INFOSECTRAIN

INTRODUCTION TO BUG BOUNTY HUNTING

Bug Bounty Hunting

Become an expert bug bounty hunter with Infosectrain. Join InfosecTrain's Bug Bounty Hunting training course to get a clear and complete idea of Bug Bounty Hunting.

Overview

Many websites, organizations, and software companies provide bug bounty programs in which users can gain credit and reward for reporting bugs, security exploits, and vulnerabilities. These programs help developers find and fix flaws before they are discovered by malicious hackers or the broader public, preventing widespread exploitation.

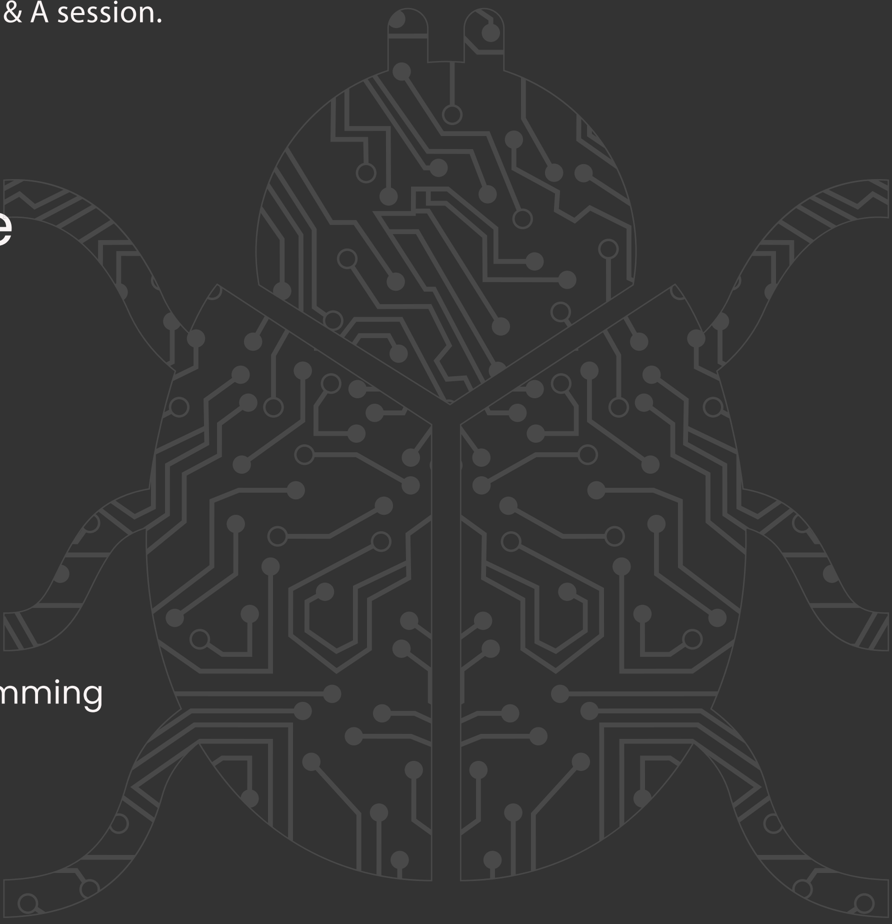
The ultimate Bug Bounty Hunting course will teach you how to seek and exploit application vulnerabilities using the necessary tools and

techniques. This course aims to provide ethical hackers with the skills they'll need to identify and disclose vulnerabilities.

Bug Bounty Hunting

InfosecTrain is one of the finest security and technology training and consulting organizations, focusing on a range of IT security training and Information Security services. InfosecTrain offers complete training and consulting solutions to its customers globally. InfosecTrain consistently delivers the industry's highest quality and best success rate, whether the requirements are technical services, certification, or customized training.

- We have certified and highly experienced trainers who have an in-depth knowledge of the subject.
- Our training schedule is flexible and we also provide recordings of the lectures.
- We deliver post-training support.
- We also bring forth an interactive Q & A session.



Target Audience

- Software Security Analyst
- Bug Bounty Programmer

Pre-Requisites

- Working knowledge of programming

Course Objectives

- Understanding of Kali Linux Fundamentals
- Familiarity with Penetration Testing
- Knowledge of Red Teaming
- Understanding the responsibilities of SOC
- Basic knowledge of Networking
- XSS and XXE Vulnerability Identification
- Acquaintance with Burp Suite
- SQL Injection Identification

Course Content

1. About Cyber Security Industry

> What is Bug Bounty
> What is Penetration Testing
> What is Red Teaming
> What is SOC
> Needs to be a Professional Bug Hunter

2. Setting up Hacking Machine

> Introduction to Linux Environment

3. Introduction to Networking

4. Web Application Fundamentals & Configurations

> HTTP and HTTPS Protocol
> HTTP Requests & HTTP Response
> URL & URI
> HTTP Methods
> HTTP Response Status Codes
> SOP & CORS

5. Introduction to Web Application Security Testing

> Types of Web Application Security Testing
> Approach for Web App Penetration Testing

6. Web Application Reconnaissance

7. Working with Burp suite

8. Exploiting Traditional Web Application Vulnerabilities

> Sub Domain Take Over o Click Jacking
> Checking Necessary Security Headers
> Checking SPF & DMARC Record
> CORS (Cross-Origin Resource Sharing)
> Testing Rate Limit

9. Introduction to Session Managements

> What is Session Management
> Testing Weak Session Logout Policy
> Testing For Session Timeout
> Session Fixation Vulnerability

10. Introduction to XSS (Cross-Site Scripting)

> Exploiting Reflected XSS
> Exploiting Stored XSS
> Exploiting DOM XSS

11. Introduction to SQL injection

> Logic behind SQL injection
> Authentication Bypass using SQL injection
> Error Balancing in SQLi
> Information Disclosure (Exploiting Database) through SQL injection
> Automate SQL injection Process

12. Introduction to File Inclusion Vulnerability

> Exploiting LFI
> Exploiting RFI

13. CSRF (Cross-Site Request Forgery Attack)

14. SSRF (Server-Side Request Forgery Attack)

> Exploiting Blind SSRF

15. IDOR (Insecure Direct Object Reference)

16. OS Command injection

17. Response Manipulation

18. Host Header Injection

19. Parameter Tampering

20. XXE (XML External Entity)

21. RCE (Remote Code Execution)

22. Introduction to Bug Bounty Platforms

> Hackerone
> Bug Crowd
> Open Bug Bounty Programs

23. Preparation for Cyber Security Interview

INFOSECTRAIN

www.infosectrain.com | sales@infosectrain.com