Bug Bounty Course by CyberBlockz

Instructor: Pranay from CyberBlockz

60 Hours | Telugu

Table of Contents

1. Introduction to Bug Bounty Programs
2. OWASP Top 10 Vulnerabilities
3. Advanced Vulnerabilities
4. Bug Bounty Tools
5. Reporting Bugs and Guidelines
6. Case Studies
7. Web Patch Management
8. Labs and Practical Assessments
9. Prerequisites

Bug Bounty Course by CyberBlockz

Introduction to Bug Bounty Programs

- What is Bug Bounty?
- Overview of Pentesting
- Ethical Hacking and its Legal Implications

OWASP Top 10 Vulnerabilities

1. Injection (SQL, Command Injection)
2. Broken Authentication
3. Sensitive Data Exposure
4. Security Misconfiguration
5. Cross-Site Scripting (XSS)
6. Broken Access Control

Advanced Vulnerabilities

1. Parameter Tampering
2. Local and Remote File Inclusion (LFI)
3. Server-Side Request Forgery (SSRF)
4. Cross-Site Request Forgery (CSRF)

Bug Bounty Heavy Tools

- BurpSuite Pro: Hands-on labs for testing vulnerabilities
- Nikto: Web vulnerability scanning
- OWASP ZAP: Automation strategies
- Nessus: Automation for pentesting

Reporting Bugs and Guidelines

- How to Write Clear Bug Reports

- Vulnerability Disclosure Best Practices

Case Studies

- Real-world case studies of bug bounty hunters.

Web Patch Management

- Importance of patch management.

- Techniques to manage patches.

Labs and Practical Assessments

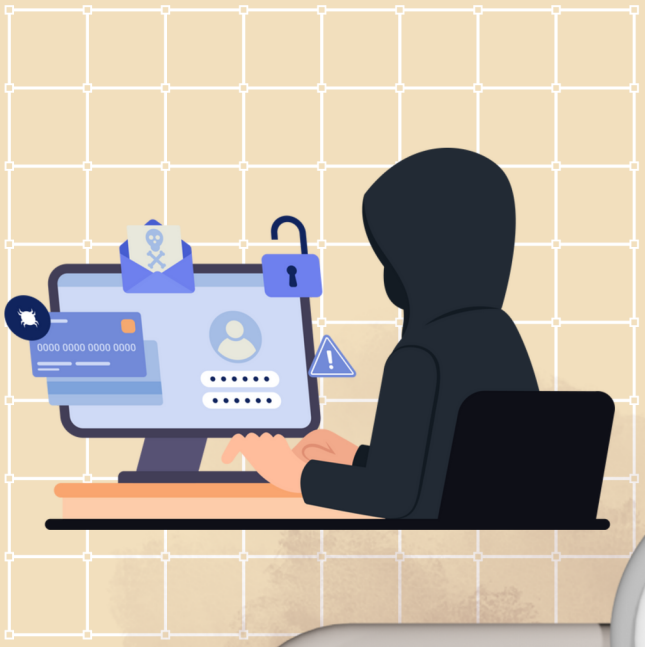
- Hands-on practice with vulnerable applications.

- Capture the Flag (CTF) challenges.

Prerequisites

- Basic Networking Skills

- Knowledge of Kali Linux Operating System



CONTACT US :

rajesh@cyberblockz.in

+91 8074557618

@cyberblockz_official

@cyberblockz

https://b3.cyberblockz.in