HACKERSPREY

A PLATFORM BUILT TO SUPERCHARGE YOUR HACKING SKILLS

6 Weeks Cybersecurity Industrial Training

Topics	Focus Areas To Be Covered
INFORMATION GATHERING	• A Word About Information Gathering • WHOIS Enumeration • Active Information Gathering • Understanding Domain Name System • DNS Enumeration
NETWORK SCANNING USING NMAP	• Network Scanning using NMAP • A Basic UDP scan with NMAP • Telnet Scanning with Brute Forcing • SMTP Reconnaissance Techniques • Comprehensive SMB Scanning • Finger Service Reconnaissance
BASICS OF HTTP	• Understanding Hyper Text Transfer Protocol • A Word About Cookies & Session Management • Understanding Document Object Model (DOM) • Overview of Same Origin Policy (SOP) • A word about CROSS-ORIGIN RESOURCE SHARING
CSRF	• Understanding Cross Site Request Forgery • CSRF Using GET Request • CSRF Using POST Request • Eliminating The CSRF Token • Manipulating The CSRF Token
XSS	• A Word About Cross Site Scripting • CSRF & XSS Key Differences • Stealing cookies using reflected XSS • Stealing money using reflected XSS • Understanding DOM • Exploiting Client-Side Code via DOM Manipulation

XSS	• Exploiting DOM XSS via Improper URL Handling • Understanding Stored XSS • Stealing Cookies using Stored Cross Site Scripting • Understanding CSP • Stored XSS With CSP
SQLI	• A Word About SQL Injection • Login Bypass Using Universal Key • Login Bypass Using Union Operator • Extracting Flags Using Blind SQL Injection • Blind SQL Injection Using Order By • Error Based Sqli
IDOR	• Understanding Insecure Direct Object Reference • Unauthorized Note Access in Prey Notes website • Exploiting IDOR Vulnerabilities with Session Hijacking
SSTI	• Understanding SSTI • Exploiting SSTI with External Config in E-commerce • SSTI Exploitation: Advanced Payloads & Filter Bypass • Bypass black Listing using External End points
ADVANCED TOPICS	• NoSQL Injection • Race Condition • Rate Limit Bypass • Github
INPUT HANDLING AND INFORMATION DISCLOSURE VULNERABILITIES	• Directory Listing • Parameter Pollution • Command Injection • Path Traversal • Web Cache Poisoning

INITIAL ACCESS, EVASION, AND PRIVILEGE ESCALATION	• External Scanning • Understanding reverse shell and bind shell • RAT vs Windows Defender • Evading Windows Defender using Freeze • Understanding NTDLL.DLL and AV Unhooking • Malware Delivery Infection Chain • Post Exploitation Reconnaissance • Bypassing UAC using COM Objects • Gaining NT Auth Shell • Exploiting Misconfiguration in Windows
GAINING ACCESS VIA SMB USING CRACKMAPEXEC	• Gaining access using SMB
ACTIVE DIRECTORIES AND VARIOUS ENUMERATION TECHNIQUES	• A word about Windows Active Directories • Enumeration using PowerView • Enumeration using BloodHound • Enumeration using RPCClient
DOMAIN PRIVILEGE ESCALATION	• Kerberoasting • AS-REP Roasting
LATERAL MOVEMENT	• Pass the Hash • Pass the ticket
DOMAIN PERSISTENCE TECHNIQUES	• Golden Ticket • Silver Ticket
ADDITIONAL ATTACKS	• LLMNR Poisoning