Advance Bug Bounty

HACKTIFY cybersecurity

Sr. No	Topic	Sub Topic	Hours
Module - 1	Introduction	Introduction • What are Advance Bug Bounties • Advance Recon Methodology • Mindmap Creation • Setting Up your Hacking environment	4
Module - 2	Recon Tactics	Recon Tactics • Effective Shodan Reconnaisance • Active Subdomain Enumeration + Resolvers • Subdomain Mastering with Advance techniques • Building an Attack Surface Mapper • Building an Bug Bounty Alert System	8

Sr. No	Topic	Sub Topic	Hours
Module - 3	OAuth Attacks	• Implicit Grant Attack • OAuth CSRF protection Attack Bypass • Leaking Authorization codes and Access tokens • Flawed Scope Validation Attack • Unverified User Registration Attack • Host header Injection Oauth Attack • Reusable OAuth access token Attacks • State Parameter Bypass	8
Module - 4	JWT Attacks	• Abusing None Algorithm • Signature Stripping • HS256 (symmetric encryption) key cracking • Cracking weak shared secrets • Substitution attack • Practical Lab • CTF	8

Sr. No	Topic	Sub Topic	Hours
Module - 5	SAML Attacks	SAML • SAML Fundamentals • SAML vs OAuth • SAML Request & Response Breakdown • XML Signatures • XML Signature Wrapping Attacks - Type 1 • XML Signature Wrapping Attacks - Type 2 • XML Signature Wrapping Attacks - Type 3 • XML Signature Wrapping Attacks - Type 4 • XML Signature Wrapping Attacks - Type 5 • XML Signature Wrapping Attacks - Type 6 • XML Signature Wrapping Attacks - Type 7 • XML Signature Wrapping Attacks - Type 8 • SAML Extractor • SAML Raider • SAML to XSS Attacks • SAML Token Recipient Confusion Attack • Xml External Entities Attacks via SAML • Mitigations	8

Sr. No	Topic	Sub Topic	Hours
Module - 6	WAF Bypasses	• XSS Bypasses • SQL Injection Bypass • ModProxy & Cloudflare Bypass • CTF	8
Module - 7	Wordpress Pentesting	Wordpress Pentesting • Wordpress Active Enumeration • Wordpress Passive Enumeration • Wordpress Users, Themes, Plugins, Versions • XML-RPC leads to DoS and DDoS • Wordpress SSRF • Wordpress Twenty Sixteen RCE • Wordpress MSF Exploitation • Wpscan • CTF	8

Sr. No	Topic	Sub Topic	Hours
Module - 8	Active Directory	Active Directory • Active Directory Fundamentals • Setting up Domain Controller • Setting up GPO • Extracting Information Windows AD • Office365 Recon • Mimikatz LSASS • Windows Local Privilege Escalation with Hot Potato • Process Injection • DLL Injection • Defense Evasion	8
Final Exam	Final Exam		2
			60

Thank You!

✉ shifa@hacktify.in

☎ +91-9106147779

+91-8160206309

in @hacktifycs

▶ @hacktifycs

@hacktifycs

www.hacktify.in

HACKTIFY
cybersecurity

Unit no. 1021,1st floor-1 Aerocity,
SakiNaka, Andheri(East),
Mumbai- 400072