WAPT – Web Application Penetration Testing

1. Module: Intro Web Application Pentest

- Web Application Frameworks
- Web Application Overview
- What is Penetration Test
- Types of Penetration Test
- Categories of Penetration Test
- Penetration Testing Methodologies
- Vulnerability Assessments versus Penetration Test
- Rules of Engagement
- OSSTMM
- NIST
- OWASP TOP 10

2. Module: Information Gathering

- Collect information of target URL
- OSIENT framework
- User Recon Techniques
- Collect information using Automated Tools
- Foot printing through Social Engineering
- Network Foot printing
- Passive Information Gathering
- Collect information through Automated Tools
- Domain Recon Technique
- Email Recon Technique
- Whois Foot printing
- Google Hacking dB
- Subdomains Find
- Directory Fuzzing
- Go Buster and Dirbuster
- Dirb

3. Module: SQL Injection Attack

- Introduction of SQL and Database
- How vulnerabilities arise
- Understand SQL queries
- Authentication Bypass
- Manual Testing on live website
- Error-based SQL injection
- UNION-based SQL Injection
- Blind SQL Injection
- Time-based SQL Injection
- Practical labs (18 labs)
- Prevent SQLi
- Writing Report

4. Module: Cross-site Scripting Attack

- Introduction of Cross-site Scripting
- Understand XSS
- How to Identify XSS Vulnerability
- Types of XSS: Reflected, Stored, DOM-based
- Types of Cross-Site Scripting
- Reflected/Nonpersistent XSS
- Vulnerable Code
- Stored XSS/Persistent XSS
- Payloads
- Blind XSS
- DOM-Based XSS
- Detecting DOM-Based XSS
- Sources (Inputs)
- Sinks (Creating/Modifying HTML Elements)
- Static JS Analysis to Identify DOM-Based XSS
- Types of DOM-Based XSS

- Reflected DOM XSS
- Stored DOM XSS
- Exploiting XSS
- Cookie Stealing with XSS
- Exploiting XSS for Conducting Phishing Attacks
- Mitigation: Output encoding, Content Security Policy (CSP)
- Preventing XXS
- Practical labs (40 labs)
- Writing Report

5. Module: Authentication & Authorization

- Introduction to Enumeration
- How vulnerabilities arise
- Username Enumeration
- Invalid Username with Invalid Password
- Valid Username with Invalid Password
- Brute Force and Dictionary Attacks
- Types of Authentication
- HTTP Basic Authentication
- HTTP-Digest Authentication
- Attacking HTTP Basic Auth
- Authentication Bypass Attacks
- Authentication Bypass Using SQL Injection
- Authentication Bypass Using XPATH Injection
- Testing for XPATH Injection
- Authentication Bypass Using Response Tampering
- Authentication Bypass with Insecure Cookie Handling
- Session Attacks
- IDOR
- 2FA bypass
- Password reset poisoning via middleware
- role-based access control
- Preventing
- Practical labs (30 labs)

- Writing Report

6. Module: Session Hijacking

- Introduction to Session Hijacking
- How vulnerabilities arise
- Application-Level Session Hijacking
- Network-Level Session Hijacking
- Compromising Session IDs
- Blind Hijacking
- Session Hijacking Tools
- Detection Methods and Tools
- Prevention Session Hijacking Attack
- Practical labs (5 labs)
- Writing Report

7. Module: File Upload Vulnerability

- Introduction of file upload vulnerabilities
- How vulnerabilities arise
- Vulnerability Scoring System
- Impact of file upload vulnerabilities
- Exploiting unrestricted file uploads to deploy a web shell
- Exploiting file upload vulnerabilities without remote code execution
- Exploiting file upload race conditions
- Uploading files using PUT
- Preventing File Upload Vulnerability
- Practical labs (7 labs)
- Writing Report

8. Module: Directory/Path traversal

- Introduction to Directory traversal
- How vulnerabilities arise
- LFI vs Directory traversal
- File path traversal, traversal sequences blocked with absolute path bypass
- File path traversal, validation of start of path

- validation of file extension with null byte bypass
- Practical Labs (6 labs)
- Prevent Directory traversal attack

9. Module: File inclusion

- Introduction to file inclusion
- Types of File Inclusion
- How vulnerabilities arise
- Local file Inclusion
- Difference between LFI and Directory Traversal
- LFI to Sensitive Data discloser
- Exploiting LFI Using PHP
- Exploiting LFI Using File Uploads
- Local File Disclosure Vulnerability
- Remote File Inclusion
- RFI Attack
- Detect file inclusion vulnerabilities
- Practical labs (5 labs)
- Prevent LFI and RFI
- Writing Report

10. Module: Cross-site Request Forgery

- Introduction to CSRF
- Impact of CSRF
- How vulnerabilities arise
- XSS vs CSRF
- Bypassing CSRF token validation
- Bypassing Same Site cookie restrictions
- Bypassing Referrer-based CSRF defenses
- Practical labs (15 labs)
- Preventing CSRF vulnerabilities
- Writing Report

