

# Bug Bounty Bootcamp – 2 Months

## Course Overview

The **Bug Bounty Bootcamp (2 Months)** is a **practical, industry-focused training program** designed to take students from **beginner to advanced level** in real-world bug bounty hunting.

This bootcamp is **not theory-based**. Every concept is taught using **live target websites, real vulnerabilities, and hands-on exploitation techniques** used by professional bug bounty hunters.

## Course Structure & Learning Modules

This bootcamp includes **21 Premium Vulnerability Modules, 5 Extra Advanced Modules, and Latest CVEs**, all covered in **deep technical detail**.

## Class Schedule & Mode

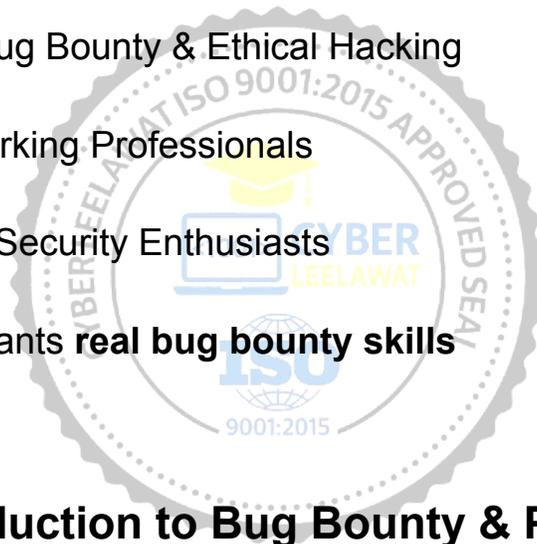
- **Duration:** 2 Months
- **Classes:** Monday to Friday
- **Mode:** Live on Google Meet
- **Practice:** Live Websites
- **Language:** 100% Hindi

## Recordings & Support

- Full Class Recordings Provided
- Lifetime Access to Recordings
- Live Doubt Solving Sessions
- Community Support Group

## Who Should Join This Bootcamp?

- Beginners in Bug Bounty & Ethical Hacking
- Students & Working Professionals
- Freelancers & Security Enthusiasts
- Anyone who wants **real bug bounty skills**



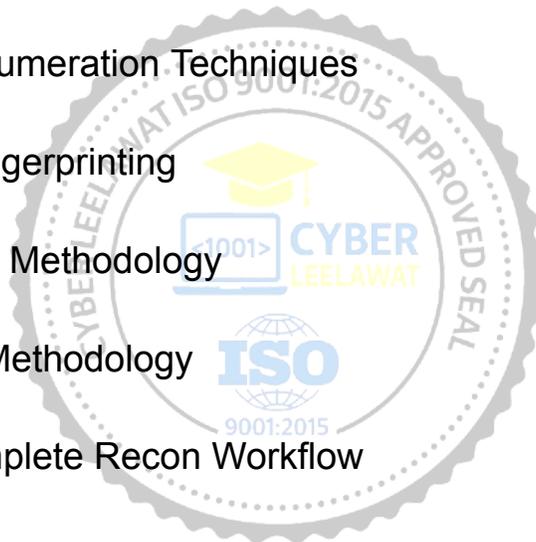
## Module 1: Introduction to Bug Bounty & Platforms

- What is Bug Bounty?
- How Bug Bounty Programs Work
- Platforms Overview:
  - HackerOne
  - Bugcrowd

- Intigriti
- Public vs Private Programs
- Bug Bounty Mindset & Ethics

## **Module 2: Target Selection & Recon (Detailed)**

- Understanding Scope Properly
- Asset Identification
- Subdomain Enumeration Techniques
- Technology Fingerprinting
- Passive Recon Methodology
- Active Recon Methodology
- Building a Complete Recon Workflow



## **Module 3: Email Security (SPF / DKIM / DMARC)**

- How Email Spoofing Works
- Understanding SPF, DKIM & DMARC
- Detecting Missing or Weak Configurations
- Real-World Email Security Misconfigurations

