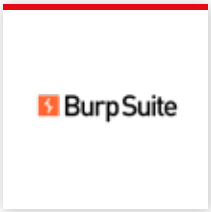
INFOSECTRAIN

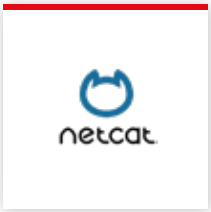
Advanced Web Application Penetration Testing (AWAPT) Training

Tools Covered

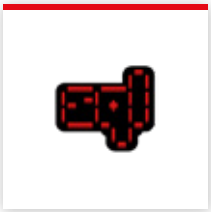
Wireshark



Burpsuite

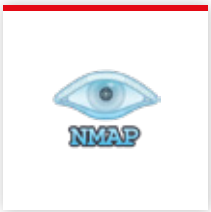


Netcat



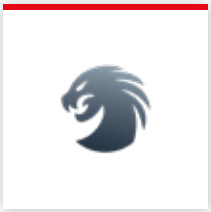
SQLMap

w3af

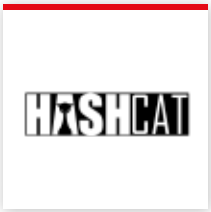


Nmap

Ffuf



Hydra

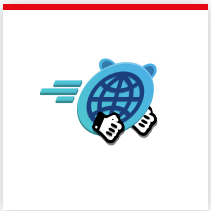


hashcat

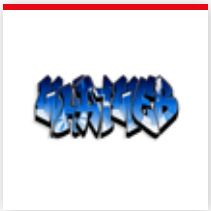
John the Riper

metasploit framework

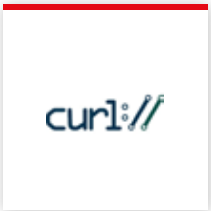
BeEF



GoBuster



Whatweb



CUrl

waybackmachine

INFOSECTRAIN

Course Highlights

- **32-Hour LIVE** Instructor-led Training
- Real-world Scenarios
- Vulnerable Webserver Practice Labs
- Real-time Simulations
- Interview Preparation & Career Guidance
- Post Training Support
- Access to Recorded Sessions
- Learn from Certified Experts
- Training Completion Certificate

INFOSECTRAIN

About Course

Web applications are the backbone of modern businesses and are often the target of sophisticated attacks. As web applications continue to evolve, so do the threats. This course will provide the expertise needed to assess, exploit, and ultimately defend web applications against these ever-growing threats. Whether you are a **developer, penetration tester, security consultant, or aspiring ethical hacker**, this course is designed to tackle the challenges of modern web security.

This comprehensive course is designed to equip cybersecurity professionals with advanced skills in Web Application Penetration Testing. Participants will gain hands-on experience in detecting the attack surface, perform the attack, and mitigating web threats using the latest tools and techniques. Through practical labs and real-world scenarios, learners will develop the expertise needed to effectively protect and defend their organizations from sophisticated Web attacks.

Course Objectives

Upon successful completion of the training, participants will be able to:

- Understand the principles of web application security and the importance of securing web technologies.
- Be proficient in using Kali Linux and its powerful tools for penetration testing.
- Gain hands-on experience with vulnerable applications to simulate real-world web security attacks.
- Automate the penetration testing workflow using tools like Burp Suite, and Nikto for vulnerability scanning.
- Master HTTP methods (GET, POST, PUT, DELETE) and understand their role in vulnerability exploitation.
- Read & Analyze Headers, Requests, and Responses: Learn to analyze web traffic and headers to uncover hidden vulnerabilities and sensitive data.
- Understand the principles of web cache and attacks
- Learn how to manipulate cookies for session hijacking and unauthorized access.
- Learn to identify and exploit insecure file upload mechanisms that allow attackers to upload malicious files (e.g., web shells).
- Understand how to exploit Cross-Site Request Forgery (CSRF) vulnerabilities to perform unauthorized actions.
- Mostly focused over serious vulnerabilities such as SQL Injection, Cross-site scripting, XML External Entity (XXE) attacks, Remote command Execution, Identifying load balancers, Remote code Execution, and more.
- Learn how to secure web applications by following industry standards such as the OWASP Top 10 and implementing best practices.
- Master the techniques for preventing SQL injection, XSS, and other injection attacks by using input validation and output encoding.
- Implement robust session handling and authentication techniques, including multi-factor authentication (MFA) and secure cookie management.

