Web Application Security Deep Dive («SWOA»)

Sie betrachten Sicherheitsrisiken Ihrer Website auf der Basis der OWASP10. Sie diskutieren aktuelle Cyber Attacken mit Blick auf Risiken & Schutzmassnahmen. Mit Hilfe der Labs lernen Sie Angriffstools zu nutzen, um Webanwendungen auf Sicherheit zu prüfen.

Dauer: 3 Tage
Preis: 3'000.– zzgl. 8.1% MWST
Kursdokumente: Digicomp Kursunterlagen (digital)

Inhalt

Tag 1 und 2

Studien zeigen, dass mehr als 90% aller Webanwendungen gravierende Sicherheitsmängel aufweisen, obwohl für die meisten Angriffsarten wirksame Gegenmassnahmen existieren. Die Schwachstellen liegen meist in Architektur und Design, in der Anwendungslogik, im Programmcode, in 3rd-Party-Libraries oder in Deployment und Konfiguration.

Anhand der OWASP Top 10 lernen Sie aktuelle Angriffsmethoden auf (Web-)Anwendungen kennen und erfahren, wie Sie sich effektiv schützen können:

- 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- A06:2021-Vulnerable and Outdated Components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

Tag 3

- Zusammenfassung OWASP Top 10
- Advanced Angriffe auf Web Applikationen
  - Umgehen von 2FA anhand eines praktischen Beispiels
  - XSS und Clickjacking
  - Angriffe auf OAuth 2.0
  - Parameter Pollution
  - Web Cache Poisoning
  - Template Injection
  - Angriffe auf JWT
  - Request Smuggling
  - Server Side Prototype Pollution
  - DOM Based Vulnerabilities
- Sichere APIs
  - Einführung in die OWASP API Top 10:2019
- Guideline zur gezielten Vorbereitung auf die BSCP-Prüfung

Key Learnings

- Wissen, dass Sie zur Verschwiegenheit, Vertraulichkeit und Geheimhaltung gegenüber dem Arbeitgeber und den Kunden verpflichtet sind
- Analysieren und Entwickeln von neuen Angriffsmethoden und Attack-Simulationen
- Berücksichtigen der Kunden-Bedürfnisse (intern wie extern)
- Gewährleisten der Cyber-Resilienz des Kunden
- Erklären komplexer Angriffe auf Web-Applikationen und Durchführen von Proof-of-Concept-Angriffen zur aktiven Ausnutzung von Schwachstellen und Sicherheitslücken
- Wissen, wie offensive Techniken eingesetzt werden, um komplexe Schwachstellen und Sicherheitslücken in Systemen, Anwendungen oder Infrastrukturen von Unternehmen verschiedener Branchen zu finden.
- Erstellen und Überprüfen von konkreten Weisungen, Standards, Baselines, Richtlinien und Betriebsdokumentationen, abgeleitet aus branchen- und marktüblichen Standards (BSI, NIST, ISO, andere)
- Durchführen komplexer Sicherheitsanalysen (Web Application Penetration Tests) und Dokumentieren der Ergebnisse in Form eines Berichtes mit Feststellungen und Handlungsempfehlungen und Integrieren der Erkenntnisse aus den Analysen in die Praxis
- Einsetzen Ihrer Fachkenntnisse zur Unterstützung interner und externer Auditoren bei der Durchführung von Security Audits und selbstständiges Durchführen von Teilaufgaben im Rahmen von Audits

Methodik & Didaktik

Das Training hat einen hohen Hands-On-Anteil gepaart mit gezielten Theorie-Inputs. Die Übungen werden anhand von Fallstudien behandelt.

Zielpublikum

Dieser Kurs richtet sich an Security-Experten und angehende 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/kurspaket-web-application-security-deep-dive