SDA.ACADEMY
Cybersecurity training

THINKCYBER

Syllabus

Web Application Hacking

CVBERIUM ARENA

-SIMULATOR-

Description

During this training, students will get knowledge and skills of the pentesters procedure to detect security vulnerabilities in web applications using a combination of manual and automated techniques and methods. Testing web-application security is not intuitive, and to be useful, you need an understanding of web application design, HTTP, JavaScript, browser behavior, and potentially other technologies.

The course helps prepare for the certification exams GWEB (SANS) and OSWE (Offensive Security).

Target audience

This course targets cyber experts who wish to learn web application penetration testing and people who wish to learn web application security advanced methods and techniques to find security holes.

Pre-requisites

Networking
Penetration Testing

Objectives:

- Learning different vulnerabilities
- Being able to perform web application penetration testing
- Discovering security holes in web application
- Using tools to automate your tasks

Module 1: Advanced Penetration Testing Skills

In this module, students will learn advanced techniques to understand penetration testing on the WebApp. Working correctly in a local proxy environment without using a browser can block us from partnering and not reveal all the site's information.

Advanced Information Gathering

- Website Spidering and Crawling
- Revealing Website History
- Web Page Snapshots
- Data Extraction and Scrapping

Advanced Discovery

- Understanding Advanced Methodologies
- Crafting Discovery PowerShell Scripts
- Weaponizing Curl and Wget in Discovery Scripts
- Using Metasploit Framework Web Modules
- Nmap NSE Scripts

Module 2: Web Ethical Hacking

In this module, students will learn how to perform hacking and testing capabilities of the web application. Students will handle the various results received and learn to gain remote control of the system with common web attacks.

Advanced Offensive Techniques

- RCE in Various Environments
- Understanding SQL Injection Techniques Manually
- Format String Vulnerabilities
- Cross-Site Scripting (XSS)
- WordPress Application Testing
- Understanding Steganography and Encryption
- Error Messages
- Common HTTP Feature
- Information Control

Module 3: Web Ethical Hacking Part B

In this module, students will learn how to perform advanced hacking and testing web application capabilities.

Attacks In-Depth

- Cross-Site Scripting
- Persistent
- Stored
- Command Injection
- Brute Force
- User Enumeration
- XML
- Privilege Escalation
- Directory traversal
- Local File Inclusion (LFI)
- Remote File Inclusion (RFI)
- File Upload Vulnerability
- File Inclusion to Reverse Shell Techniques
- Blind SQL Injection
- The SQL Query to Reverse Shell Techniques

Module 4: Mitigations

In this module, students will learn how to protect web application vulnerabilities.

Mitigations

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting
- Insecure Deserialization
- Insufficient Logging