SETC Training Corporate Logo

IT Security Training: Securing Web Applications (PROSECP, 4 jours)

Description

This IT security training course provides participants with a complete exploration of web application security. Participants are first introduced to the essential concepts of open-source intelligence and social engineering while they begin to understand the hacker mindset. This is followed by a complete dissection of the infrastructure that supports web application operations. The training then digs into the details of the OWASP top 10 while they are taught how to perform complex web attacks such as SQL injection, cross site scripting, verb tempering, XXE attacks and more. Finally, participants are shown how to analyse JavaScript and how to write secure code in support of corporate applications. The course ends with a multifaceted discussion on security configuration and monitoring an enterprise environment including Lenox and active directory security.

Tarifs

- Tarification: $3,750/person
- Rabais de 10% lorsque vous inscrivez 3 personnes.

Plan de cours

Introduction

A Word on the Importance of Social Engineering

A Word on the Importance of Open-Source Intelligence

Understanding the Hacker Mindset

The Critical Importance of User Education

The Architecture Of Web Applications

Understanding The Client Server Dynamic: From Request to Reply

From Hostname to Payload: DNS, Protocols and Web Servers

The Role and Position of the Database Server

The Role and Position of the Web Server

Exploring DNS Zones and Records

The Role of Certificates and TLS

Dissecting Web Traffic: Ports and Protocols

About Threat Intelligence, Risk Management and Vulnerability Assessments

Using Metasploit, nmap and Other Tools to Build a Target Profile

The Topology of Web Vulnerabilities: Where to look?

Overview of the OWASP Top 10 2021

Number 10: Server-Side Request Forgery

Number 9: Security Logging and Monitoring Failures

Number 8: Software and Data Integrity Failures

Number 7: Identification and Authentication Failures

Number 6: Vulnerable and Outdated Components

Number 5: Security Misconfiguration

Number 4: Insecure Design

Number 3: Injection

Number 2: Cryptographic Failures

Number 1: Broken Access Control

A Web Security Action Plan

Analysis Tools and Techniques

JavaScript Code Analysis

Unpack Multiple Layers of Packed JavaScript Code

Detect And Remove Injected Dead Code

Reverse Engineering Advanced JavaScript Obfuscation Methods

JavaScript Static and Dynamic Analysis: Using the Tools of The Trade

Exploiting Web Sites – Injection and Cross-Site Scripting

What is Injection and What Makes it Possible?

Performing an Injection Attack – Part I

Performing an Injection Attack – Part II

Using mapsql to Identify Injection Vulnerabilities

What is Cross-Site Scripting and What Makes it Possible?

Performing an XSS Attack – Part I

Performing an XSS Attack – Part II

Using nikto to Scan for Web Vulnerailities

Exploiting Web Sites – Verb Tampering and IODR

Exploring HTTP VERBS

About HTTP Verb Tampering

Detecting and Exploiting HTTP Verb Tampering vulnerabilities

Secure Server Configuration: Preventing HTTP Verb Tampering Vulnerabilities

Exploiting Web Sites – IODR

What are IDOR vulnerabilities, and how do they occur

Examples of code vulnerable to IDOR

Different types of IDOR vulnerabilities

How to detect IDOR vulnerabilities

Various methods of exploiting IDOR vulnerabilities

Preventing IDOR vulnerabilities

Exploiting Web Sites – XXE

What are XXE Vulnerabilities, and how do they occur?

Examples of Code Vulnerable to XXE

Identifying and Exploiting XXE Vulnerabilities

XXE Prevention Techniques

Secure Coding

Identifying Common Security Issues Made in JavaScript Code

Identifying A Command Injection Vulnerability in JavaScript Codes

Identifying An Advanced Cross-Site Scripting (XSS) Vulnerability

Verifying The Existence of The Vulnerability

Patching The Identified Errors and Vulnerabilities

Security Management

NIST Guidelines for Password Strength

Designing Security Management Processes

Securing Active Directory and Linux Machines

Planning for Secure Password Storage

A Word on Other Services: IPMI, DNS, SMTP and More

Ensuring Secure Configurations

Ensuring Monitoring