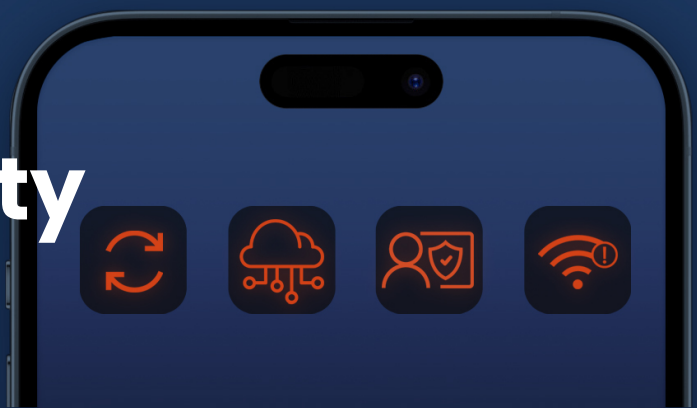
ZIMPERIUM

Mobile App Security

Critical Vulnerability Checklist for iOS



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.

Network Communication

- [ ] Is the app sending any unencrypted communications?
- [ ] Are device details being leaked in outbound communications?
- [ ] Are user details being leaked in outbound communication?
- [ ] Is user location being leaked in outbound communications?
- [ ] Is the app sending data to embargoed countries?
- [ ] Are you using GET parameters to send data?

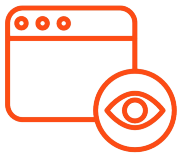
Certificate Validation and Pinning

- [ ] Are you using certificate pinning?
- [ ] Are you using a custom implementation of certificate validation?
- [ ] Is the app using self-signed certificates?

Data Leakage

- [ ] Is contact information being leaked?
- [ ] Is the app leaking calendar events?
- [ ] Is the address book being leaked?
- [ ] Are cookies protected against XSS attacks?
- [ ] Are cookies protected against MITM attacks?
- [ ] Is sensitive data being leaked to system logs?
- [ ] Are Vendor ID and Advertising IDs being leaked?

WebView and URL Schemes



- [ ] What is the current configuration of the WebView in the application, and does it expose any URL schemes beyond the system-defined ones?
- [ ] Are developer-generated URL schemes introducing security risks?
- [ ] Is JavaScript inline execution enabled in this application?

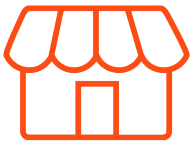
Third-Party and Cloud Dependencies

- [ ] Are third-party libraries not downloading unapproved content?
- [ ] Are cloud storage APIs correctly configured?

Hardware and API Usage

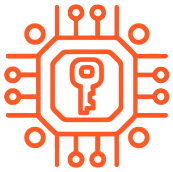
- [ ] Is the app capable of installing another app?
- [ ] Is the app accessing device hardware that is not authorized?
- [ ] Is the app using private APIs?

App Distribution



- [ ] Is the app distribution-signed with a compromised or malicious certificate?
- [ ] Is the app using a distribution signing method intended for in-house usage?

Cryptography and Memory Safety



- [ ] Does the app create a weak encryption key?
- [ ] Is the app allocating a memory region with write and execute permissions?

User Interaction and Consent

- [ ] Does the app initiate network communication without the user's request?

Vulnerability Severity

- [ ] he app has a vulnerability with a CVSS score of Critical.

App Updates

- [ ] Are app updates being delivered securely, and is the update mechanism protected against tampering?

Permissions

- [ ] Does the app ask for excessive permissions that can be abused?

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