Web Application Hacking and Security - WAHS Syllabus

Advanced Web Application Penetration Testing	2 Hours
Advanced SQL Injection (SQLi)	2 Hours
Reflected, Stored and DOM-based Cross Site Scripting (XSS)	2 Hours
Cross Site Request Forgery (CSRF) – GET and POST Methods	2 Hours
Server-Side Request Forgery (SSRF)	2 Hours
Security Misconfigurations	2 Hours
Directory Browsing/Bruteforcing	2 Hours
Network Scanning	2 Hours
Auth Bypass	2 Hours
Web App Enumeration	2 Hours
Dictionary Attack	2 Hours
Insecure Direct Object Reference Prevention (IDOR)	2 Hours
Broken Access Control	2 Hours
Local File Inclusion (LFI)	2 Hours
Remote File Inclusion (RFI)	2 Hours

Arbitrary File Download	2 Hours
Arbitrary File Upload	2 Hours
Using Components with	2 Hours
Known Vulnerabilities	2 Hours
Command Injection	2 Hours
Remote Code Execution	2 Hours
File Tampering	2 Hours
Privilege Escalation	2 Hours
Log Poisoning	2 Hours
Weak SSL Ciphers	2 Hours
Cookie Modification	2 Hours
Source Code Analysis	2 Hours
HTTP Header modification	2 Hours
Session Fixation	2 Hours
Clickjacking	2 Hours