

**Attacking Web Applications (AWA) — Course Content**

**Module 1 – Introduction to Web Application Security**

* Understanding web application architecture
* HTTP basics: requests, responses, headers, and status codes
* Common attack surfaces in modern web apps
* OWASP Top 10 overview

**Module 2 – Reconnaissance & Information Gathering**

* Passive recon (Google dorking, WHOIS, Shodan)
* Active recon (subdomain enumeration, directory brute-forcing)
* Identifying frameworks, CMS, and third-party libraries

**Module 3 – Authentication Attacks**

* Brute-force and credential stuffing
* Authentication bypass techniques
* Multi-factor authentication (MFA) attacks
* Exploiting insecure password reset mechanisms

**Module 4 – Session Management Attacks**

* Session hijacking & fixation
* Predictable session tokens
* Cross-Site Request Forgery (CSRF) exploitation
* Cookie manipulation and replay attacks

**Module 5 – Cross-Site Scripting (XSS)**

* Reflected, stored, and DOM-based XSS
* Bypassing input filters and sanitization
* Advanced payload delivery and exploitation
* Stealing cookies, session tokens, and performing keylogging

**Module 6 – SQL Injection (SQLi)**

* In-band, blind, and error-based SQL injection
* UNION-based exploitation
* Extracting data, bypassing authentication
* SQLi in NoSQL databases (MongoDB, Firebase)

**Module 7 – Command Injection**

* OS command injection basics
* Blind command injection
* Chaining commands and reverse shells
* Exploiting insecure file uploads for RCE

**Module 8 – File Upload Attacks**

* Uploading malicious scripts (PHP, ASP, JSP)
* Bypassing file extension checks and MIME filters
* Exploiting image metadata for code execution
* Webshell deployment and usage

**Module 9 – Insecure Direct Object References (IDOR)**

* Exploiting predictable identifiers
* Horizontal and vertical privilege escalation
* Automating IDOR exploitation with scripts

**Module 10 – Server-Side Request Forgery (SSRF)**

* SSRF basics and use cases
* Exploiting internal networks and cloud metadata endpoints
* SSRF chaining to RCE

**Module 11 – XML External Entity (XXE) Attacks**

* Parsing vulnerabilities in XML processors
* File disclosure via XXE
* SSRF through XXE payloads

**Module 12 – Deserialization Vulnerabilities**

* Insecure object deserialization in Java, PHP, Python
* Remote code execution via deserialization
* Identifying and exploiting insecure serialization libraries

**Module 13 – API Attacks**

* API discovery and fuzzing
* Exploiting insecure authentication & authorization
* Mass assignment vulnerabilities
* Rate-limit bypasses

**Module 14 – Web Application Logic Flaws**

* Business logic exploitation
* Race conditions
* Abuse of workflow and transaction processes

**Module 15 – Bypassing Web Application Firewalls (WAFs)**

* WAF fingerprinting
* Payload obfuscation and encoding
* Advanced bypass techniques for XSS and SQLi

**Module 16 – Exploiting Third-Party Components**

* Supply chain attacks
* Vulnerabilities in CMS (WordPress, Drupal, Joomla)
* Exploiting outdated JavaScript libraries

**Module 17 – Client-Side Attacks**

* Clickjacking
* HTML5 storage abuse
* Cross-origin resource sharing (CORS) misconfigurations

**Module 18 – Advanced Recon & Automation**

* Using Burp Suite Pro for automation
* Custom scripts with Python for fuzzing and exploitation
* Integrating with open-source tools like OWASP ZAP

**Module 19 – Reporting & Remediation**

* Documenting vulnerabilities
* Proof-of-concept (PoC) creation
* Writing mitigation and prevention strategies

**Module 20 – Final Web Application Pentest**

* Full-scope assessment of a live lab application
* Combining multiple vulnerabilities into chained exploits
* Final report and presentation