INFOGRAPHIC

NowSecure | OWASP

5 Common OWASP-MASVS Secure Coding Mistakes

Learn about the most prevalent mobile app security oversights and how developers can avoid them.

Recognized around the world, the OWASP Mobile Application Security Verification Standard (MASVS) sets a minimum bar for developers to follow when building high-quality mobile apps. But NowSecure benchmark analysis reveals that 95% of mobile apps fail one or more OWASP MASVS checks, putting organizations at risk of data leaks and damaged brand reputation.

These are some of the prevalent OWASP MASVS vulnerabilities that NowSecure Platform automated mobile application security testing and NowSecure mobile pen testing typically uncover.

95% of mobile apps **fail 1+** OWASP MASVS checks

1 Network Communication

Common Problems

- Lacks network encryption
- Insufficient certificate validation
- Custom or misconfigured network APIs

54% Mobile apps with **insecure network communication**

Secure Coding Best Practices

- Use TLS throughout the app.
- Use platform-provided network configurations (iOS App Transport Security & Android Network Security Configuration).
- Choose platform-provided network APIs and use secure defaults.

2 Platform Interaction

Common Problems

- Uses custom URL schemes
- Loads JavaScript from untrusted sources
- Uses the clipboard for app-to-app communication

47% Mobile apps with **insecure platform interaction**

Secure Coding Best Practices

- Use verified deep links such as Android App Links or iOS Universal Links.
- Validate source of sensitive JavaScript code.
- Use secure platform-provided security IPC mechanisms.

3 Code Quality

Common Problems

- Insecure third-party dependencies
- Insufficient input validation
- App installable on outdated operating systems

43% Mobile apps with **insecure code quality**

Secure Coding Best Practices

- Keep third-party dependencies up to date.
- Validate and sanitize input data.
- Target recent mobile OS versions.

4 Storage

Common Problems

- Stores credentials unencrypted
- Stores sensitive files unencrypted
- Leaks sensitive data to insecure locations

32% Mobile apps with **insecure storage**

Secure Coding Best Practices

- Use the platform-provided key/credential storage.
- Encrypt sensitive files.
- Remove sensitive data storage.

5 Cryptography

Common Problems

- Uses hardcoded keys
- Uses weak cryptographic algorithms
- Uses weak random number generators

22% Mobile apps with **insecure cryptography**

Secure Coding Best Practices

- Use the platform-provided key storage.
- Choose strong, current cryptography.
- Use cryptographically secure PRNG and avoid using non-random sources.

Develop & Release Secure Mobile Apps

Address common mistakes during the development process and ensure your mobile apps meet OWASP MASVS requirements to significantly strengthen mobile application security and privacy.

Upskill developers in secure coding practices with NowSecure Academy training and use NowSecure Platform automated mobile application security testing and NowSecure MASVS pen testing to find and fix security issues prior to release.

© 2024 NowSecure. All Rights Reserved.