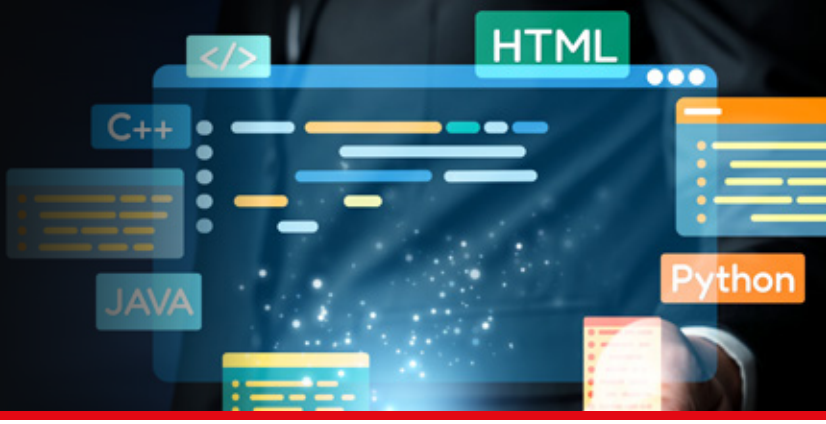
Target Audience

- Penetration Testers
- Security Analysts
- Developers
- IT Professionals
- Security Consultants/Cybersecurity Professionals
- Bug Bounty Hunters
- Students

Pre-requisites

- Basic understanding of web technologies (HTTP, HTML, JavaScript, etc.).
- Basic understanding of Linux and Windows.
- Basic understanding of Database and Networking.
- Knowledge of programming languages like Python, Java, or PHP is beneficial. (optional)

INFOSECTRAIN



Course Content

- **Introduction to Web Penetration Testing**
  - Fundamentals of web application penetration testing.
  - Importance of securing modern web applications.
  - Testing Methodologies: Explore Black Box, White Box, and Grey Box testing approaches.
- **Understanding HTTP and Web Technologies**
  - HTTP communication and protocols.
  - HTTP request/response headers and their significance.
  - Practical demo: Analyzing HTTP communication with Wireshark and Netcat.
  - Deep dive into HTTP methods, verbs, and status codes.
  - HTTP verb tampering with Nmap and Metasploit.
  - HTTP/HTTPS comparison and TLS/SSL handshake.
- **Deep Dive into Web Penetration Labs and Advanced Traffic Interception**
  - Understanding of the web penetration lab setup and the functionalities of the Kali Linux Operating System.
  - Setting up and configuring Burp Suite for HTTP/HTTPS traffic interception.
  - Understanding target scope and creating project files.
  - Burp Suite tools: Dashboard, Proxy, Intruder, Repeater, Scanner,
  - Collaborator, and Extender.

- Configuring SSL/TLS certificates for secure interception.
- Advanced traffic manipulation and injection using Burp.

Information Gathering and Reconnaissance

- Passive and active reconnaissance techniques.
- Extracting application endpoints, technologies, and server configurations.
- Tools for vulnerability scanning: Nmap, Nikto etc.
- Techniques to identify hidden endpoints and sensitive data.
- Exploiting version disclosure vulnerabilities.

Fuzzing, Brute Force, and Dictionary Attacks

- Parameter fuzzing techniques to discover hidden vulnerabilities.
- Directory brute-forcing using Gobuster and FFUF.
- Password brute-forcing with Hydra and dictionary attacks.
- Cracking hashed passwords using tools like John the Ripper and Hashcat.
- Authentication bypass using advanced SQL injection techniques.

HTTP Cache Exploitation

- Understanding private vs. public cache mechanisms.
- Exploiting HTTP response cache headers.
- HTTP parameter pollution and smuggling attacks.
- HTTP cache deception techniques and demonstrations.

