secarma
CYBERSECURITY EXPERTS

A Advise C Certify T Test

Mobile Application Security Testing

Mobile applications and the devices upon which they run, have quickly become a core part of everyday life.

With a surge in mobile application development and developers under time pressure to provide new functionality, attacks against mobile applications are a significant concern for businesses.

Who Is It For?

This service is for organisations who develop mobile applications, that handle sensitive data or interact with backend systems. Just as bespoke web applications can create paths in for malicious users, so can mobile applications.

Whether it's an application developed for public use or something internal for you team, we can give an independent view to the risk exposure it causes for your business.

How Can We Help?

Our Mobile Application Security Testing service will find vulnerabilities, prioritise them and recommend remedial actions. This will help you to understand and then mitigate your risks.

For development teams, we will also help you integrate secure development practices into your development lifecycle, baking in security-by-design and improving the security of subsequent applications.

In addition to penetration testing applications, we can also provide code-assisted penetration testing – where we review the code alongside the penetration testing activities to allow for a more efficient security assessment or to allow for a higher level of assurance.

What We Test

Our mobile application testing methodology looks at the system as a whole. We review the application itself, but also the interactions with backend systems such as APIs and data stores. Using the OWASP Mobile Top 10 as a foundation, we review all areas of application functionality, such as:

- **Application logic**

  Abuse of functionality and logical flaws within applications.

- **Authentication**

  Username enumeration, brute force attacks, and credential stuffing.

- **Authorisation**

  Insufficient credential and session management.

- **Cryptography**

  A review of the cryptographic configuration of sensitive data in storage and transit.

- **Code Review**

  We can review code for deprecated or vulnerable functions, as well as reviewing the quality of security implementations.

3 Archway, Birley Fields, Manchester M15 5QJ
0161 513 0960
secarma.com
actnow@secarma.com

Secarma's methodology for Mobile Application Security Testing is informed by common vulnerabilities, such as those on the OWASP Mobile Top 10. Our assessments include the following assessment areas:

Methodology

- **Information Gathering**

  Before the engagement begins, we will map the attack surface of the application and its backend services.

- **Application Mapping**

  We will map the application by navigating through the exposed functionality and APIs to determine the full attack surface.

- **Information Leakage & Verbose Errors**

  Applications that disclose information unintentionally such as through verbose error messages, will be leveraged to gain more insight into technologies and configuration options in use.

  Proof Of Concept & Confirmation

  Where vulnerabilities are discovered a proof of concept exploit will be created to demonstrate the potential business risk. This ensures that false positives are removed by manually confirming and demonstrating all discovered vulnerabilities.

- **Exploitation**

  Exploitation involves discovering weaknesses within exposed applications and leveraging those weaknesses.

Vulnerabilities

- **Business Logic Flaws**

  We attempt to bypass the expected logic flow of the application to demonstrate risk.

- **Platform Usage**

  We'll review the use of platform security features to ensure that permissions and security features are appropriate.

- **Broken Authentication & Access Control**

  Broken authentication includes issues such as weak session management flaws, lack of bruteforce protection, and lack of credential stuffing protection.

- **Broken Cryptography**

  We review how the application stores and transmits data to find cryptographic weaknesses in protocols, ciphers, and implementations.

- **Security Misconfiguration**

  Common and default misconfigurations allow for information exposure or include lack of application hardening through security headers.

- **Code-Assisted Testing**

  If desired, we can review the code alongside the application to allow for more efficient testing or to provide a higher level of assurance.

Assessment can include both unauthenticated and authenticated assessments, to demonstrate the risks of an opportunistic attacker without any access, as well as a rogue user.

3 Archway, Birley Fields, Manchester M15 5QJ
0161 513 0960
secarma.com
actnow@secarma.com