QUALYSEC
BEYOND CYBERSECURITY

METHODOLOGY

MOBILE APP PENETRATION TESTING

MOBILE

APPLICATION ASSESSMENT

Qualysec's mobile application assessment methodology locates security weaknesses in mobile applications and infrastructure. These assessments, which can be done with zero, partial, or full knowledge, begin with enumerating and analyzing applications in an organization's infrastructure. Then, the assessment team uses both industry-standard and internal tools, along with expert-guided testing techniques, to discover mobile application security deficiencies. After identifying vulnerabilities, the team manually exploits the cataloged weaknesses to compromise sensitive data, credentials, and systems on both the client device and server side of a mobile deployment. Finally, the assessment concludes with a comprehensive report of all security issues found in the target environment, including detailed remediation recommendations and steps.

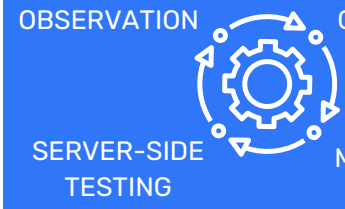
PROCESS OVERVIEW

Phase 1

PRE-ASSESSMENT

Phase 2 &3

DISCOVERY & TESTING



Phase 4

ANALYSIS & REPORTING

PHASE 1 : PRE-ASSESSMENT

To ensure the timely and successful completion of the project, the necessary assessment requirements must be met.

PRE-ASSESSMENT REQUIREMENTS	
ASSETS	Before starting a mobile application assessment, the assessment team requires the following information: • Client and server architecture design documentation • Application documentation and dataflow diagrams • Third-party libraries used in the application, including their respective versions • Mobile version(s) and hardware (e.g., phone, Kindle, etc.) supported • Platform used to distribute the application, or the APK and IPA binary file if none • The Android Studio project or Xcode project and any dependencies, if the mobile application assessment is part of a hybrid application assessment • Server-side source code if applicable • Protocols and processes configured for use within the organization's mobile infrastructure • Two sets of credentials for each application role
OBJECTIVES	Before the work begins, Qualysec collaborates with the client's team to establish the engagement's scope, restrictions, and main objectives, which may include: • Increasing privileges vertically/horizontally • Gaining access to valuable assets, such as restricted resources, account credentials, or sensitive customer data
DUE CARE	The assessment team conducts a review of all pre-assessment information and proposed testing activities to evaluate their potential adverse effects on the mobile application and its underlying API and infrastructure. This review includes identifying all primary and secondary targets.

PHASE 2 : INFORMATION GATHERING

The assessment team performs extensive data collection to evaluate the application and related services employed within the organization's environment.

INFORMATION GATHERINGACTIVITIES	
APPLICATION REGISTRATION/ STARTUP OBSERVATION	The assessment team examines the registration and initial launch process for the mobile application. The team undertakes the following actions: • Installing the application on a rooted device • Extracting the entire application installation directory from the device before first-time startup, using tools such as adb pull (Android), iFunBox (iOS), or SCP (iOS) • Setting up a Man-in-the-Middle (MitM) attack on the device with Burp Suite Pro or a similar intercepting proxy • Launching the application using tools such as Filemon and/or iSpy/Frida on the device • Recording all network traffic from the device with Wireshark and Burp Suite Pro • Monitoring all file access and creation with Filemon and/or iSpy
SERVER-SIDE DISCOVERY	The assessment team conducts scans on all servers related to the mobile application from various perspectives: • Internet and web services that support the application • External connections that the application may utilize The scanning process includes: • Utilizing Burp to scan relevant URLs • Performing standard TCP/UDP port scans • Carrying out other content discovery activities

PHASE 3 : MOBILE PENETRATION TESTING

Once all preparatory requirements have been met and ample information about the environment has been obtained, the assessment team carries out the following actions to discover and exploit vulnerabilities specific to the mobile application.

INFORMATION GATHERING ACTIVITIES	
RUNTIME PATCHES	The team intercepts, alters, and circumvents client-side security measures (such as anti-jailbreaking and anti-debugging) by using hooking, debugging, and runtime patching techniques. Additionally, it examines the internal workings of the application. These runtime attacks are tailored to each specific application.
NETWORK INTERCEPTION	The team intercepts and examines client-server network traffic using a proprietary methodology and toolset. If necessary, the team employs SSL man-in-the-middle attacks to view and manipulate encrypted data streams. The team analyzes the application traffic to detect issues related to sensitive information disclosure, such as Social Security numbers or credit card data.
FILESYSTEM STORAGE	The team scans the device's file system for traces left by the client application, focusing specifically on sensitive information like credentials, personally identifiable information (PII), encryption keys, and any other data that could benefit an attacker.
DEVICE KEYSTORE STORAGE	When feasible, the team tries to retrieve the information stored within the device's keystore/keychain and manually examines the data to identify sensitive information.

BINARY REVERSE ENGINEERING	When necessary, the team reverse-engineers and modifies the client application at the binary level to bypass client-side security measures, such as anti-jailbreak detection or license key verification.

SERVER-SIDE TESTING

API	The assessment team employs standard web API penetration testing methods against identified application server deployments that the mobile client application interacts with. The discovered issues may include: • Skipping authentication and authorization controls • Inserting arbitrary commands • Abusing improper session management • Identifying weaknesses in data security and encryption • Bypassing client-side validation • Abusing query injection and input validation • Utilizing file transfer capabilities • Bypassing application and service logic

PHASE 4 : ANALYSIS AND REPORTING

Qualysec uses internal expertise and industry-standard methodologies to assign severity ratings to vulnerabilities. The severity of each finding is evaluated independently and those with higher ratings have higher technical and business impact with fewer dependencies.

TECHNICAL ANALYSIS ACTIVITIES	
LIKELIHOOD DETERMINATION	For every vulnerability, the assessment team evaluates the probability of it being exploited based on the following factors: • The motivation and capability of the potential threat source • The characteristics of the vulnerability • The presence and effectiveness of countermeasures • Whether physical access to a device and/or jailbreak is needed.
IMPACT ANALYSIS	For each vulnerability that may be successfully exploited, the assessment team examines and evaluates the effects of the exploit on the organization and its customers in terms of confidentiality, integrity, and availability.
SEVERITY DETERMINATION	Qualysec assigns severity ratings using internal expertise and widely-used rating methodologies such as the Open Web Application Security Project (OWASP) and the Common Vulnerability Scoring System (CVSS). The severity of each finding is assessed independently of other findings. Vulnerabilities with a higher severity rating have greater technical and business impact and require fewer dependencies on other weaknesses.

PHASE 5 : REMEDIATION REVIEW (OPTIONAL)

If requested, the assessment team can repeat the scanning and testing of the identified vulnerabilities once the client confirms that the vulnerabilities have been resolved.