SecurityCompass
ADVISORY

aws Azure Google Cloud

Mobile Penetration Testing

With an experienced, innovative team and an effective, streamlined approach to penetration testing, Security Compass helps you identify vulnerabilities before launch to deliver secure mobile applications.

The Challenges of Securing Mobile Applications

Mobile applications connect users to products and services wherever they are. However, convenience sometimes comes at a cost. Data, and the users that create and manage data, need to be kept safe. Security, however, should not interfere with accessibility and overall user experience.

Devices (hardware/OS) and application choices (software) are individual to each user, presenting unique differences in the environments that applications run in. Though mobile platforms provide users rich customization, this can make it difficult to understand and address core elements required to balance security and usability. Additionally, device jailbreaking and rooting remains a valid means of subverting security features and gaining access to restricted data.

Where Mobile Penetration Testing Fits In

The quick pace of project sprints and high user expectations for the launch of newly developed applications can leave security tasks unfinished or unimplemented. Fitting penetration testing into that schedule can be even more difficult. Not doing so may lead to the launch of an application with unidentified vulnerabilities, which may affect the confidentiality, integrity, and availability of customer data.

With an effective and streamlined penetration testing program, Security Compass can help organizations identify and address these security issues before launch without impacting deadlines.

Our Approach

Security Compass is the industry leader in the world of penetration testing. Our expertise and credentials across multiple platforms and business categories make us your ideal partner in your mobile security journey.

We are certified professionals:

More than **25** of our penetration testers are OSCP, OSWE, or OSCE certified.

We have extensive experience:

We logged more than **77,000** hours of security assessment work in 2019.

We pursue innovation:

Our research department **actively contributes intel** to help the industry identify new security vulnerabilities.

SecurityCompass

Typically, our approach includes the activities outlined below:

- **Business logic analysis:** Understanding how the application is designed to be used by the intended audience. **This perspective is crucial to understanding the end-to-end flow of the data and how the design may be misused.**
- **Identifying the attack surface:** Alongside business logic analysis, **this includes identifying the features** and use cases that may be abused for malicious purposes.
- **Threat modelling:** Enumerating the available features and data workflows helps to **identify and anticipate potential threats** and generate potential solutions.
- **Dynamic testing analysis:** Reviewing application roles and the client-server API communication to identify flaws related to active and **real-time usage of the application.** This phase also includes memory and ephemeral log analysis and review of NFC, Bluetooth, and other transmission of data via radios.
- **Bypassing root/jailbreak detection:** Root access to the device file systems allows for unrestricted access to system files and process information, which may reveal **sensitive data or otherwise bypass built-in system-level controls for data protection**. Additionally, this level of access may allow attackers to create malicious versions of the application, affecting reputation and revenue.
- **Bypassing SSL pinning:** SSL pinning ensures the **communication between the mobile application and the application server is secure**. Since many of the traditional ways of implementing SSL pinning can be bypassed, it is important to review the effectiveness of this feature.
- **Static testing analysis:** This phase helps in identifying **security flaws outside of active and real-time users** of the application. It also helps in identifying insecure coding practices, such as hardcoded credentials or PII and sensitive information in comments. Additionally, this phase targets discovery of obsolete or vulnerable libraries and application permission analysis.
- **Device based testing:** Forensic review of system-level files helps in **identifying instances where sensitive data may be written to disk via logs, user preferences, or database files**. This may help uncover gaps in compliance (e.g. PCI, HIPAA, etc.).

Security Compass

You receive:

Preliminary report: A weekly report that outlines the nature of each vulnerability, its impact to your business and technical environment, and remediation recommendations.

Technical report: A final report outlined in a technical manner to provide security teams with the information required to address identified issues.

Executive summary: This report summarizes the results by outlining high-level risks to the business and provides key trends, strengths, systemic issues, and strategic recommendations.

Industry Leaders in Mobile Penetration Testing

Put our cutting-edge offensive security experience to work for you and learn how prepared your company is to defend against real-world attackers.

Contact Us

Google Cloud aws Azure