HTTP Session Management

- HTTP basic authentication and session cookies.
- Understanding cookie attributes: Secure, HttpOnly, and SameSite.
- Exploiting session fixation and session hijacking vulnerabilities.
- Advanced MITM (Man-in-the-Middle) attack scenarios.
- Session management best practices for security.

Same-Origin Policy (SOP): The Core of Web Security

- Fundamentals of SOP and cross-domain requests.
- Understand the working of URL and Browser.
- Browser handling of JavaScript, frames, windows, and sites.
- Limitations of SOP and common bypass techniques (jsonp).
- CORS misconfigurations and CSRF attack exploitation.
- Advanced CORS attack scenarios and mitigation techniques.

File Upload Vulnerabilities

- Understanding malicious file upload vulnerabilities.
- Exploiting file upload functions to bypass restrictions.
- Local File Inclusion (LFI) and Remote File Inclusion (RFI) attacks.
- Practical demos: Web shells using Netcat, Python, and PHP.
- Remote Code Execution (RCE) via LFI/RFI exploitation.
- Null-byte extension bypass techniques.
- Mitigation.

SQL Injection Exploitation

- Understanding SQL queries and three-tier architecture.
- In-band, blind, time based and second-order SQL injection techniques.
- Exploiting SQL injection to extract sensitive data.
- Advanced SQLMap usage for database exploitation using sqlmap.
- Real-world SQL injection scenarios and mitigation techniques.

Cross-Site Scripting (XSS)

- Types of XSS: Stored, Reflected, and DOM-based attacks.
- Session hijacking and cookie theft using XSS.
- Exploiting XSS vulnerabilities with BeEF framework.

- XSS bypass techniques for modern web defenses.
- Effective mitigation strategies against XSS.

Indirect Object Reference (IDOR)

- Privilege escalation in web applications.
- Understanding horizontal and vertical privilege escalation.
- Exploiting IDOR in files, APIs, and databases.
- Advanced IDOR attack techniques and Mitigation.

Server-Side Request Forgery (SSRF)

- Identifying SSRF vulnerabilities in web applications.
- Exploiting blind SSRF vulnerabilities for data exfiltration.
- Escalating SSRF to Remote Code Execution (RCE).
- Mitigation techniques for SSRF vulnerabilities.

Path and Directory Traversal

- Discovering and exploiting path traversal vulnerabilities.
- Advanced techniques for bypassing path restrictions and filters.
- Real-world directory traversal attack scenarios.

Command Injection

- Identifying and exploiting basic command injection vulnerabilities.
- Discovering blind and asynchronous blind command injection attacks.
- Using Burp Collaborator for advanced exploitation.
- Real-world command injection and mitigation.

XML Injection and XXE Attacks

- Understanding XML structure and DTDs (Document Type Definitions).
- Exploiting XXE vulnerabilities and triggering OOB resource interactions.
- XML injection scenarios and mitigation techniques.

Bonus: Web Penetration Testing Report

- Understanding OWASP Top 10 framework.
- Scoring vulnerabilities using CVSS (Common Vulnerability Scoring System).
- Crafting professional penetration testing reports.
- Proof of Concept (PoC) creation and documentation.
- Presenting findings to stakeholders effectively.

Bonus Content

Interview Preparation and Guidance	Vulnerable webserver Lab for practise	Cheat sheet for various attacks like SQL Injection, XSS Injection, XML etc	Custom built list/ repos of openly available resources

System Requirements

1. Hardware:

CPU: Intel i5/i7 or AMD Ryzen 5/7 (Quad-core or better)	RAM: 8 GB (minimum), 16 GB (recommended)	Storage: 50 GB SSD (minimum), 250 GB (recommended)

2. Software:

Host OS: Kali Linux (recommended), Windows 10/11, or Ubuntu	VM software: VMware Workstation or VirtualBox	Essential tools: Burp Suite, Kali Linux.

INFOSECTRAIN
Educate. Excel. Empower.

Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on