TÜVIT

Web Application 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.
ALLGEMEIN			
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	Stichprobenartige automatisierte Tests & manuelle Penetrationstests	Automatisierte Tests & manuelle Penetrationstests, die durch automatisierte Tools meist nicht gefunden werden.	Automatisierte Tests & tiefergehende manuelle Penetrationstests, die durch automatisierte Tools meist nicht gefunden werden.
Testfälle	Stichprobenartige Untersuchung	Testfälle, welche die OWASP Top 10 Schwachstellen berücksichtigen & somit die am häufigsten ausgenutzten Sicherheitsrisiken für Webanwendungen enthalten.	Testfälle, welche die OWASP Top 10 Schwachstellen berücksichtigen (siehe Regular Pentest) & zusätzliche, ausgewählte Testfälle/Anforderungen aus dem OWASP Application Security Verification Standard (ASVS)
TESTINHALTE			
Portscans (Webserver)	Basis Portscan (Top 100 TCP)	Erweiterter Portscan (Top 1000 TCP/Top 10 UDP)	Kompletter Portscan (alle 65535 TCP/Top 10 UDP)
Schwachstellenscan (Webserver)		Basis Schwachstellenscan	Vollständiger Schwachstellenscan

	☆ SPOT CHECK LEVEL 1	☆☆ REGULAR PENTEST LEVEL 3	☆☆☆ ADVANCED PENTEST LEVEL 3
SSL/TLS Überprüfung/ Scans (Webserver)	✓	✓	✓
Bereitstellung technischer Anhänge, z.B. der Roh-Ergebnisse der Port- & Schwachstellenscans			✓
BERICHT			
Übersicht aller (auch positiver) Testfälle im Bericht			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