Synack Mobile Application Security Testing

If it connects to, or resides on the Internet and is vulnerable, Synack can exploit it. No matter the target, Synack expertly pairs the Synack Red Team (SRT) with Hydra to help organizations find and fix as many security vulnerabilities as possible. When it comes to Mobile Application Security Testing (MAST), the Synack Red Team and Hydra combine various elements of Static (SAST) and Dynamic (DAST) analysis and manual testing techniques to help organizations understand how malicious hackers could compromise their mobile apps and associated APIs.

Hydra Technology
Through proprietary SAST, DAST and vulnerability scanning, Hydra surfaces vulnerabilities and flaws, including those found in common vulnerability frameworks (such as the OWASP Top 10, published CVEs, etc.), and monitors Android and iOS app stores for newly introduced versions or rogue apps. Hydra surfaces all intel to the SRT to further enable their testing efforts.

Synack Red Team (SRT)
Through a variety of manual techniques complemented by Hydra output, hundreds of SRT members from around the globe apply their own unique skills and tradecraft to test mobile applications for any/all variants of vulnerabilities allowed by the engagement scope, including those that automated tools simply cannot detect such as business logic and customized configuration flaws.

Synack’s Operations Team
Synack Operations fully manages all engagements, freeing up your security teams from the endless tasks of vulnerability triage and validation—allowing you to focus efforts instead on efficient, effective vulnerability remediation and risk reduction.

WHAT YOU GET:

Validated, Actionable Reports—Fully verified and prioritized vulnerability reports containing clear descriptions, reproduction steps, and screenshots and/or PoC videos, as well as recommended mitigation and/or remediation steps.

Analytics & Trends—Our real-time analytics provide you with vulnerability trends across all your assets. This coverage can help you spot systemic problems and understand where you can improve your security practices throughout the SDLC.

End-to-End Management & Support—Synack Operations and the SRT serve as the constant support and communication touch points throughout the vulnerability/engagement lifecycle, from the discovery of vulnerabilities, to verifying patches, and everything in between.
1. **Synack Solutions Architects/Project Managers + Clients**—Synack Operations works closely with client teams to determine the mobile application(s) in scope, rules of engagement and objectives, necessary integrations, etc. and subsequently onboards client teams and the application(s) to the Synack platform for testing.

2. **Hydra + Internal Synack Analysis**—Once uploaded to the Synack platform, Synack’s internal Research and Operations team and Hydra begin application testing and analysis, and continuously push information to our SRT to notify them of new intel for further investigation/validation. Preliminary and ongoing analysis includes (but is not limited to):
   - Continuous monitoring of Google Play Android App Store and Apple iOS App Store for newly introduced apps/versions
   - Application disassembly followed by layers of static and dynamic analysis (SAST) & (DAST)
   - Application binary and API functions analyzed using proprietary plugins by Hydra
   - Network capture of activity derived from the running application
   - Device Permission Analysis- what actions can the app perform (Address Book, Microphone, Camera, location services, etc.)?

3. **Synack Red Team (SRT) Testing**—Upon testing “go-live”, all SRT mobile application security experts are granted access to test the mobile app(s) in scope for vulnerabilities to be reported to the Synack Operations team. SRT analysis includes (but is not limited to):
   - A diverse and wide-range of manual testing techniques, procedures, and methodologies
   - Utilization of Hydra & Synack internal teams’ outputs and intel to drive targeted testing efforts towards areas of suspected vulnerabilities and/or newly introduced changes to the application
   - Testing/analysis using common and/or self-built hacker “toolkits”

4. **Synack Operations Management & Coordination**—Synack Operations experts triage and validate/invalidate all incoming SRT vulnerability report submissions and ensure report legitimacy and quality before your teams ever see it. Synack Operations responsibilities include (but are not limited to):
   - Triaging and full manual reproduction of all submissions from the Synack Red Team within 1-business day
   - Filtering all invalid, out-of-scope, and duplicate vulnerability reports, and ensuring all reports contain clear descriptions, severity ratings, reproduction steps, PoC screenshots and/or videos (if applicable), and recommended mitigation/remediation steps
   - Reporting only valid and complete vulnerability reports to clients in a prioritized fashion—over 98% of reports are accepted by clients as “valid, must fix” vulnerabilities
   - Managing all aspects of bounty determination and payouts to SRT members within 24 hrs. post-validation, guaranteed
   - Maintaining ongoing communications with client stakeholders and SRT members (when necessary) and managing patch verification requests once a patch has been deployed

5. **You, the Client**
   - Notified of newly discovered vulnerabilities through updated alerts to the client dashboard (and direct outreach via Synack Operations, when necessary)
   - Verify the validity, severity, and impact of reported vulnerabilities—working with Synack Operations to address any needed clarification or discrepancies (extremely rare)
   - Integration and assignment of vulnerability into your vulnerability management/ remediation workflow
   - Track progress of the vulnerability from “find-to-fix”
   - Once a patch is deployed, request a patch verification through dashboard to alert SRT and Operations to validate whether the patch sufficiently fixes the flaw (if not, revert to step C)