## Module 4: Origin IP Disclosure (Deep Level)

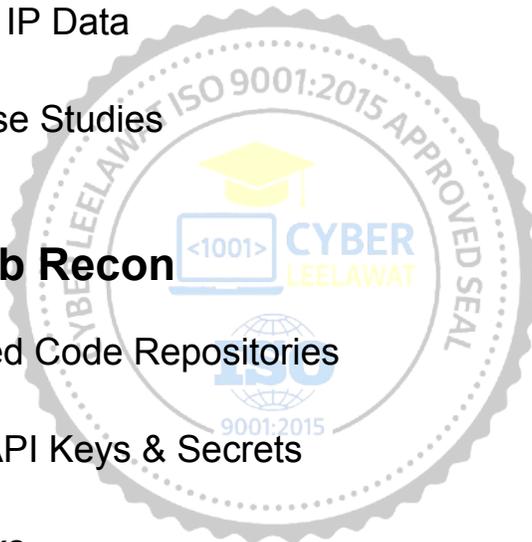
- Understanding CDN & WAF Protection
- Cloudflare Bypass Techniques
- Finding Origin IP via:
  - DNS Records
  - HTTP Headers
  - Historical IP Data
- Real-World Case Studies

## Module 5: GitHub Recon

- Finding Exposed Code Repositories
- Searching for API Keys & Secrets
- Credential Leaks
- Configuration File Exposure
- Automating GitHub Recon

## Module 6: JavaScript Recon

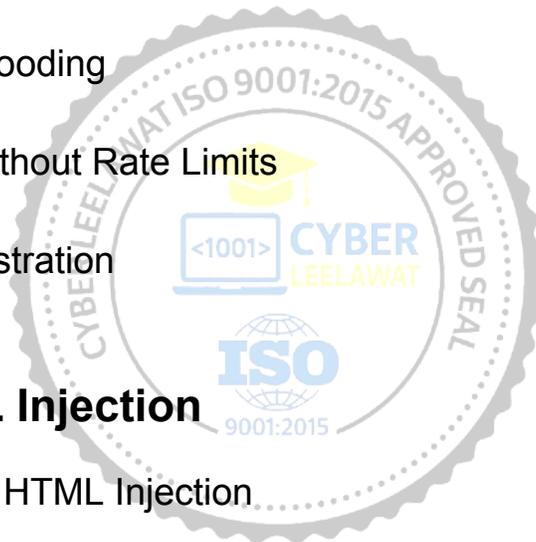
- JavaScript File Analysis



- Finding Hidden Endpoints
- Extracting Tokens & API Keys
- Client-Side Logic Flaws

## **Module 7: No Rate Limit Vulnerabilities**

- Understanding Rate Limiting
- API Abuse
- OTP & SMS Flooding
- Brute Force Without Rate Limits
- Impact Demonstration



## **Module 8: HTML Injection**

- Understanding HTML Injection
- UI-Based Injection Attacks
- Input Validation Bypass
- Real Impact Scenarios

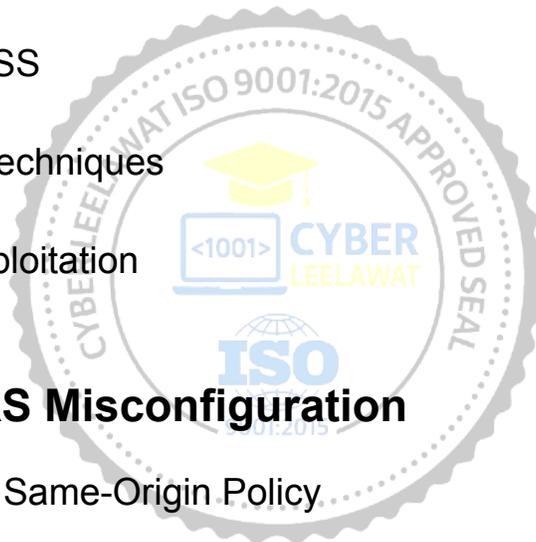
## **Module 9: Exif Data Leakage**

- Understanding Image Metadata

- Extracting Sensitive Information from Images
- Tools & Techniques
- Real-World Examples

