CYBERGUARDX

Ethical Hacking Bug Bounty

Diploma

CYBERGUARD Academy | CYBERGUARD | TheBlueGuard

About the Diploma

Diploma is a **175-hour, 6-month** program designed to equip students with no prior security knowledge with the skills required to become professional penetration testers and bug bounty hunters. This hands-on program covers ethical hacking fundamentals, web security vulnerabilities, attack methodologies, and advanced exploitation techniques. The curriculum progresses from basic web security concepts to advanced topics like logical vulnerabilities, authentication bypasses, access control flaws, and HTTP request smuggling.

By the end of the program, students will be prepared to identify and exploit web vulnerabilities, participate in bug bounty programs, obtain the eWPT (eLearnSecurity Web Penetration Tester) certification from INE, and pursue penetration testing careers

Diploma Objectives

By completing this diploma, students will:

Understand the fundamentals of web security & ethical hacking

Learn reconnaissance, enumeration, and exploitation techniques

Master OWASP Top 10 vulnerabilities and beyond

Gain expertise in logical vulnerabilities, business logic flaws authentication bypasses and access control issues

Work with real-world bug bounty platforms

Develop skills in advanced attack techniques like HTTP request smuggling & supply chain attacks

Learn defensive security techniques, including vulnerability patching and mitigation

Practice on PortSwigger Web Security Academy Labs for hands-on experience after each vulnerability

Earn a recognized certification (eWPT) upon successful completion

Diploma Structure & Timeline

Duartion:175 Hours (6 month , 2 sessions per week)

Format: Hands -on training , live exploitation ,and real-world testing

Final Capstone Project: Practical assessments on PortSwigger Web Security Academy Labs

Final Certification & Career Opportunities

Upon completion, students will: Receive a Web Penetration Testing & Bug Bounty

Be prepared to earn the eWPT (eLearnSecurity Web Penetration Tester) certification from INE

Be ready to work as Penetration Testers, Web Security Analysts, or Bug Bounty Hunters

Gain hands-on experience through PortSwigger Web Security Academy Labs

Diploma Modules & Detailed Topics

Foundations of Web Security & Ethical Hacking (20 Hours, 5 Sessions)

Introduction to the OWASP Top 10 & Bug Bounty Programs

Introduction to Cybersecurity & Web Security

Reconnaissance & Information Gathering (24 Hours, 6 Sessions)

OSINT Techniques & Target Enumeration

Automated Recon Pipelines for Bug Bounty Hunting

Authentication & Access Control Bypasses (28 Hours, 7 Sessions)

Broken Authentication & Session Management Exploits

2FA Bypass Techniques & Logic Flaws

Business Logic & Logical Vulnerabilities (28 Hours, 7 Sessions)

Understanding Logical Flaws in Web Applications

CAPTCHA & Rate Limiting Bypasses.

Client-Side Security & Cross-Site Attacks (24 Hours, 6 Sessions)

Hands-on Labs: PortSwigger - XSS Exploits

Clickjacking & UI Redressing Attacks

Path Traversal & File-Based Attacks (24 Hours, 6 Sessions)

Hands-on Labs: PortSwigger - Path Traversal

Misconfigured File Upload Vulnerabiliti

Advanced HTTP Request Smuggling &Web Desync Attacks (24 Hours, 6 Sessions)

Hands-on Labs: PortSwigger - HTTP Smuggling

Identifying Frontend-Backend Parsing Discrepancies

Supply Chain Attacks & Emerging Threats (24 Hours, 6 Sessions)

Hands-on Labs: PortSwigger - Supply Chain Attacks

Exploiting Open-Source Dependencies in Web Applications