CYBERIUM ARENA

— SIMULATOR —

SYLLABUS

WEBAPP SECURITY

MAIN FEATURES

Labs

The labs hold questions and tasks to support the training.

Book

The coursebooks accompany the lecturers and students alike in cybersecurity studies.

Scenarios

Provide participants possible situations from cybersecurity or cyberterrorism to solve.

Project

Trainees must complete a practical built-in project, produce defense and assault tools.

CYBERIUM ARENA
— SIMULATOR —

Description

This program's primary goal is to help security specialists understand web application risks and vulnerabilities in their organizations and conduct web application security assessments. 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.

MODULES

Module 1: Introduction to Web App

WebApp Concepts
Web Application Architecture
Client, Server, and Database
Fingerprinting Websites
Securing the Admin Interface
Parameter Tampering
HTTPS Encryption
WebApp Basics
HTML
PHP
HTTP Response Codes

Module 2: Web Languages

Javascript
Modifying HTML
Hijacking Forms
Social Engineering
HTML Parsing
JSON Parsing
XML Parsing
SQL Database
Creating Databases
Understanding SQL Injection
Testing for SQL Injection
Exploiting SQL Injection
Blind SQL Injection

Module 3: WebApp Vulnerabilities

Working with Burpsuite
Brute Force
Command Injection
User Enumeration
Local File Inclusion
Reflected XSS
Stored XSS
DOM Based XSS

Module 4: WebApp Penetration

Attacks In-Depth
Privilege Escalation
Directory traversal
Local File Inclusion (LFI)
Remote File Inclusion (RFI)
File Upload Vulnerability
File Inclusion to Reverse Shell Techniques
SQL Injection Techniques Manually
Format String Vulnerabilities
WordPress Application Testing