

Web Application Security – Foundation («SWO»)

Entwickeln Sie sichere Websites. In diesem Training lernen Sie OWASP Top 10 kennen, um damit offensive Angriffstechniken auszuführen und Schwachstellen in Ihren (Web-)Applikationen zu finden.

Dauer: 2 Tage

Preis: 2'100.– zzgl. 8.1% MWST

Kursdokumente: Digicomp Kursunterlagen (digital)

Inhalt

Studien belegen, dass über 90% aller Webapplikationen schwerwiegende Sicherheitsmängel aufweisen, obwohl für die meisten Angriffsarten wirkungsvolle Gegenmassnahmen existieren. Schwachstellen sind meist in Architektur und Design, in der Anwendungslogik, im Programmcode, in 3rd-Party Libraries oder in Deployment und Konfiguration zu finden.

Auf Basis der [OWASP Top 10](#) lernen Sie die aktuellen Angriffsmethoden auf (Web-)Applikationen kennen und lernen, wie wirkungsvolle Schutzmassnahmen ergriffen werden sollten:

- 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- A06:2021-Vulnerable and Outdated Components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

Key Learnings

- Wissen, dass Sie zur Verschwiegenheit, Vertraulichkeit und Geheimhaltung gegenüber dem Arbeitgeber und den Kunden verpflichtet sind
- Berücksichtigung der Kunden-Bedürfnisse (intern wie extern)
- Sicherstellen der Cyber-Resilienz im Austausch mit dem Kunden
- Auseinandersetzen mit verschiedenen möglichen Bedrohungsszenarien
- Verwenden des OWASP (insbesondere der OWASP Top 10) als Hilfsmittel zur Durchführung offensiver Angriffstechniken, um Schwachstellen in (Web-)Anwendungen zu finden
- Installieren, Konfigurieren und Betreiben von Tools zum Auffinden und Analysieren von Schwachstellen sowie Durchführen von Web Application Penetration Tests
- Anwenden Ihres Fachwissens zur Unterstützung interner und externer Revisoren bei der Durchführung von Security Audits
- Entwickeln eines Grundverständnisses für die Prinzipien sicherer Softwareentwicklung

Zielpublikum

Dieser Kurs richtet sich an Softwareentwickler und -tester, Webmaster, -entwickler und -publisher, Systemingenieure und Administratoren, CISOs und IT-Security-Verantwortliche.

Anforderungen

Grundkenntnisse in der Web Anwendungsentwicklung, Kenntnisse im Umgang mit Webservern, Kenntnisse grundlegender Webtechnologien wie HTML und Javascript werden vorausgesetzt.

- [Einführung in JavaScript \(«ISC»\)](#)

Weiterführende Kurse

- [CAS Cyber Security Expert \(«CSECAS»\)](#)
- [Advanced Penetration Tester \(«ADVPEN»\)](#)
- [Basic Penetration Tester \(«BASPEN»\)](#)
- [Prüfung zum Basic Penetration Tester](#)

Haben Sie Fragen oder möchten Sie einen Firmenkurs buchen?

Wir beraten Sie gerne unter 044 447 21 21 oder info@digicomp.ch. Detaillierte Infos zu den Terminen finden Sie unter www.digicomp.ch/weiterbildung-security/cyber-security-defense/kurs-web-application-security-foundation