Module: Web application security

Do you want to secure your web applications? This training teaches you how to detect attacks and secure web applications. In particular, you will be able to: know the different attacks and protect yourself against them, secure access and sessions, implement good practices in terms of web security.

Prerequisites : Good knowledge of the web, programming language.

Ways to take this course:	Online Instructor Led Online self-paced Video On Demand
Video conference tool :	ZOOM
Duration :	21 H (3 days)

OUTLINE

Introduction

Overview of web security
Terminology, standards and laws
Think tanks about security
WASC typology
Top 10 OWASP

HTTP protocol

Client/server, Ajax and DOM
Headers
Status codes
HTTP methods
Opening on Burp Suite

Web application vulnerabilities

Injections: SQL, LDAP, code...
URL protection
Insecure storage
Cross Site Scripting (XSS)
Session and authentication
Exposing sensitive data
CSRF attack, phishing
Vulnerabilities on configurations
DDOS-like attacks. Insecure deserialization
Vulnerable components
Site analysis with the OWASP ZAP tool

Security-related technologies

Firewalls: tools, techniques
HTTP request filters. Message imprint
SHA-x and MD5 algorithms. Digital signature
Public key/ private key
Key chest and trust chest
Certificate authorities. Data encryption
AES and RSA algorithms. SSL, TLS protocols
PKI, X509 certificates. HTTP authentication
Certificate authentication
Network frame analyzer
HTTP scanning proxy

Secure Web Applications

Re-post data
Timeout and disconnection
Hide URLs. Data validation
Cookies and digital certificates
Session ID and transaction token
Session stealing (MITM proxy). Diversion
XSS or Cross Site Scripting. Using direct references
CSRF (Anti-CSRF Token). DBMS Access security
SQL / Code injection. Using JavaScript
Escaping HTML tags
Authentication with captcha
Brute force attacks: cewl + Cupp.py
Passwords: salting, etc.
Access control, privileges
Securing a file upload

Module: Web application security

Do you want to secure your web applications? This training teaches you how to detect attacks and secure web applications. In particular, you will be able to: know the different attacks and protect yourself against them, secure access and sessions, implement good practices in terms of web security.

Prerequisites : Good knowledge of the web, programming language.

Ways to take this course:	Online Instructor Led Online self-paced Video On Demand
Video conference tool :	ZOOM
Duration :	21 H (3 days)

OUTLINE

Secure Web Services

SOAP, REST, gRPC
Authentication
Authorization
Confidentiality and integrity
Security: OAUTH, SAML, Token
Web Services security

Control web application security

Penetration test, Burp suite
Security audit
Vulnerability scanners
Efficient technology watch
Security incident reporting
Mobile devices: threats and risks
Mobile Hacking Tools
Mobiles: security