

# BUG BOUNTY

**TRAINING & PROGRAM**

POWERED BY IGNITE TECHNOLOGIES



# BUG BOUNTY

A Bug Bounty program is a crowdsourcing initiative hosted by the organizations in order to give a platform to security researchers and white hat hackers from across the globe to showcase their skills and discover any security holes in their infrastructure. Depending upon the severity level of the bug reported and the details presented within the Proof of Concept (POC), they are either rewarded with remuneration or recognition as a token of appreciation.

While a large majority of the bug bounty programs are public, certain are private events and are strictly invite-based. Such programs have stringent terms and conditions that the invitees must always abide by

During this course, you will acquire knowledge in the fundamentals of application security vulnerabilities and penetration testing.

## PREREQUISITES

In order to initiate the Bug Bounty Training, you should be aware of the basic concepts of the development web-applications; frontend and backend



COURSE DURATION: 25 to 30 HOURS

## Why to choose Ignite Technologies?

Ignite believes in “Simple Training makes Deep Learning” which help us in Leading International CTF market.

- Ignite Technologies is leading Institute which provides Cyber Security training from Beginner to Advance as mention below:

1. Networking
2. Ethical hacking
3. Bug Bounty
4. Burp Suite for Pentester
5. Windows for Pentester
6. Linux for Pentester
7. Computer Forensic
8. CTF-2.0
9. Privilege Escalation
10. Red Team Operations
11. Infrastructure Penetration Testing
12. API Penetration Testing
13. Android Penetration Testing

- World RANK -1st, in Publishing more than 400 walkthroughs (Solution) of CTFs of the various platform on our reputed website "[www.hackingarticles.in](http://www.hackingarticles.in)".
- We Provide Professional training that includes real-world challenges.
- Ignite's Students are placed in a TOP reputed company in the overworld.
- Hands-on Practice with 80% Practical and 20% Professional Documentation.
- ONLINE classes are available

## Career in IT Security Domain:

Chief Information Security  
Senior Security Consultant  
Cryptographer  
Penetration Tester  
Researcher

Officer Incident Analyst | Responder  
Software code Analyst  
Risk Controller  
Security Architect  
Exploit Developer

Information Security Analyst  
Digital Forensic Expert  
International Trainer  
Security Engineer  
Ethical Hacker

# COURSE OVERVIEW

## 1. INTRODUCTION

- Introduction Web Servers & Web Applications
- The Bug Bounty Program
- Web Application Penetration Testing & its methodologies
- Introduction to HTTP Protocol
- OWASP & its Top 10
- Introduction to Burp Suite

## 2. PENTEST LAB SETUP

- Web Applications Installation on Windows
- Web Application Installation on Ubuntu
- Web Application Installation on Docker
- Web Application Installation on AWS

## 3. INFORMATION GATHERING & RECONNAISSANCE

- What Is Information Gathering?
- Information Gathering Cheatsheet
- DNS Enumeration
- Perform Web Application Fingerprinting
- Spider/Crawl For Missed or Hidden Content Directory Brute Forcing
- Google Advanced Search

## **4. NETCAT FOR PENTESTER**

- Introduction to Netcat
- Netcat as Banner Grabber
- Netcat File Transfer
- Netcat Reverse Shell
- Netcat Shells Over Payload

## **5. CONFIGURATION MANAGEMENT TESTING**

- Enumerate Infrastructure and Application Admin Interfaces
- Check For Backup and Unreferenced Files for Sensitive Information
- Check HTTP Methods Supported And Cross Site Tracing (XST)
- Test File Extensions Handling
- HTTP Strict Transport Security
- Test Network/Infrastructure Configuration

## **6. CRYPTOGRAPHY**

- Check SSL Version, Algorithms, Key Length
- Check For Digital Certificate Validity (Duration, Signature And Cn)
- Check Credentials Only Delivered Over Https
- Check That The Login Form Is Delivered Over Https
- Check Session Tokens Only Delivered Over Https
- Check If Http Strict Transport Security (Hsts) In Use

## **7. AUTHENTICATION**

- What is Authentication?
- HTTP Authentication Exploitation
- Introduction to Broken Authentication
- Broken Authentication Exploitation.

