BUG BOUNTY SYLLABUS

Module 1: Introduction to Bug Bounty & Web Security

- Understanding Bug Bounty Programs
- How Bug Bounty industry works & reward process
- Responsible disclosure & legal considerations
- Skillset and roadmap for Bug Bounty Hunter
- Types of testing & real community success stories

Module 2: Burp Suite Professional – Complete Mastery

- Installing Java and Burp Suite setup
- Browser configuration & Proxy integration
- Working with Foxy Proxy
- Burp Suite interface walkthrough
- Essential modules & extensions from BApp Store
- Intercepting, modifying, and replaying requests

Module 3: Reconnaissance & Information Gathering (Hunter-Style Recon)

Goal: Maximize attack surface like top hunters

- Active & Passive Recon concepts
- Scanning with Nmap
- Technology fingerprinting using WhatWeb & Wappalyzer
- Advanced Google Dorks
- Subdomain enumeration methods & tools
- GitHub reconnaissance & asset discovery
- HTTP Status analyzer & online recon utilities
- Exploring tools like: Censys, crt.sh, Wayback Machine, DNS Dumpster, Shodan

---

Module 4: Web Vulnerabilities & Exploitation Techniques

🔥 ***Every vulnerability includes: Theory + Hunting Techniques + Labs + Live Proof-of-Concept + Mitigation***

1. **HTML Injection**
2. **Critical Parameter / Source Code Flaws & Path Traversal**
3. **Cross-Site Scripting (XSS)**

- Reflected / Stored / DOM / Blind XSS
- Advanced exploitation
- XSS automation using Burp

4. **Host Header Injection Attack**
5. **Cross-Site Request Forgery (CSRF)**

- Account takeover demos
- Anti-CSRF token handling

6. **SQL Injection**

- Authentication bypass
- GET / POST / Header / Cookie-based SQLi
- SQLMap automation & manual exploitation
- Dumping databases

7. **Command Injection (CMDi)**
8. **Insecure Direct Object Reference (IDOR)**

- Account takeover scenarios

9. **Rate Limiting & Authentication Abuse**

- Login throttling bypass
- Password reset attack chains
- Mass account creation attacks

10. **Parameter Tampering & Insecure Deserialization**
11. **Sender Policy Framework (SPF) Email Spoofing**
12. **Web Shell Uploading & Defacement**
13. **File Inclusion (LFI / RFI / Path Traversals)**
14. **Metadata (EXIF) Exposure Attacks**
15. **OTP Bypass**

16. **Wordpress Vulnerabilities**
- XMLPRPC Hunting
- User/Admin disclosure

17. **Session / Authentication Vulnerabilities**
- Session Hijacking
- Weak Authentication
- Cookies hunting

18. **Bruteforce and Dictionary Based Attacks**
19. **Mobile Application Hunting**
- Androd Application code Hunting
- IOS Application code Hunting

20. **Account Lockout Bugs**
21. **Cryptography Vulnerabilities**
22. **Multifactor/2FA Bypass hunting**

Module 5: Hands-On Practical Labs

- Real-world exploitation labs
- Anonymous reporting techniques
- Red teaming approach for bounty hunting

Module 6: Capture-The-Flag (Mini Bug Bounty Practice)

- Solving CTF Challenges
- Write-up approach

Module 7: Professional Bug Reporting & Documentation

- Writing clear Proof of Concept reports
- Creating video POC demos
- Sample winning reports and walkthroughs
- How to get appreciation, acknowledgments & HOF

Module 8: Bug Bounty Platforms & Hunting Strategy

- Overview & working process of platforms:
    - HackerOne
    - BugCrowd
    - Intigriti
    - YesWeHack
    - Synack
    - OpenBugBounty
    - Facebook / EC-Council / Private Programs/ responsible Disclosures
- Filtering valuable programs to hunt
- My personal hunting methodologies