11. Module: Server-site Request Forgery

- Introduction to SSRF
- How vulnerabilities arise
- Impact of SSRF
- Types of SSRF
- Basic SSRF against the local server
- Remote SSRF
- Simple SSRF
- Local server SSRF
- Blind SSRF
- Prevent SSRF
- Practical labs (10 labs)
- Writing Report

12. Module: Business logic Vulnerability

- Introduction to Business logic Vulnerability
- How vulnerabilities arise
- Techniques of
- Client-side controls
- Price Tempering
- High-level logic vulnerability
- Inconsistent security controls
- Low-level logic flaw
- Weak isolation on dual-use endpoint
- Authentication bypass via flawed state machine
- Infinite money logic flaw
- Prevent Business logic Vulnerability
- Practical labs (11 labs)
- Writing Report

13. Module: Deserialization attacks

- Introduction to Deserialization attacks
- How vulnerabilities arise

- Modifying serialized objects
- Modifying serialized data types
- Using application functionality to exploit insecure deserialization
- Arbitrary object injection in PHP
- Exploiting Java deserialization with Apache
- Developing a custom gadget chain for PHP deserialization
- Practical labs (10 labs)
- Prevent Deserialization Attack
- Writing Report

14. Module: XML External Entity Path Injection

- Introduction to XXE and XML entity
- How vulnerabilities arise
- Types of XXE
- Exploiting XXE using external entities to retrieve files
- Exploiting XXE to perform SSRF attacks
- Blind XXE with out-of-band interaction
- Blind XXE with out-of-band interaction via XML parameter entities
- Exploiting blind XXE to exfiltrate data using a malicious external DTD
- Exploiting blind XXE to retrieve data via error messages
- Exploiting XXE via image file upload
- Practical labs (10 labs)
- Prevent XXE
- Writing Report

15. Module: HTTP Host header attacks

- Introduction to HTTP and HTTP code and Request Method
- Introduction to HTTP Host Header Attack
- How vulnerabilities arise
- Basic password reset poisoning
- Host header authentication bypass
- Web cache poisoning via ambiguous requests
- Host validation bypass via connection state attack
- Password reset poisoning via dangling markup

- Practical labs (7 labs)
- Prevent HTTP Host header Attack
- Writing Report

16. Module: Cross-origin resource sharing

- Introduction of CORS
- Understand CORS
- SOP
- ACAO
- CORS vulnerability with basic origin reflection
- CORS vulnerability with trusted null origin
- CORS vulnerability with trusted insecure protocols
- Practical labs (3 labs)
- Prevent CORS
- Writing Report

17. Module: Clickjacking

- Introduction of Clickjacking
- Clickjacking with prefilled from input
- Frame busting scripts
- Basic clickjacking with CSRF token protection
- Clickjacking with form input data prefilled from a URL parameter
- Exploiting clickjacking vulnerability to trigger DOM-based XSS
- Multistep clickjacking
- Practical labs (5 labs)
- Prevent Clickjacking
- Writing Report

18. Module: Web Sockets

- Introduction of Web sockets
- Manipulating Web Socket Traffic
- Intercept and modifying messages
- Manipulating Web socket Connections

- Exploiting Vulnerabilities
- Securing a WebSocket Connection
- Practical labs (3 labs)
- Prevent Web Sockets
- Writing Report

19. Module: Information Disclosure

- Introduction of Information Disclosure or Cryptographic failure
- How vulnerabilities arise
- Impact
- Testing for Information Disclosure
- Information disclosure in error messages
- Information disclosure on debug page
- Source code disclosure via backup files
- Authentication bypass via information disclosure
- Practical labs (5 labs)
- Prevent Information Disclosure
- Writing Report

20. Module: NoSQL Injection Vulnerability

- Introduction of NoSQL Databases
- Difference Between SQL and NoSQL
- NoSQL syntax injection
- NoSQL operator injection
- Detecting NoSQL Injection
- Exploiting syntax injection to extract data
- Exploiting NoSQL operator injection to extract data
- Timing based injection
- Practical labs (4 labs)
- Preventing NoSQL injection
- Writing Report

21. Module: Race Condition

- Introduction of race condition

- Limit overrun race conditions
- Hidden multi-step sequences
- Methodology
- Multi-endpoint race conditions
- Single-endpoint race conditions
- Session-based locking mechanisms
- Preventing Race Condition
- Practical labs (6 labs)
- Writing Report

22. Module: JWT

- Introduction of JWT
- Use of JWT
- JWT authentication bypass via unverified signature
- JWT authentication bypass via flawed signature verification
- JWT authentication bypass via weak signing key
- JWT authentication bypass via kid header path traversal
- Preventing JWT Vulnerability
- Practical labs (8 labs)
- Writing Report

23. Module: Command Injection

- Introduction of Command Injection
- Injecting OS Command
- Blind Command Injection Vulnerabilities
- Exploiting by redirecting output
- Exploiting using Out-of-band techniques
- Preventing Command Injection
- Practical labs (5 labs)
- Writing Report

Note :- Total number of Labs :- 285