

- **Course Name :** Bug Bounty Program
- **Course Duration :** 60 hrs
- **Course Fee :** INR 10,000/participant

✓ **Pre-requisites:** Basic knowledge of Hacking

✓ **Course Module:**

**1. Introduction to Web-Application Penetration**

- a. Black Box Testing
- b. White Box Testing

**2. Introduction to OWAP**

- a. Top 10 Vulnerability

**3. Attacking the Authentication**

- a. Username Enumeration
- b. Invalid username with Invalid password
- c. Valid username with invalid password
- d. Exploiting Password Reset features

**4. Brute Force Attack and Dictionary Attack**

- a. Bypassing Brute Force Security
- b. Bypassing Brute Force Security By Changing User-Agent

**5. CAPTCHA Bypass**

- a. CAPTCHA Validation Flaw
- b. CAPTCHA Reset Flaw
- c. Manipulating User-Agent

**Ignite Technologies**

**Powered by RMAR Technologies Pvt. Ltd.**

**Corporate Office:** 3<sup>rd</sup> Floor, 26 Pusa Road, Adjoint Karol Bagh Metro Station Gate No. 4, New Delhi, India

**Email:** [rahul@ignitetechnologies.in](mailto:rahul@ignitetechnologies.in) **Contact No.:** +91-9599387842,

**Website:** [www.ignitetechnologies.in](http://www.ignitetechnologies.in) [www.rmar.in](http://www.rmar.in)

## 6. SQL Injection

- a. What is SQL Injection
- b. Types of SQL Injection
- c. Union Based SQL Injection
- d. Error Based SQL Injection
- e. Bling SQL Injection

## 7. Testing for SQL Injection

- a. Enumerating DB User
- b. Enumerating Tables
- c. Enumerating Columns
- d. Extracting Data from Columns

## 8. XSS ( Cross-site Scripting )

- a. How to identify XSS Vulnerability
- b. Types of Cross-Site Scripting
- c. Persistent XSS and Non Persistent XSS
- d. Vulnerable codes and Payloads

## 9. Exploiting XSS Vulnerability

- a. Cookie Stealing with XSS
- b. Exploiting XSS for Conducting Phishing Attack

## 10. Privilege-Escalation Vulnerability

- a. Live Examples on Vulnerability

**Ignite Technologies**

**Powered by RMAR Technologies Pvt. Ltd.**

**Corporate Office:** 3<sup>rd</sup> Floor, 26 Pusa Road, Adjoint Karol Bagh Metro Station Gate No. 4, New Delhi, India

**Email:** [rahul@ignitetechnologies.in](mailto:rahul@ignitetechnologies.in) **Contact No.:** +91-9599387842,

**Website:** [www.ignitetechnologies.in](http://www.ignitetechnologies.in) [www.rmar.in](http://www.rmar.in)

11. **CSRF ( Cross Site Request Forgery )**
  - a. How to Attack
  - b. GET Based CSRF
  - c. POST Based
  
12. **CSRF Protection Techniques**
  - a. Referrer Based Checking
  - b. Anti CSRF Tokens
  
13. **CSRF Token Bypass**
  - a. Tokens not Validated upon Server
  - b. Analyzing Weak Anti-CSRF Token
  - c. Bypassing CSRF with XSS
  
14. **Broken Authentication and Session Management**
  
15. **Insecure Direct Object Reference ( IDOR )**
  
16. **Security Misconfiguration**
  
17. **Sensitive Data Exposure**
  
18. **Un-validated Redirect and Forwards**
  
19. **Rate Limiting**
  - a. Bypassing Rate Limiting
  - b. Changing User-Agent to bypass Rate Limiting

**Ignite Technologies**

**Powered by RMAR Technologies Pvt. Ltd.**

**Corporate Office:** 3<sup>rd</sup> Floor, 26 Pusa Road, Adjoint Karol Bagh Metro Station Gate No. 4, New Delhi, India

**Email:** [rahul@ignitetechnologies.in](mailto:rahul@ignitetechnologies.in) **Contact No.:** +91-9599387842,

**Website:** [www.ignitetechnologies.in](http://www.ignitetechnologies.in) [www.rmar.in](http://www.rmar.in)

20. Clickjacking Vulnerability
21. Business Logic Bugs
22. Some Ways to Find Logical Vulnerability
  - a. Misusing Features of Application
  - b. Exploring Functionality & their Weakness
  - c. Chaining of Different Vulnerability
  - d. Out of the box thinking & Experimentation
23. Writing Exploitation Codes in PHP
24. Burp Tools and Mozilla Extension
  - a. Burp Suite
  - b. Data Tamper
  - c. Live – HTTP Header
  - d. User-Agent Switcher
  - e. Hackbar
25. Mobile App Security Testing
  - a. Leaking of Tokens
  - b. Insecure Storage and etc.
26. Bug Bounty
  - a. Where to start
  - b. How to Report Bugs in Prope3r and Efficient Way

**Ignite Technologies**

**Powered by RMAR Technologies Pvt. Ltd.**

**Corporate Office:** 3<sup>rd</sup> Floor, 26 Pusa Road, Adjoint Karol Bagh Metro Station Gate No. 4, New Delhi, India

**Email:** [rahul@ignitetechnologies.in](mailto:rahul@ignitetechnologies.in) **Contact No.:** +91-9599387842,

**Website:** [www.ignitetechnologies.in](http://www.ignitetechnologies.in) [www.rmar.in](http://www.rmar.in)