

# BURP SUITE FOR PENTESTER

**iGNITE**  
Technologies



TRAINING & PROGRAM POWERED BY  
IGNITE TECHNOLOGIES

**Enroll Now**



[www.ignitetechnologies.in](http://www.ignitetechnologies.in)



+91 959 938 7841

# BURP SUITE FOR PENTESTER

Bug Bounty without Burp Suite? Impossible to think that of!! In today's era, web-application penetration testing is one of the most significant field in the Information Security concept. However, within all this, Burp Suite plays a major role, whether it's a basic web-application scan or the exploitation for the identified vulnerabilities, burp suite does it all.

This course will covers up everything that could help you to move forward over with your Bug Bounty journey. The fruitful essence of the course is its systemic structure & real Environment Practice with about 50+ hands-on practical over Burp Suite's Professional Edition from the Basics to Advanced.

## Prerequisites

There is nothing as such in-advanced you need to aware of before initiating this course, but still it would be a great learning if the candidate is aware of the known-vulnerabilities and the OWASP TOP 10.

Burp Suite for Pentester would be plus point for the students who have already enrolled with the Ignite's Bug Bounty Program.



**COURSE DURATION: 12 to 15 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. Network Penetration Testing -2.0
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 walkthrough (Solution) of CTFs of the various platform on our reputed website “[www.hackingarticles.in](http://www.hackingarticles.in)”.

• We Provide Professional training that include real world challenges.

• Ignite’s Student are placed in TOP reputed company in over world

• 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

## INTRODUCTION TO BURP SUITE

Burp Suite - An Overview  
Burp Suite Installation  
Configuring Burp Proxy for Web Applications

- o Manual Configuration
- o Using Browser's Extension

Configuring Burp Proxy for Android Applications

## THE BURP COLLABORATOR

Introduction to Burp Collaborator  
Detecting vulnerabilities with Collaborator Client

- o Blind OS Command Execution
- o Cross-Site Scripting Detection
- o Blind XXE
- o Server-Side Request Forgery
- o Fuzzing for SSRF Detection

## BURP SUITE AS A VULNERABILITY SCANNER

Introduction to Burp's Crawler  
Auditing Applications with Burp Suite  
Advanced Crawling & Scanning  
Burp Suite's Task tab

## BURP SUITE FUNDAMENTALS

Initiating with the Project Options  
Intercepting HTTP Browser's Request  
Fuzzing with Intruder  
HTTP Response with Repeater  
The Sequencer & Comparer tabs  
Burp Clickbandit  
Save Output Results

## THE BURP'S HACK BAR

Introduction to Hack Bar  
The Hack Bar Installation  
Exploiting vulnerabilities with Hack Bar

- o SQL Injection
- o SQLi Login Bypass
- o Cross-Site Scripting
- o Local File Inclusion
- o XXE Injection
- o Unrestricted File Upload
- o OS Command Injection

## ADVANCED FUZZING

Introduction to Fuzzing

Burp Suite as a Fuzzer

Fuzzing with built-in payloads

- o Fuzzing for Login credentials.
- o Fuzzing for SQL Injection
- o Fuzzing to find Hidden Files
- o Fuzz to find Restricted File

Upload Extensions

- o Fuzzing for Cross-Site Scripting
- o Fuzzing for OS Command

Injection

- o Fuzzing for Hidden Directories
- o Fuzzing for HTTP Verb

Tampering

- o Manipulate Burp Suite's pre-defined payloads

- o Injecting our customized payload lists.

Fuzzing with the Attack Type

- o Cluster Bomb
- o Battering ram
- o Pitchfork

Fuzzing with the Payload Types

- o Brute forcer
- o Character Frobber
- o Case Modification
- o Numbers
- o Username Generator

## PAYLOAD PROCESSING

Add prefix

Add suffix

Match / Replace

Substring

•Reverse substring

•Modify case

Encode

Decode

Hash

Add raw payload

Skip if matches regex

## BURP SUITE ENCODER & DECODER

URL Encoder & Decoder

HTML Encoder & Decoder

•Base64 Encoder & Decoder

ASCII Hex Encoder & Decoder

Hex Encoder & Decoder

Octal Encoder & Decoder

Binary Encoder & Decoder

Gzip Encoder & Decoder

## TOP 10 VULNERABILITY PLUGINS

Active Scan++  
XSS Validator  
Upload Scanner  
HTTP Request Smuggler  
Turbo Intruder  
CSRF Scanner  
CMS Scanner  
CO2  
Authorize  
Bypass WAF

## PAYLOAD PROCESSING

- Add prefix
- Add suffix
- Match / Replace
- Substring
- Reverse substring
- Modify case
- Encode
- Decode
- Hash
- Add raw payload
- Skip if matches regex

## ENGAGEMENT TOOLS

- Find References
- Discover Content
- Schedule Task
- Generate CSRF POC

**EXCLUSIVE TRAINING  
PROGRAM FOR BUG  
HUNTERS**

