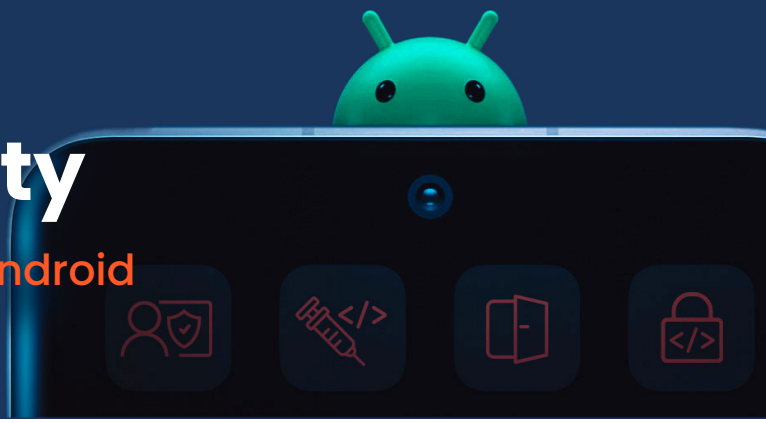
ZIMPERIUM

Mobile App Security

Critical Vulnerability Checklist for Android



Mobile app developers and security engineers must stay vigilant against potential vulnerabilities in the rapidly evolving threat landscape. From safeguarding sensitive data to implementing robust encryption, each item on the list serves as a crucial checkpoint to help ensure your applications are secure, compliant, and resilient. While this checklist aims to highlight key security issues, it's important to recognize that it is not exhaustive. This checklist is an essential starting point in your mobile app security journey.

Instructions for Use

1. Review each item on the checklist before releasing the app.
2. Mark items as complete only when fully addressed and validated.
3. Use this checklist in conjunction with a comprehensive security audit for best results.
4. If any item on the checklist raises concerns, seek further review or remediation steps.

Your Mobile App Security Essentials

Below is a list of questions to help mobile app developers and security engineers evaluate and ensure the security of their mobile apps.

Debug and Development Configuration

- [ ] Have you ensured that debug information is stripped from the release version of the app?
- [ ] Verify the 'android: debuggable' attribute is set to 'false' in the production manifest.

Application Shielding

- [ ] Have you implemented code obfuscation techniques to protect against reverse engineering?
- [ ] Are mechanisms in place to detect and address attempts of code tampering?
- [ ] Have you implemented integrity protection measures to make code and read-only data challenging to modify?

Cloud Storage and API Security

- [ ] Are Amazon S3 buckets secured against unauthorized file and directory listing?
- [ ] Are FirebaseIO and Google Storage configurations preventing world-viewable files?
- [ ] Have you implemented secure storage solutions for API keys to prevent unauthorized access?
- [ ] Do Azure Storage containers restrict anonymous access?

Endpoint and Data Transfer Security

- [ ] Do you regularly audit and secure endpoints to prevent malware distribution risks?
- [ ] Does SSL communication use secure methods, and have you avoided using the getInsecure API?
- [ ] Have you established a proper chain of trust validation for all endpoints?

Input and User Data Protection

- [ ] Have you replaced visible password input types with more secure input methods?
- [ ] Have you prevented saving device identifiers to external storage?

Cryptography and Key Management

- [ ] Are you utilizing secure cryptographic key management, especially for private keys?
- [ ] Have you avoided exposing secret keys in the code and used a secure keystore?
- [ ] Have you determined appropriate sizes for encryption keys to mitigate risk?
- [ ] Are you avoiding encryption schemes with known vulnerabilities?
- [ ] Are cryptographic keys secure even on compromised mobile devices?

Code and Dependency Security

- [ ] Have you ensured there is no inclusion of exploitable code, such as Metasploit code?
- [ ] Is the OpenSSL library updated to a non-vulnerable version?
- [ ] Have you removed references to remote servers with known vulnerabilities, such as FREAK?

Data Storage and Permissions

- [ ] Have you limited access to Content Providers and ensuring they are not exported unless protected by signature-based permissions?
- [ ] Have you audited undeclared permissions to ensure they align with the app's privacy policy?
- [ ] Have you controlled access to content providers and properly configured permission settings?

SQL and Code Injection Protection

- [ ] Are you using parameterized queries or equivalent protections to prevent SQL injection vulnerabilities?

Ad Platforms and Third-party Services

- [ ] Have you reviewed third-party ad platforms for privacy concerns and vulnerabilities?

Backdoor and Unintended Access Prevention

- [ ] Implement safeguards against potential backdoor threats and ensure only secure intent redirection.
- [ ] Are secure intent redirection mechanisms in place?

File Handling and Integrity

- [ ] Have you set up permissions and safeguards to prevent unauthorized file writes or tampering with executable files?

Network Communication

- [ ] Are you enforcing consistency in protocol handling, especially with the Apache HttpClient?
- [ ] Is TrustManager configured to validate server certificates accurately?

Error Handling

- [ ] Are SSL/TLS communication errors handled securely without bypassing them?

Malware Protection

- [ ] Have you reviewed and remediated any malware findings within open-source and third-party components?

Privilege and Role Management

- [ ] Are app resource values used as predicates for important privileges, like admin access, securely managed?

Software Bill of Material

- [ ] Have you reviewed the software bill of materials (SBOM) for any known issues and vulnerabilities within third-party code?

Running on Rooted/Emulated Device

- [ ] Have you implemented measures to identify whether the application runs on an emulator or rooted device?

Free Trial: Get Answers Within Minutes

Ready to take your iOS app security to the next level? Try our free 30-day trial to scan unlimited apps for vulnerabilities and answer security checklist questions in minutes. Ensure your apps meet the highest security standards and start securing them today—risk-free!

Activate Your Free Trial Now

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com
Zimperium, Inc
4055 Valley View, Dallas, TX 75244