## **Module 10: Cross-Site Scripting (XSS) – All Types**

- Reflected XSS
- Stored XSS
- DOM-Based XSS
- Filter Bypass Techniques
- Real-World Exploitation



## **Module 11: CORS Misconfiguration**

- Understanding Same-Origin Policy
- Weak CORS Implementations
- Exploiting Misconfigured CORS
- Data Theft via CORS

## **Module 12: IDOR (Insecure Direct Object Reference)**

- Broken Access Control Concepts

- Identifying IDOR Vulnerabilities
- Horizontal & Vertical Privilege Escalation
- Real-World IDOR Exploits

## **Module 13: CSRF (Cross-Site Request Forgery)**

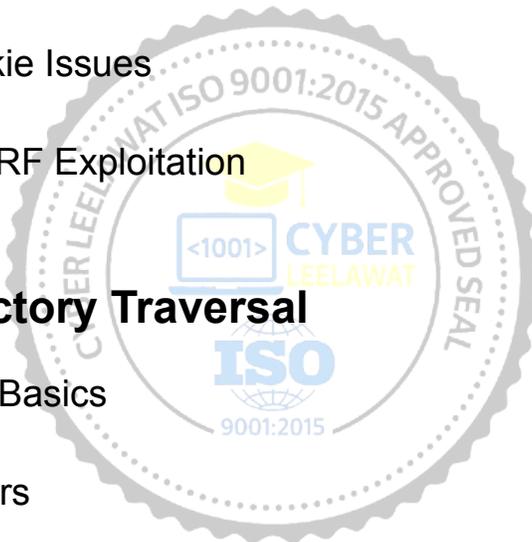
- Understanding CSRF Attacks
- Token Validation & Bypass
- SameSite Cookie Issues
- Real-World CSRF Exploitation

## **Module 14: Directory Traversal**

- Path Traversal Basics
- Bypassing Filters
- Reading Sensitive Files
- Real Server Exploitation

## **Module 15: File Upload Vulnerabilities**

- Understanding File Upload Logic
- Bypassing File Type Restrictions



- Uploading Web Shells
- Achieving Remote Code Execution

## **Module 16: SSTI (Server-Side Template Injection)**

- Understanding Template Engines
- Identifying SSTI
- Payload Development
- Server-Side Code Execution

## **Module 17: Open Redirect**

- Understanding Open Redirect Issues
- Redirect Chain Attacks
- Phishing & Token Theft Scenarios
- Real-World Impact

## **Module 18: OTP Bypass**

- OTP Logic Flaws
- Verification Bypass Techniques
- Reuse & Brute Force Issues



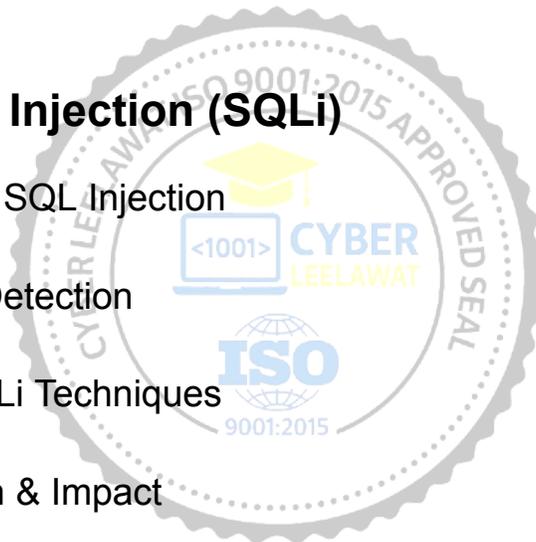
- Business Impact Analysis

## **Module 19: Business Logic Flaws**

- Understanding Application Logic
- Identifying Logical Vulnerabilities
- Real-World Exploitation
- High-Impact Bug Reports

## **Module 20: SQL Injection (SQLi)**

- Understanding SQL Injection
- Manual SQLi Detection
- Automated SQLi Techniques
- Data Extraction & Impact



## **Module 21: SSRF (Server-Side Request Forgery)**

- Understanding SSRF
- Accessing Internal Services
- Cloud Metadata Exploitation
- Real-World SSRF Attacks