Introduction to application security

Course: **00176**
Filter: **Beginner**
Duration: **2 days**
Category:: **Cyber Security**
Price: **1450,00 €**

About Course

The aim of this technical training is to instruct programmers in the rules to be to follow in terms of application protection. The omnipresence of AI and the proliferation of cyber-attacks means that security needs to be built in right from the application design phase. design phase. Through practical exercises, participants will acquire the knowledge they need to to detect vulnerabilities and implement countermeasures

What you'll learn

- Understand the importance of security by design
- Identify potential application vulnerabilities
- See the different approaches that attackers use in order to better counter them
- Experiment with vulnerabilities using exercises in a controlled environment

Targeted audience

- Anyone working in application, web or local development and software tools that can open access doors
- Architects and managers of development teams
- Anyone wishing to add a high-demand expertise to their CV
- Anyone with an interest in cyber security in general

Pre-requisites

- Understanding development vocabulary
- Basic programming skills recommended
- A certain level of comfort with Docker for setting up the lab environment

Curriculum

Module 1: Introduction to application security and setting up the environment

- What is OSINT and how attackers use it to gather information about your systems
- What is BURP?
- Exercise: brute force login

Module 2: OWASP TOP-10 - Broken Access Control

- Explanation of the flaw
- Exercise: finding exposed URLs where access is not properly controlled in a web application
- Mitigation methods

Module 3: OWASP TOP-10 - Cryptographies

- Explanation of the di?erent cryptographic attacks
- Exercise: Identification of a password hash in the application and ‘cracking’ using common Internet tools » à l’aide d’outils communs sur Internet
- Explanation of the Padding Oracle flaw and exercise
- Mitigation methods and best practices

Module 4: OWASP TOP-10- Injection

- Explanation of the di?erent types of XSS
- Exercise: Performing a DOM XSS reflection
- Exercise : Performing a Stored XSS
- Exercice : Capturer le jeton d’authentification d’un administrateur en XSS
- CSRF concepts
- Mitigations

- SQL Injection: Explaining the attack
- Awareness and exercise in taking control of a database with sqlmap
- Mitigations and best practices
- Exercise: Exfiltration and password cracking
- Command injection: Explanation
- Command injection and reverse shell exercise
- Mitigation methods and best practices
- Example of XXE
- Exercise on XXE, data exfiltration
- Mitigation methods and best practices

Module 5: OWASP TOP10 – Security misconfiguration

- Explanation of the subject
- Examples of problems and threat scenarios
- Mitigation methods and best practices
- Notions of pipeline, source code management, cloud

Module 6: OWASP TOP10 - Vulnerable and/or obsolete components

- Identifying obsolete and vulnerable components
- Exercise: Exploiting a vulnerable module for data exfiltration
- Mitigation methods (integration of identification modules into the pipeline)

Module 7: OWASP TOP10 - Authentication or authorisation problems

- Explanation of the subject
- Presentation of the OWASP cheatsheet for best practices
- Exploiting secret questions and password bypassing
- Mitigation methods and best practices

Module 8: OWASP TOP10 – Software and Data Integrity Failures

- Explanation of the subject
- Exercise: reverse shell based on a serialization flaw in Python
- Mitigation methods and best practices

Module 9: OWASP TOP10 – SSRF

- Explanation of SSRF
- Lesson 2: Exercise: Displaying an image available only from the Docker infrastructure from outside Docker
- Means of mitigation and best practices

Module 10: Conclusion

- Notions d’architecture applicative sécuritaire
- Récapitulation des failles vues pendant le cours
- Importance de la sécurité des applications