- Test For User Enumeration
- Test For Bruteforce Protection
- Test For Default Logins
- Test Password Reset and/or Recovery
- Test Password Change Process
- Test CAPTCHA
- Test Password Quality Rules
- Test For Autocomplete on Password Forms/Input
- Mitigation Steps

## **8. SESSION MANAGEMENT**

- What are Sessions and Cookies?
- Introduction to Session Management
- Check session tokens for cookie flags
- Check session cookie duration
- Test session cookies for randomness
- Insecure Session Exploitation
- Mitigation Steps

## **9. LOCAL FILE INCLUSION**

- Introduction to Local File Inclusion
- Basic LFI Technique
- Null byte Technique
- Base64 Technique
- Fuzzing Technique
- LFI Suite

- LFI over File Upload
- LFI Log Poisoning
- Mitigation Steps

## 10. REMOTE FILE INCLUSION

- Introduction to RFI
- Why Remote file Inclusion Occurs?
- Remote File Inclusion Exploitation
- Basic Remote File Inclusion
- Reverse Shell through Netcat
- RFI over Metasploit
- Bypass a Blacklist Implemented
- Null Byte Attack
- Exploitation through SMB Server
- Mitigation Steps

## 11. PATH TRAVERSAL

- Linux Server Path Traversal Exploitation
- Basic Path Traversal
- Blocked Traversal Sequence
- Validated Path Traversal
- Path Disclosure in URL
- Null Byte Bypass
- Windows Server Path Traversal Exploitation
- Basic Path Traversal
- Double dots with Forward-Backward Slashes
- Blocked Traversal Sequences

## **12. OS COMMAND INJECTION**

- Introduction to Command Injection
- How Command Injection Occurs?
- Metacharacters
- Types of Command Injection
- Impact of OS Command Injection
- Manual Exploitation
- Exploitation through Automated tools
- Blind OS Command Injection
- Detection
- Exploitation
- Mitigation Steps

## **13. OPEN REDIRECT**

- Introduction to Open Redirection
- Open Redirection Impact
- Open Redirection Exploitation
- Basic Redirection
- Encoded Redirection
- URL Redirection with Hash Values
- Redirection with Hash Values Using Salt.
- Redirection over inside a Web Page
- DOM-Based Open Redirection
- Mitigation Steps



## **14. UNRESTRICTED FILE UPLOAD**

- Introduction to Unrestricted File Upload
- Impact of Unrestricted File Upload
- File Upload Exploitation
- Basic File Upload
- Content-Type Restriction
- Double Extension File Upload
- Image Size Validation Bypass
- Blacklisted Extension File Upload
- Mitigation Steps

## **15. PHP WEB SHELLS**

- Introduction of PHP Web shells
- simple backdoor.php
- qsd-php backdoor web shell
- php-reverse-shell.php
- Metasploit php shell
- Weevely php web shell
- PHP bash web shell

## **16. HTML INJECTION**

- Overview to Hyper Text Markup language
- Introduction to HTML Injection
- Impact of HTML Injection

- HTML Injection v/s XSS
- Types of Injection
- Stored HTML
- Mitigation Steps

## 17. Cross-Site Scripting (XSS)

- What is JavaScript?
- JavaScript Event Handlers
- Introduction to Cross-Site Scripting (XSS)
- Impact of Cross-Site Scripting
- Types of XSS
- Reflected XSS Exploitation
- Stored XSS Exploitation
- DOM-based XSS Exploitation
- Cross-Site Scripting Exploitation using Burp Suite
- Mitigation Steps

## 18. CLIENT-SIDE REQUEST FORGERY

- Introduction to Cookies & Session ID's
- Introduction to SOP & CORS
- Introduction to CSRF Vulnerability
- CSRF Tokens & Their Exploitation
- Mitigation Steps

## 19. SQL INJECTION

- What are Databases?
- Introduction to SQL Injection
- SQL Injection Error Based
- SQL Injection via SQLmap
- Manual SQL Exploitation
- Boolean Based Exploitation
- SQL Injection Form Based Exploitation
- Authentication Bypass
- Remote Code Execution with SQLmap
- Mitigation Steps

## 20. XXE INJECTION

- Introduction to XML
- Introduction to XXE Injection
- XXE for SSRF
- XXE Billion Laugh Attack
- XXE Exploitation
- Blind XXE
- Mitigation Steps

## 21. BONUS SECTION

- Automated Vulnerability Scanner
- Firefox Add-ons
- Encoding Methods
- Reporting

THIS COURSE IS DESIGNED  
THAT COVERS ALL MAJOR  
VERTICALS OF **OWASP** WEB  
APPLICATION SECURITY  
TESTING GUIDE V4.