TÜVRheinland®
Genau. Richtig.

Webapplikationen

Eine Webapplikation (bspw. Onlineshops, Online-Banking, soziale Netzwerke oder Online-Spiele) wird auf Schwachstellen getestet, die von Angreifern häufig für Angriffe ausgenutzt werden oder deren Angriffe erleichtern können. Mit Hilfe von manuellen und automatisierten Tests wird die Webapplikation im zeitlichen Rahmen der Analyse strukturiert auf Schwachstellen untersucht.

Leistungsbeschreibung und Prüfumfang

Im Rahmen eines Penetrationstests wird **eine** Webapplikation, die über eine URL identifiziert wird, auf Schwachstellen hin untersucht, die es einem Angreifer erlauben, die Vertraulichkeit, Integrität oder Verfügbarkeit der Webapplikation oder der darin verarbeiteten Daten zu gefährden.

Der Penetrationstests richtet sich bei uns nach dem OWAS Web Application Security Testing Guide (WSTG) aus und ist in die folgenden Phasen unterteilt:

- Vorgespräch
- Passive Phase
- Aktive Phase
- Berichtserstellung

In einem Vorgespräch wird der Untersuchungsbereich des Penetrationstests definiert und ein möglicher Fokus des Tests diskutiert. Im Vorgespräch werden zur Definition des Untersuchungsbereichs die URLs bzw. IP-Adressen benötigt, unter welchen die Webapplikation erreichbar ist. Ferner wird im Vorgespräch besprochen, ob und welche Zugangsdaten benötigt werden, um den authentifizierten Bereich der Webapplikation analysieren zu können und welche weiteren Punkte für einen effiziente Testdurchführung benötigt werden. Zuletzt wird der genaue Testzeitraum im Vorgespräch vereinbart.

Zum Zeitpunkt des vereinbarten Termins wird der Penetrationstest gestartet. Dieser setzt sich aus drei Phase zusammen und hat unter anderem das Ziel, Schwachstellen zu identifizieren, die unter der OWASP Top 10 bekannt sind:

- A01:2021 -- Broken Access Control
- A02:2021 -- Cryptographic Failures
- A03:2021 -- Injection
- A04:2021 -- Insecure Design
- A05:2021 -- Security Misconfiguration
- A06:2021 -- Vulnerable and Outdated Components
- A07:2021 -- Identification and Authentication Failures
- A08:2021 -- Software and Data Integrity Failures
- A09:2021 -- Security Logging and Monitoring Failures
- A10:2021 -- Server-Side Request Forgery

Zur Identifizierung der Schwachstellen werden die folgenden beiden Phasen durchlaufen:

1. Passive Phase
2. Aktive Phase

Innerhalb der passiven Phase interagiert TÜV Rheinland mit der zu untersuchenden Webapplikation. Hierbei gewinnt TÜV Rheinland einen Überblick über die bereitgestellten fachlichen Funktionen und eingesetzten Technologien der Webapplikation. Die passive Phase wird durch den Einsatz von Tools, wie z.B. Intercepting-Proxies oder Tools zum Enumerieren von Informationen unterstützt. Das Ziel der passiven Phase ist die Ermittlung von möglichst vielen und detaillierten Informationen, die TÜV Rheinland helfen, die Angriffsfläche besser einzuschätzen und im Anschluss möglichst effizient angreifen zu können.

In der aktiven Phase wird die im Untersuchungsbereich befindliche Webapplikation mit Methoden des WSTGs auf Schwachstellen untersucht, welche es einem Angreifer erlauben, die Vertraulichkeit und Integrität der Webapplikation sowie der darüber verarbeiteten Daten zu beeinträchtigen. Diese beinhaltet z. B. die Suche nach sogenannten SQL-Injection-Schwachstellen, die es Angreifern erlauben, Daten aus der angebundenen Datenbank zu extrahieren. Bei dem Paket S werden hierbei ausschließlich automatisierte Tests eingesetzt und es findet kein manuelles Testen statt.

Bei den Paketen M und L wird die Applikation zusätzlich auch manuellen Tests unterzogen, bei denen die Tester neben ihrer Expertise auch ihre Kreativität einfließen lassen, um mögliche Schwachstellen zu identifizieren. Bei den Paketen M und L kann in Abhängigkeit von den bereitgestellten Benutzerzugängen ebenfalls der authentifizierte Bereich der Webapplikation untersucht werden, um sowohl vertikale als auch horizontale Berechtigungsprüfungen durchzuführen. Über die Bereitstellung von unterschiedlichen Benutzern verschiedener Benutzerrollen wird zudem die Testtiefe erhöht (nur Pentest M und L). Basierend auf den identifizierten Schwachstellen werden diese durch TÜV Rheinland ausgenutzt, um weitere Informationen und ggf. einen tiefgehenden Zugriff in die Webapplikation zu erhalten. Sofern erfolgreich, werden die neu gewonnenen Informationen genutzt, um ggf. weitere Schwachstellen zu identifizieren.

! Die Testabdeckung hängt von der Komplexität der Webapplikation und dem investierten Aufwand für den Test ab. Je höher die Anzahl der Testtage, desto mehr Tests und Angriffsvarianten können berücksichtigt werden und desto größer ist die Abdeckung der getesteten Funktionen innerhalb der Webapplikation.

Nach dem Penetrationstest wird ein Bericht erstellt, der aus den folgenden Bestandteilen besteht:

- Management-Summary;
- Definition des Geltungsbereichs (z.B. Auflistung der Zielsysteme);
- Beschreibung der angewandten Methodik;
- Übersichtstabelle der gefundenen Schwachstellen;
- Informationen über die gefundenen Schwachstellen mit allgemeinen Empfehlungen, wie die gefundenen Schwachstellen adressiert werden können;
- Bewertung der Kritikalität des technischen Risikos auf Basis einer vierstufigen Skala: kritisch, hoch, mittel und gering;
- zusätzliche tabellarische Auflistung der gefundenen Schwachstellen (MS-Excel);

Mit der Option „Standard“ werden lediglich Schwachstellen aufgeführt, die unsere Experten im Rahmen des Penetrationstest identifiziert haben. Dies ist beim Pentest „S“ die einzige mögliche Auswahl.

Mit der Option „Standard Plus“ dokumentieren unsere Experten, welche Tests des WSTGs durchgeführt wurden. Wurde ein Test durchgeführt, wird zwischen A*utomatisiert, Manuell* und der Kombination aus beiden unterschieden.

Mit der Option „Premium“ liefern wir zusätzlich zu dem Abschlussbericht der Option „Standard Plus“ einen Kurzbericht, der als Nachweis für die Durchführung eines Penetrationstests genutzt werden kann. Der Kurzbericht umfasst die folgenden Informationen:

- Management-Summary;
- Definition des Geltungsbereichs (z.B. Auflistung der Zielsysteme);
- Beschreibung der angewandten Methodik;
- Auflistung der durchgeführten Tests nach OWASP WSTG.

Zusätzlich prüfen wir auf Wunsch im Rahmen von **einem** Nachtest, ob die identifizierten Schwachstellen von Ihnen erfolgreich behoben wurden.

Optional haben sie die Möglichkeit, dass wir Ihnen die Ergebnisse in einer Ergebnispräsentation darstellen und mit Ihnen gemeinsam die Ergebnisse besprechen.