continued research to assessments, culminating a deep and thorough understanding of mobile applications.

Mobile applications come in many forms and while each may have its nuance, the same security principals apply regardless of the technology stack used.

Whether your application is native (written in Java/Kotlin or Objective-C/Swift) or uses a cross platform framework such as Cordova or Ionic, the same security risks are applicable and by extension are tested using the same methodologies. This even applies to simple applications that wrap parts of a web application in a WebView to USSD platforms.

The rise of rapid, agile development processes leveraging CI/CD pipelines has succeeded at scaling software delivery tremendously, but with the risk of scaling errors as well. The SensePost team offers an engagement model that can add value by injecting into that process. In addition to doing the basics with OWASP'S Top 10 and SANS top 25, we offer bespoke assessments tailored around your deployment.

Why Orange Cyberdefense?

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group, providing managed security, managed threat detection & response services to organizations around the globe. As a leading go-to security provider, we strive to protect freedom and build a safer digital society.

We are threat research, intelligence-driven, offering unparalleled access to current and emerging threats. With a 25+ year track record in information security, 250+ researchers & analysts and 16 SOCs distributed across the world and sales and services support in 160 countries, we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

We are proud of our high-end security research unit, thanks to which we publish regularly white papers, articles and tools on cybersecurity which are widely recognised and used throughout the industry and featured at industry conferences including, Infosec, Manchester DTX, RSA, BlackHat and DefCon.

SensePost is an ethical hacking team of Orange Cyberdefense, offering offensive security consulting services and trainings. With a 20-year track record, SensePost is seen as trusted advisors who deliver insight, information and systems to enable our customers to make informed decisions about information security that support their business performance.

With team members that include some of the world's most preeminent cybersecurity experts, SensePost has helped governments and blue-chip companies both review and protect their information security and stay ahead of evolving threats. They are also a prolific publisher of leading research articles and tools on cybersecurity which are widely recognised and used throughout the industry and feature regularly at industry conferences including Black Hat and DefCon.

Key service components

Mobile application assessments, whilst similar in process and methodology to those of application assessments, include a number of mobile-specific tests. They are broken down into two key areas:

Static Analysis
Static analysis generally refers to the inspection of application source code (if provided), or the decompiled / disassembled code obtained by reverse engineering the target application. Focus areas include insecure usages of platform specific API's and or the overall attack surface of the app.

Dynamic Analysis
Dynamic analysis refers to the phase where a target application is executed either on a physical device or within a simulator/emulator, using the apps features just like a user would be expected to. Testing performed in this phase includes platform specific interactions (local file storage, keychain usage etc.) but also interactions with a remote service the application relies on. Runtime binary instrumentation is often used in this phase to test security features of the mobile application itself.

Each of the above approaches results in an extensive testing methodology.