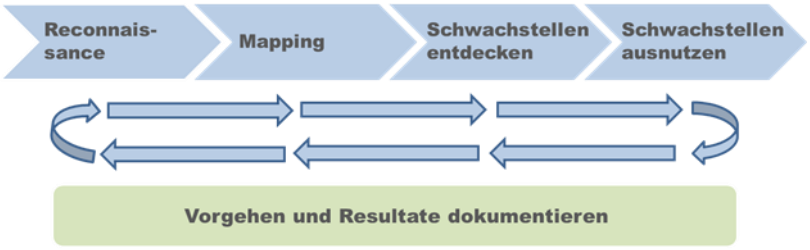
Kurs – Application Penetration Testing

Software ist in vielen Unternehmen heute nicht nur Mittel zum Zweck, sondern oft unternehmenskritisch. Es existieren unzählige Systeme, wo sensitive Daten und Prozesse durch nicht erkannte Software-Schwachstellen einem Risiko ausgesetzt sind.

Dieser Kurs führt die Teilnehmer in die Welt des Application Penetration Testing ein und gibt ihnen einen Einblick in die neusten und am häufigsten angewandten Angriffstechniken.

Kursinhalt

Am ersten Tag werden die Teilnehmer zuerst in die wichtigsten Elemente des eigentlichen Penetration Testing eingeführt und lernen die nötigen Hilfsmittel kennen.



Der Hauptteil bezieht sich auf die OWASP Top 10 und deren Anwendung als Penetration Tester.

Übersicht der Top 10 OWASP Themengebiete:

- A1: Injection
- A2: Cross-Site Scripting (XSS)
- A3: Broken Authentication and Session Management
- A4: Insecure Direct Object References
- A5: Cross-Site Request Forgery (CSRF)
- A6: Security Misconfiguration
- A7: Insecure Cryptographic Storage
- A8: Failure to Restrict URL Access
- A9: Insufficient Transport Layer Protection
- A10: Unvalidated Redirects and Forwards

In den drei Kurstagen werden diese Themen jeweils nacheinander wie folgt gemeinsam erarbeitet:

- Theorieteil
- Hacking (Hands-on)
- Besprechung Hands-on

Abschluss: Hacking-Challenge

Der Abschluss des Kurses bildet eine Hacking Challenge, bei der die Teilnehmer an einer realen Applikation ihr neues Wissen unter Beweis stellen können.

Teilnehmer

Teilnehmer dieses Kurses sind:

- Penetration Tester
- Software Entwickler
- Technische Mitarbeiter

Max. Anzahl Teilnehmer: 10

Ihr Vorteil

- Sie erhalten mit wenig Zeitaufwand eine Einführung in das Thema
- Erhöht das Sicherheitsbewusstsein
- Ermöglicht es Ihnen, selber einfache Application Penetration Tests durchzuführen

Kursort & Zeiten

- Raum Zürich
- Kurszeiten: 9:00 – 17:00
- Interne Kurse auf Anfrage

Dauer & Preis

- 3-tägiger Kurs
- CHF 3'450.- (pro Teilnehmer, exkl. MwSt.)
- Inkl. Verpflegung

SCHULUNGEN

Kursinhalt

Protect7
your application security experts

Tag 1

Allgemeine Grundlagen	HTTP, Proxies
Programmiersprachen	Allgemein, Javascript, Python
A1 – Injection	SQL, LDAP, Command, CRLF, Code ...

Tag 2

A2 – Broken Authentication and Session Management
A3 – Cross Site Scripting
A4 – Insecure Direct Object Reference
A5 – Security Misconfiguration
A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control

Tag 3

A8 – Cross Site Request Forgery
A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards
XML - Attacks
Hacking Challenge

SCHULUNGEN