TÜVIT

Mobile Security

Übersichtstabelle Penetrationstests

	☆ SPOT CHECK LEVEL 1	☆☆ REGULAR PENTEST LEVEL 3	☆☆☆ ADVANCED PENTEST LEVEL 3
	Erste Einschätzung Erste Einschätzung des Sicherheitsniveaus im Rahmen einer Stichprobe.	**Für die meisten Anwendungen** Tiefergehende Untersuchung zur Ermittlung der häufigsten auftretenden Risiken bzw. Schwachstellen für Apps.	**Hohes Sicherheitsniveau** Erweiterte, tiefergehende Untersuchung mit mehr Testfällen, bspw. für Anwendungen die geschäftskritische Vorgänge & sensible Daten verarbeiten.
TESTMETHODEN			
Angreifer-Niveau	Simulation eines Angreifers, der einfache Techniken verwendet, um leicht zu findende/ausnutzbare Schwachstellen (Low-Hanging-Fruits) zu ermitteln.	Simulation eines entschlossenen Angreifers, der aktuelle Angriffstechniken aus der Hackerszene anwendet.	Simulation eines entschlossenen & geschickten Angreifers, der aktuelle Angriffstechniken aus der Hackerszene anwendet & die Webanwendung gezielt ins Visier nimmt.
Testmethoden	Automatisierte Tests & Stichprobenartige manuelle Penetrationstests	Automatisierte Tests & manuelle Penetrationstests, die durch automatisierte Tools meist nicht gefunden werden.	Automatisierte Tests & tiefergehende manuelle Penetrationstests, welche durch automatisierte Tools meist nicht gefunden werden.
Testfälle	Stichprobenartige Untersuchung	Es werden ausgewählte Anforderungen aus dem OWASP Mobile Application Verification Standard (MASVS) betrachtet (siehe Testinhalte).	Es werden Anforderungen aus dem OWASP Mobile Application Verification Standard (MASVS) betrachtet (siehe Testinhalte).
ANFORDERUNGEN OWASP MOBILE APPLICATION VERIFICATION STANDARD (MASVS)			
MASVS Level	Level 1 (Stichprobe)	Level 1	Level 1 & 2
Datenspeicherung & Datenschutz (V2)	(✓)	✓	✓
Authentifizierung & Session Management (V4)	(✓)	✓	✓

	☆ SPOT CHECK LEVEL 1	☆☆ REGULAR PENTEST LEVEL 3	☆☆☆ ADVANCED PENTEST LEVEL 3
Netzwerk-kommunikation (V5)	(✓)	✓	✓
Plattform-Interaktion (V6)*	(✓)	✓	✓
Manipulationssicher-heit/Resilienz (V8)		(✓)	✓
Kryptografie (V3)*			✓
Code-Qualität & Build-Einstellungen (V7)*			✓
Architektur, Design & Bedrohungsanalysen (V1)			Optional beauftragbar
BACKEND-SYSTEME/API-ENDPUNKTE			
SSL/TLS Überprüfung	✓	✓	✓
Test auf API-/Anwen-dungsebene (OWASP Top 10 Risiken)	(✓)	(✓)	✓
Portscan		**Basis Portscan** (Top 100 TCP/Top 10 UDP)	**Kompletter Portscan** (alle 65553 TCP/Top 10 UDP)
Schwachstellenscan		**Basis** Schwachstellenscan	**Vollständiger** Schwachstellenscan
BERICHT			
Übersicht aller (auch positiver) Testfälle im Bericht		Optional beauftragbar	Optional beauftragbar
SONSTIGES UND TESTZEITRÄUME			
Re-Test der Findings nach Behebung	Nicht inklusive	Bis zu 5 (innerhalb von 3 Monaten)	Unbegrenzt (innerhalb von 3 Monaten)
Testzeitfenster	≤ 3 Tage	≥ 5 Tage	≥ 10 Tage

* Einige Testfälle sind nur prüfbar sofern auch der Quellcode der App zur Verfügung gestellt wird.

Legende: (✓) Stichprobenartige Untersuchung /Ausgewählte Anforderungen

Hinweis: Die Prüftiefe bei einem App-Pentest ist stark abhängig von den eingesetzten Schutzmechanismen der App. So können Schutzmaßnahmen, welche bspw. eine gerootetes (Android) Gerät oder ein Gerät mit Jailbreak (iOS) erkennen, einzelne Tests erschweren oder unmöglich machen. Auch ein Schutz der Netzwerkkommunikation, bspw. mittels Zertifikat-Pinning, erschwert eine Analyse oder macht diese unmöglich. Aus diesem Grund wird bei Pentests von Apps empfohlen seitens des Auftraggebers eine zweite App-Variante (eine „Debug-App“) mit deaktivierten Schutzmechanismen bereitzustellen.