

# TABLE OF CONTENT

1

## Introduction to Bug Bounty

---

- What is a Bug Bounty Program?
- Popular Bug Bounty Platforms
- Bugcrowd (Demo)
- HackerOne(Demo)
- Benefits of Bug Bounty
- Brief About Common Vulnerabilities
- Hacking Terminologies

2

## Information Gathering Basics

---

- What is Information Gathering?
- Concept of Digital Footprinting
- What Information to gather?
- What is Whois Information
- Information gathering about People & Organization
- Gathering Information about Websites
- Google Dorking & GHDB

3

## Setting Up Labs

---

- DVWA Introduction & Configuration
- bWAPP Introduction & Configuration

4

## Introduction to Burp Suite

---

- Introduction to Burp Suite
- Steps to Configure (Demo)

5

## SQL Injection

---

- Introduction to SQL
- Writing Basic SQL Query
- Different types of comments used in SQL

6

- SQLi Introduction & Impact
- Union Based SQLi (Demo)
- Boolean Based SQLi
- Time Based SQLi

## Web Application Attacks

---

- Validation Bypass (Client and Server)
- IDOR Vulnerability
- IDOR on bWAPP
- Rate Limiting Flaw
- File Upload Vulnerability
- File Upload on DVWA
- Live IDOR POC
- Live Rate Limiting Flaw POC

7

## Cross site Script

---

- What Is Cross Site Scripting(XSS)?
- Stored XSS
- Stored XSS (DVWA)
- Reflected XSS
- Reflected XSS (DVWA)
- DOM based XSS
- Blind XSS
- Live XSS POC

8

## Header Injection & URL Redirection

---

- Host Header Injection methods & URL redirection
- Live Host Header Injection POC
- Live URL Redirection POC

9

## Client Side Attack

---

- Understanding Session, Cookies & Session Fixation
- Forced Browsing
- Cross Site Request Forgery Introduction
- CSRF Attack(DVWA)
- Open Redirections
- Personally Identifiable Information (PII) Leakage
- Sensitive Information Disclosure
- Live CSRF POC
- Live Sensitive Information POC
- Live Session Fixation POC

10

## Brute Forcing

---

- Brief about Brute Force
- Brute Force (DVWA)
- Live OTP Brute Force POC

11

## Security Misconfigurations & Exploiting Web Apps

---

- Security Misconfigurations & Improper File Handling
- Guessing Weak Passwords
- Live SPF Record Missing POC

12

## Insecure CORS

---

- Concept about CORS

13

## File Inclusion

---

- Local File Inclusion
- Remote File Inclusion
- File Inclusion (DVWA)
- Live LFI POC

14

## Server-Side Request Forgery

---

- What is SSRF?

15

## Insecure Captcha

---

- Brief about Insecure Captcha
- Live Captcha Bypass POC

16

## Automating VAPT & Advanced Information Gathering

---

- Introduction to Automated VAPT & Advance Level Information Gathering

17

## Documenting & Reporting Vulnerability

---

- Introduction to VAPT Reporting

18

## Conclusion

---

- Conclusion of Bug Bounty