Web Application Security Deep Dive («SWOA»)

You will look at the security risks of your website based on OWASP10. You will discuss recent cyber-attacks in terms of risks and mitigations. Using the labs, you will learn how to use attack tools to test web applications for security.

Duration: 3 days
Price: 3'000.–
Course documents: Digicomp courseware (digital)

Content

Day 1 and 2

Studies show that more than 90% of web applications have serious security flaws, even though effective countermeasures exist for most types of attacks. The vulnerabilities are usually in the architecture and design, application logic, code, third-party libraries, or deployment and configuration.

With the help of the OWASP Top 10, you will learn about the current attack methods against (web) applications and how you can protect yourself effectively:

- 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- A06:2021-Vulnerable and Outdated Components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

Day 3

- Summary OWASP Top 10
- Advanced Web Application Attacks
  - Bypassing 2FA with a practical example
  - XSS and Clickjacking
  - OAuth 2.0 Attacks
  - Parameter Poisoning
  - Web cache poisoning
  - Template Injection
  - JWT attacks
  - Request Smuggling
  - Server Side Prototype Pollution
  - DOM-based vulnerabilities
- Secure APIs
  - Introduction to OWASP API Top 10:2019
- How to prepare for the BSCP exam

Key Learnings

- Understanding that you are bound to secrecy, confidentiality, and non-disclosure to your employer and customers
- Analyzing and developing new attack methods and attack simulations
- Considering the needs of the customer (internal and external)
- Ensuring the client's cyber resilience
- Explaining complex web application attacks and performing proof-of-concept attacks to actively exploit vulnerabilities and security gaps
- Understanding how offensive techniques are used to find complex vulnerabilities and security gaps in the systems, applications, or infrastructure of organizations in various industries
- Creating and reviewing specific policies, standards, baselines, guidelines, and operational documentation derived from industry and market standards (BSI, NIST, ISO, others)
- Performing complex security analyses (web application penetration tests) and documenting the results in the form of a report with findings and recommendations for action, as well as integrating the findings from the analyses into practice
- Using your knowledge to support internal and external auditors in conducting security audits, and independently performing subtasks as part of audits

Methodology & didactics

The training has a high hands-on component coupled with targeted theoretical input. Exercises are based on case studies.

Target audience

This course is aimed at security professionals and aspiring penetration testers.

Any questions?

We are happy to advise you on +41 44 447 21 21 or info@digicomp.ch. You can find detailed information about dates on www.digicomp.ch/courses-security/cyber-security-defense/course-package-web-application-security-deep-dive