**SL-WPTE – Web Penetration Testing Expert**

**Course Syllabus**

---

**Course Overview**

This course provides students with a complete, practical introduction to **Web Application Penetration Testing** following **PTES**, **OWASP WSTG**, and **PortSwigger Web Security Academy** methodologies.
Students will develop hands-on experience with reconnaissance, exploitation, reporting, and remediation planning.

---

**Structure**

- **Total Meetings:** 15
- **Format:** Instructor-led theory, guided labs (PortSwigger + OWASP Juice Shop), class missions, home missions, and self-investigate tasks.
- **Final Project:** Simulated penetration test & reporting exercise.

---

**Meetings Breakdown**

---

**Meet 1 – Introduction & HTTP Fundamentals**

- PTES & OWASP WSTG methodology
- HTTP methods, headers, cookies, status codes, TLS basics
- Burp Suite setup & workflow

---

**Meet 2 – Information Gathering**

- Fingerprinting, reconnaissance, discovery techniques
- Directory/file brute-forcing
- Subdomain & technology enumeration
- PortSwigger: *Information Disclosure Labs*

---

**Meet 3 – Configuration & Deployment Management**

- Debugging info leaks
- Directory listing & stack traces
- Missing/misconfigured headers
- Hardening best practices

---

**Meet 4 – Identity Management Testing**

- Username enumeration
- Brute force & account lockout logic
- Multi-factor authentication weaknesses
- PortSwigger: *Authentication Labs (part 1)*

---

**Meet 5 – Authentication Testing**

- Password reset logic flaws
- Reset poisoning & bypass
- Credential stuffing & weak password defenses
- PortSwigger: *Authentication Labs (part 2)*

**Meet 6 – Authorization Testing**

- IDOR (Insecure Direct Object References)
- Horizontal & vertical privilege escalation
- Role misconfigurations
- Access control best practices

---

**Meet 7 – Session Management Testing**

- Cookies & tokens
- JWT attacks: weak keys, algorithm confusion, unverified signatures
- Session fixation & hijacking
- PortSwigger: *JWT Labs*

---

**Meet 8 – Input Validation I (Cross-Site Scripting)**

- Reflected, DOM, and stored XSS
- Context-based injection
- Content Security Policy bypasses
- PortSwigger: *XSS Labs*

---

**Meet 9 – Input Validation II (SQL Injection)**

- UNION-based, error-based, and blind SQLi
- Database fingerprinting & data extraction
- PortSwigger: *SQLi Labs*

---

**Meet 10 – Error Handling & Logging**

- Error message leakage
- Stack trace exposure
- Logging best practices & monitoring

---

**Meet 11 – Cryptography Testing**

- TLS/SSL misconfigurations
- Weak hashing & encryption
- Practical cipher testing tools

---

**Meet 12 – Business Logic Testing**

- Workflow bypass
- Race conditions
- Financial logic abuses
- Real-world case studies

---

**Meet 13 – Client-Side Testing**

- DOM-based vulnerabilities
- Prototype pollution
- CORS misconfigurations
- Clickjacking attacks
- PortSwigger: *DOM XSS & Prototype Pollution Labs*

---

**Meet 14 – API Testing**

- REST & GraphQL testing
- BOLA (Broken Object Level Authorization)
- Parameter manipulation & over-fetching
- OWASP API Top 10

---

**Meet 15 – Final Simulation & Reporting**

- Full penetration test simulation
- Attack chain execution
- Report writing & presentation
- Peer review and defense

**Evaluation**

- **Class Missions:** Practical in-class labs
- **Home Missions:** Individual assignments after each meet
- **Self-Investigate:** Independent research on standards & real-world cases
- **Final Project:** End-to-end penetration test + report