Web Application Pentesting

HACKTIFY
cybersecurity

Sr. No	Topic	Sub Topic	Hours
Module - 1	Introduction	• What are WebApplications • Introduction to VAPT • VAPT vs Bug Bounties • Some Basic Terminologies • Setting Up your Hacking environment	4
Module - 2	Penetration Testing Fundamentals	Fundamentals • OWASP10 • OWASP 2013 vs 2017 vs 2021 • Mitre Framework • Top 10 Rules for Bug Bounties • CVSS Framework	2

Sr. No	Topic	Sub Topic	Hours
Module - 3	Authentication Bypass	• OTP Bypass • Captcha Bypass • Response Manipulation • Status code manipulation • OTP Code leakage • JS File Analysis • 2FA Code Reusability • Lack of Bruteforce Protection • Missing 2FA code integrity validation • Password Reset Disable 2FA • Backup Code Abuse • Clickjacking disables 2FA • Enabling 2FA doesn't expire previous sessions • Bypass 2FA with null or 00000 • Mitigations	4

Sr. No	Topic	Sub Topic	Hours
Module - 4	Cross Site Scripting	XSS • Reflected XSS • Stored XSS • DOM XSS • Blind XSS • Post based XSS • PostMessage • Mitigations	4
Module - 5	Rate Limiting	Rate Limiting • No Rate Limiting • Rate Limit Bypass using headers • Rate Limit Bypass using special characters • Race Conditions • Mitigations	4

Sr. No	Topic	Sub Topic	Hours
Module - 6	CSRF	Cross Site Request Forgery • CSRF Attacks • CSRF to Account Takeover • CSRF to Account Delete • CSRF Bypass Techniques • Mitigations	4
Module - 7	Open Redirect	Open Redirect • Open Redirect Attack • Open Redirect DOM Based Attacks • Open Redirect Bypasses • Mitigations	4

Sr. No	Topic	Sub Topic	Hours
Module - 8	Cross Origin Resource Sharing Attacks	CORS • CORS Attacks via CURL • CORS Attacks via Burpsuite • CORS Attacks Suffix match • CORS Attacks Prefix Match • CORS Attacks Not escape dot • CORS Attacks Substring Match • CORS Attacks Trust Null • CORS Attacks Mitigations	4
Module - 9	Click Jacking Attacks	Click Jacking Attacks • X-Frame Options • iFrames • Mitigations	4

Sr. No	Topic	Sub Topic	Hours
Module - 10	HTML Injection Attacks	• HTML Injection Atacks • HTML Injection Iframes • HTML Injection Deface • Mitigations	4
Module - 11	Broken Link Hijacking	• Broken Link Hijacking - Social Media Links • Broken Link Hijacking - Github/S3 Buckets • Mitigations	4
Module - 12	Session related Issues	• Session Hijacking • Session Fixation • Failure to Invalidate Session • Mitigations	4

Sr. No	Topic	Sub Topic	Hours
Module - 13	SQL Injection Attacks	• SQL Injection Types • SQL Injection with SQLMap • SQL Injection Bypass with Atlas • Mitigations	4
Module - 14	Server Side Request Forgery	• SSRF Fundamentals • Internal SSRF • External SSRF • Microstratergy SSRF • Mitigations	4
Module - 15	Local File Inclusion	• Local File Attacks • Local File MPEG Attacks • Local File Inclusion Linux Attacks • Local File Inclusion Windows Attacks • Mitigations	4

Sr. No	Topic	Sub Topic	Hours
Module - 16	Remote Code Execution	• RCE • Apache Struts2 RCE • File Upload RCE • Apache Tomcat WAR RCE • Mitigations	4
Module - 17	Subdomain Takeovers	• Subdomain Takeovers • Active Subdomain Takeovers • Passive Subdomain Takeovers • Subdomain Takeovers - AWS • Subdomain Takeovers - Shopify • Subdomain Takeovers - Can I Take Over XYZ 2 • Subdomain Takeovers - New Exclusive Takeover Template • Mitigations	4

Sr. No	Topic	Sub Topic	Hours
Module - 18	Bug Bounty RoadMap	• Bugcrowd Platform • Hackerone Platform • Intigriti Platform • RVDP NCIIPC • Private RVDP Programs	4
Module - 19	Capstone Project	Capstone Project • Web App Capstone Project • Proffesional Report Writing	4
Module - 20	Final Exam	• Final Exam	2
			76

Thank You!

shifa@hacktify.in

+91-9106147779

+91-8160206309

@hacktifycs

@hacktifycs

@hacktifycs

www.hacktify.in

HACKTIFY
cybersecurity

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