

Dieses Dokument enthält eine Checkliste zur Erstellung von Ausschreibungen oder Beauftragungen von Penetrationstest. Es dient als Richtlinie um alle wichtigen Fragen im Vorfeld zu klären.

Hinweis:



Wenn Sie sich bei einigen Punkten nicht sicher sind, sprechen Sie diese direkt mit möglichen Testern ab. Lassen Sie sich das Vorgehen erklären oder Beispielberichte zeigen, um zu sehen, was sie erwartet.

Einführung enthält:

- ☐ ... was getestet wird (z. B. Web App, Netzwerk, etc.)
- ☐ ... wieso getestet wird (z. B. regulatorische Anforderungen, Test vor Release etc.)
- ☐ ... Zusammenfassung was genau gemacht werden soll (z. B. Test am aktiven Gerät, ohne Code)

Scope enthält:

- ☐ ... was das Testsystem tut (z. B. Banking Anwendung, Unternehmensnetzwerk, Mobile-Game etc.)
- ☐ ... wie das Testsystem aufgebaut ist (z. B. Frontend + Backend + zwei Domänen)
- ☐ ... welche Technologien zum Einsatz kommen (z. B. Node.js, AD, Rust, CAN, TCP/IP)
- ☐ ... was genau von dem Testsystem getestet werden soll (z. B. nur Backend)
- ☐ ... worauf beim Testen der Fokus gelegt werden soll (z. B. Nutzer-Registrierung, Heartbeat Service)
- ☐ ... was nicht getestet werden soll (z. B. nicht das Frontend)
- ☐ ... wie der Tester Zugang zum Testsystem erhält (z. B. Virtuelle Maschine, Dev Umgebung)
- ☐ ... weitere Informationen zum Zugang (z. B. Testaccounts)
- ☐ ... welche zusätzlichen Dokumente bei Teststart bereitgestellt werden (z. B. Softwarearchitektur)

Methodik enthält:

- ☐ ... welche Testumfänge erwartet werden (z. B. vollständiger Black-Box Tests)
- ☐ ... in welchem Umfang Automatisierung von Tests zulässig ist (z. B. nicht für API-Requests)
- ☐ ... welche Standards beim Test eingehalten werden sollen (z. B. OWASP, PTES)

Rules of Engagement enthält:

- ☐ ... welche Arten von Angriffen erlaubt sind (z. B. Wörterbuchangriffe auf Logins)
- ☐ ... welche Arten von Angriffen nicht erlaubt sind (z. B. Denial-of-Service)
- ☐ ... wie die Kommunikation zwischen Tester und Unternehmen aussehen soll (z. B. täglich, einmalig)
- ☐ ... ob und falls ja, wie kritische Findings sofort kommuniziert werden sollen

Anforderungen an den Bericht enthält:

- ☐ ... was in die Managementzusammenfassung gehört (z. B. Zusammenfassung der Aktivitäten, Gesamteinschätzung des Sicherheitszustands, weiteres Vorgehen etc.)
- ☐ ... wie die einzelnen Findings aufgelistet werden sollen (z. B. Beschreibung, Risiko & Impact (z. B. via CVSS), Nachweis, Schritte zum Reproduzieren, Handlungsempfehlung)

Sonstiges enthält:

- ☐ ... wann der Test nach Möglichkeit starten soll
- ☐ ... ob ein Retest durchgeführt werden soll