Web Application Ethical Hacking & Penetration Testing

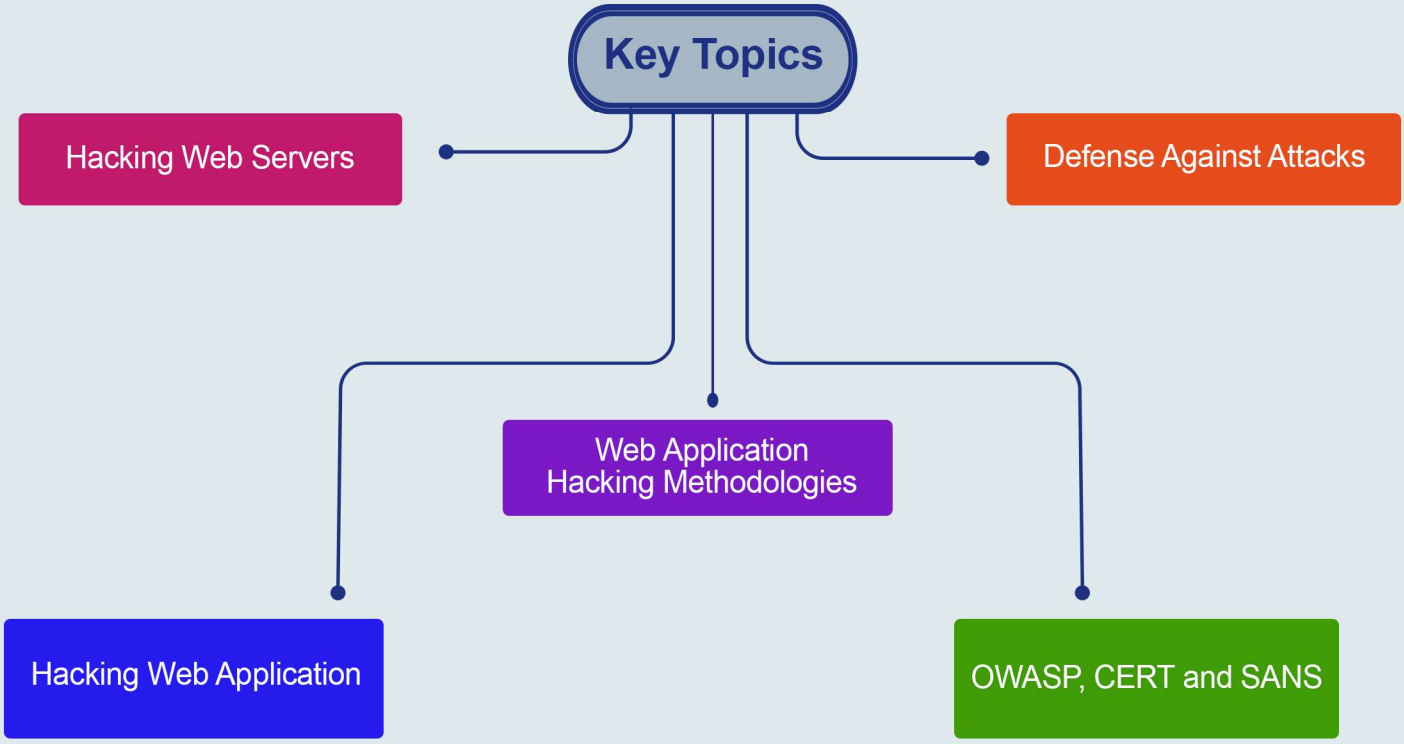
Terminus System

About the Course

The major cause of web insecurity is insecure software development practices. Ethical hacking is a process of detecting vulnerabilities in an application, system, or organization's infrastructure that an attacker can use to exploit an individual or organization. They use this process to prevent cyberattacks and security breaches by lawfully hacking into the systems and looking for weak points.This highly intensive and interactive course provides essential application security training for web application, web service and software developers and architects. Students will learn the most common threats against web applications. More importantly, students will learn how to design and code secure web solutions .

Learning Objectives

Key Topics



Pre Requisites

- Ethical Hacking & Penetration Testing Concepts Course
- Ethical Hacking & Penetration Testing Tools Course
- Web Application Security Course

Terminus System

What You Will Receive

- Course Presentation File
- Complementary Files
- Web Application Ethical Hacking & Penetration Testing eBook

Who Should Attend

- PenTesters
- CISOs
- Security Analysts
- Web App Developers

Syllabus

Hacking Web Servers

- Web Server Attack Methodology
- DoS/DDoS Attacks
- DNS Server Hijacking
- DNS Amplification Attack
- Directory Traversal Attacks
- Man-in-the-Middle/Sniffing Attack
- Phishing Attacks
- Website Defacement
- Web server Misconfiguration
- HTTP Response Splitting Attack
- Web Cache Poisoning Attack
- SSH Brute-force Attack
- XML Content Attacks
- Web Service Attacks
- Infrastructure Attacks
- Default Content and Settings
- Countermeasures

Web Application Hacking Methodologies

- OWASP TOP 10 Web Vulnerabilities
- CERT
- SANS CWE Top25

Syllabus

Hacking Web Application

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities
- Broken Access Control
- Security Misconfiguration
- SQL and Other Injection
- Cross Site Scripting (XSS)
- Insecure Deserialization
- Session Management
- Insecure Direct Object Reference
- Cross Site Request Forgery
- Buffer Overflow
- Local File Inclusion

Defense Against Attacks

- Authentication and Session Management
- Access Control Design
- Edge Level Protection
- Code Audit
- OWASP Countermeasures

Hands-on Training

- Lab 1 - Footprint the Webserver
- Lab 2 - Crack FTP Credentials
- Lab 3 - Web Application Reconnaissance
- Lab 4 - Web Spidering
- Lab 5 - Web Application Vulnerability Scanning
- Lab 6 - Brute Force Attack
- Lab 7 - Cross-Site Request Forgery attack
- Lab 8 - Enumerate and Hack Web Application
- Lab 9 - Exploit a Remote Command Execution
- Lab 10 - Gain Backdoor Access via a WebShell
- Lab 11 - Session Hijacking
- Lab 12 - Hacking Web Servers
- Lab 13 - Operating System and Application-Level Attacks
- Lab 14 - SQL Injection