ABOUT THE COURSE

Attacking Web Applications course covers about a plethora of web application attack techniques & methodology to compromise Web Applications & APIs.

This instructor-led training focuses on web application vulnerability discovery and exploitation. The course also covers the class of vulnerabilities which are not detected by vulnerability scanners.

WHO SHOULD ATTEND?

- Penetration Testers
- Security Engineers
- Web Developers
- Information Security Engineers
- Security Researchers
- Security Architects
- Engineering Managers
- Security Interns

DARKRELAY SECURITY LABS

ATTACKING WEB APPLICATIONS

www.darkrelay.com

Course Introduction

- Lab Setup
- Introduction to Kali Linux & Tools
- Burp Suite & ZAP Overview
- HTTP Internals
- OWASP & CWE
- OWASP Checklist & Testing Guide

Information Gathering

- Active Information Gathering
- Passive Information Gathering

Injection Attacks

- SQL Injection
- Blind SQL Injection
- OS Command Injection
- XXE Injection
- Server-Side Template Injection

Web API Attacks

- Mass Assignment
- SQL Injection
- Path Traversal
- Open Redirection
- IDOR

Client-Side Attacks

- XSS
- CSRF

Server-Side Attacks

- SSRF

File Inclusion

- Local File Inclusion
- Remote File Inclusion

Weak Cryptography

- SSL Issues
- Weak Password Hashing

Session Hijacking

- Session Hijacking Using XSS
- Session Cookie Misconfiguration

File Upload Attacks

- File Upload Bypass
- Malicious File Uploads

CORS

- CORS Misconfiguration

Web Sockets

- CSWH

Fuzzing

- ZAP Fuzzer
- Intruder
- Wfuzz

SAST

- XSS
- SQL Injection
- IDOR
- CSRF
- File Inclusions
- OS Command Injection

DAST

- ZAP
- Burp Suite Pro

CVSS

- Severity Rating