CORSO WAPT:
WEB APPLICATION PENETRATION TESTING

Durata: 24 ore

PROGRAMMA

MODULO 1: INTRODUZIONE ALLA SOFTWARE SECURITY

- Proprietà di sicurezza (CIA)
- Vulnerabilità del Software
- Rischio di sicurezza digitale
- Attività di testing
- Il sistema CVE
- Il sistema CVSS
- OWASP
- Imparare tramite le CTF

MODULO 2: INTRODUZIONE AL WAPT

- Ripasso protocollo HTTP
- Configurazione del proxy HTTP
- Deployment di applicazioni vulnerabili
- Utilizzo di Burp Suite

MODULO 3: WAPT TESTING

- Information Disclosure
- Injection Vulnerabilities
- Authentication
- Authorization
- Session Management
- Business Logic Vulnerabilities
- Validation Vulnerabilities
- Cryptography
- Insecure Configuration

MODULO 4: WAPT REPORT WRITING

- Come scrivere un PoC
- Come organizzare un report

Scopri di più sul corso WAPT.

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO WAPT:
WEB APPLICATION PENETRATION TESTING

Durata: 24 ore

OVERVIEW DEL CORSO

Il corso Web Application Penetration Testing (WAPT) è pensato per chi vuole andare oltre la teoria della sicurezza e sperimentare in prima persona come avvengono gli attacchi alle applicazioni web.
Attraverso un approccio pratico e guidato, i partecipanti avranno accesso a un ambiente di laboratorio che simula scenari reali, lavorando su un'applicazione vulnerabile scritta in C# con .NET Core. Durante le esercitazioni sarà possibile mettere alla prova metodologie e strumenti utilizzati dai penetration tester professionisti, come Burp Suite, ripercorrendo le fasi tipiche di un test offensivo e imparando a individuare più di 40 vulnerabilità differenti.
Il percorso non si limita alla scoperta delle vulnerabilità: ogni esercitazione è accompagnata da riflessioni su rischi, impatti e possibili mitigazioni, con riferimenti agli standard di settore (OWASP, CVE, CVSS). In questo modo i partecipanti svilupperanno non solo la capacità di eseguire test tecnici, ma anche la consapevolezza di come presentare i risultati in maniera chiara e professionale, redigendo report e Proof of Concept (PoC) che possano essere condivisi con sviluppatori, responsabili di progetto e management.

A CHI È RIVOLTO IL CORSO?

Il corso è rivolto a:

- Software Architect
- Technical Lead
- Software Developer (Fullstack, Backend, Frontend)
- DevOps EngineerQA Tester
- E tutti professionisti tecnici coinvolti nello sviluppo, test e gestione di software.

COSA SAPRAI FARE ALLA FINE DEL CORSO?

Al termine del corso i partecipanti saranno in grado di:

- Comprendere i concetti fondamentali della sicurezza del software e del rischio digitale.
- Utilizzare Burp Suite e altri tool per l'analisi del traffico HTTP e l'intercettazione delle richieste.
- Eseguire un penetration test completo su un'applicazione web vulnerabile in .NET Core.
- Identificare e sfruttare vulnerabilità comuni e avanzate (SQLi, XSS, CSRF, IDOR, privilege escalation, misconfigurazioni, ecc.).
- Riconoscere problematiche legate ad autenticazione, autorizzazione e gestione delle sessioni.
- Valutare la severità delle vulnerabilità con CVSS e collocarle nel contesto OWASP Top 10.
- Documentare correttamente le evidenze tecniche attraverso Proof of Concept riproducibili.
- Strutturare un report di penetration test professionale, distinguendo tra dettagli tecnici e sintesi per il management.
- Collegare le vulnerabilità rilevate alle misure di mitigazione e alle buone pratiche di sviluppo sicuro.

CONTATTI

info@nexsys.it

www.nexsys.it