Mr.Hacker

Bug Bounty Masterclass

Ethical Hacking · Web Penetration Testing · Responsible Disclosure

✔ *All techniques are practised on authorised platforms only (HackerOne, Bugcrowd, personal lab environments). Unauthorised testing is illegal.*

9 Sections	24+ Lessons	Beginner → Expert	Real-World Labs

■ SECTION 1

Introduction to Bug Bounty

- › An Overview of Ethical Hacking
  #intro
- › Understanding the Importance of Ethical Hacking
  #importance
- › The Role of an Ethical Hacker
  #roles

■ SECTION 2

Setting Up the Environment

- › Install Burp Suite Professional on Windows 10
  #setup
  - · Download & Install Burp Suite
  - · Configure Burp Suite for testing
- › Create AWS Linux Instance
  #aws
  - · AWS Account Setup & Linux Distribution
  - · Instance Configuration & Launch

■ SECTION 3

Learning the Basics

- › HTML Injection on a Real Website
  #basics
  - · Understand HTML Injection
  - · Identify Vulnerabilities & Exploitation
- › Data Tampering on a Real Website
  #dataTampering
  - · Identify & Exploit Data Tampering
- › Open Redirect on a Real Website
  #openRedirect
  - · Identify & Exploit Open Redirect

■ SECTION 4

Advanced Techniques

- › Cross-Site Request Forgery (CSRF)
  #csrf
  - · Understand, Identify & Exploit CSRF
- › Password Reset Poisoning
  #passwordResetPoisoning
  - · Understand, Identify & Exploit Reset Poisoning
- › Account Takeover via Password Reset Poisoning
  #accountTakeover
  - · Full walkthrough: Identify & Exploit ATO

■ SECTION 5

Expert Techniques

› Cross-Site Scripting (XSS) on a Real Website

#xss

- · Understand XSS types (Reflected, Stored, DOM)
- · Identify & Exploit XSS vulnerabilities

› Bypass OTP on a Real Website

#otpBypass

- · Understand OTP Bypass logic flaws
- · Identify & Exploit OTP weaknesses

■ SECTION 6

Mastering Techniques

› File Upload Bug on a Real Website

#fileUploadBug

- · Understand & Exploit file upload misconfigurations

› Blind XSS on a Real Website

#blindXSS

- · Understand Blind XSS vs standard XSS
- · Identify & Exploit Blind XSS

› Bypass Payment Gateway on a Real Website

#paymentGatewayBypass

- · Understand payment logic flaws
- · Identify & Exploit payment bypass

› Local File Inclusion → Remote Code Execution

#LFIToRCE

- · Identifying LFI in real websites
- · Exploiting LFI to achieve RCE
- · Mitigation & prevention strategies

■ SECTION 7

JWT Token Security

› Understanding JWT Tokens

#jwttokens

- · How JWT works & common vulnerabilities
- · How to secure JWT implementations

› Account Takeover via JWT Tokens

#hack_via_jwt

- · Real-life walkthrough of JWT exploitation
- · Prevention measures & secure signing

■ SECTION 8

SQL Injection & Credentials

› Finding SQL Injection in Real Websites

#sqlinjection

- · Identifying & exploiting SQL injection
- · Mitigation strategies

› Finding Exposed Admin Credentials

#admincredentials

- · Discovering misconfigured admin endpoints
- · Best practices for securing admin access

› Auto Login Admin Account Vulnerabilities

#autologin

- · How auto login can be exploited
- · Safeguarding against auto login flaws

■ SECTION 9

Course Wrap-Up

› Summary of the Course

#summary

› Future Learning Path

#futureLearning

- · Recommended certifications: eWPT, OSCP, BSCP
- · Bug bounty platforms: HackerOne, Bugcrowd, Intigriti