Web Application Penetration Testing Syllabus

LEVEL I

Introduction, OWASP Top 10	2 Hours - Day 1
Installing Lab	2 Hours - Day 2
Enumeration	2 Hours - Day 3
Vulnerability Scanning	2 Hours - Day 4
Introduction to burpsuite,Authentication bypass using burpsuite	2 Hours - Day 5
Html injection, Introduction about cookie	2 Hours - Day 6
XSS (reflected, stored, DOM)	2 Hours - Day 7
XSS Advance	2 Hours - Day 8
Introduction to BeeF and browser Hijack	2 Hours - Day 9
Cookie stealing and session Hijack	2 Hours - Day 10
Broken Access Control	2 Hours - Day 11
Broken session and security misconfiguration	2 Hours - Day 12
Using Components with Known Vulnerabilitie	2 Hours - Day 13
Uploading web shell	2 Hours - Day 14
Uploading web shell filter bypass Evaluation	2 Hours - Day 15
Path traversal, LFI and RFI basic	2 Hours - Day 16
LFI RFI advance	2 Hours - Day 17
Lab solving	2 Hours - Day 18
Lab solving	2 Hours - Day 19

Lab solving	2 Hours - Day 20

LEVEL II

Introduction to A1 Vulnerabilities	2 Hours - Day 1
Advance Burpsuite (repeater, sequencer, decoder)	2 Hours - Day 2
Error Based SQL injection for GET method basic and advance	2 Hours - Day 3
Error Based SQL injection for POST method basic and advance	2 Hours - Day 4
Boolean based SQL injection basic	2 Hours - Day 5
Boolean based SQL injection advance	2 Hours - Day 6
Time based SQL injection	2 Hours - Day 7
WAF bypassing	2 Hours - Day 8
Web shell uploading using SQL injection	2 Hours - Day 9
XPATH injection basic and advance	2 Hours - Day 10
XXE Injection	2 Hours - Day 11
OS Command Injection and handling web server	2 Hours - Day 12
CSRF for GET method	2 Hours - Day 13
CSRF for POST method	2 Hours - Day 14
CSRF Filter Bypass	2 Hours - Day 15
CTF Lab Solving	2 Hours - Day 16
CTF Lab Solving	2 Hours - Day 17
CTF Lab Solving	2 Hours - Day 18
CTF Lab Solving	2 Hours - Day 19
CTF Lab Solving	2 Hours - Day 20