# BUG BOUNTY

## TRAINING PROGRAM

CONTACT US NOW

☎ +91-9599387841

- DURATION -40 HOURS TRAINING
- ONLINE-LIVE SESSIONS
- WEEKEND BATCH

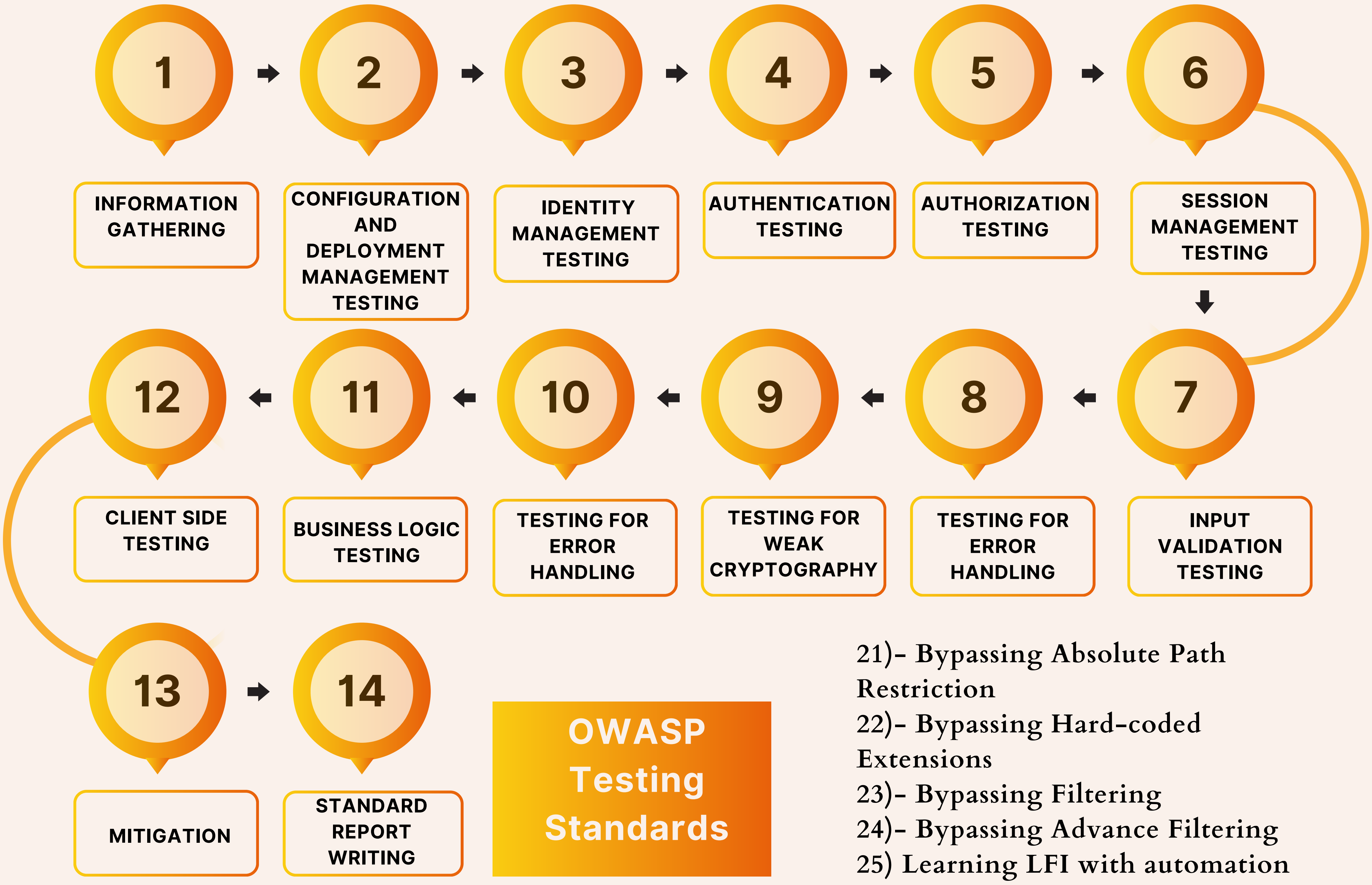
APPLY NOW

iGNITE Technologies

www.ignitetechnologies.in

www.hackingarticles.in

# Course Outline: 40 Hours



1)- Introduction to Web Pentesting and types of pentesting
2)- Web Server Configuration
3)- Web Application Lab Setup
4) Burpsuite Pro with Licence
5)- Burpsuite Installation and proxy setup
6)- HTTP Headers and their importance
7)- HTTP methods Exploitation
8)- Broken Authentication
9)- Broken Access Control
10) Information Disclosure
11) Information Leakage in Debug Pages
12)- Understanding of different encoding methods and hashing formats
13)- Source code Disclosure via Backup Files
14)- Session Hijacking
15)- Understanding of Error Messages
16) Cookie Manipulation
17)-Accessing Private User Data
18)- Understanding of Request Parameter
19)-Privilege Escalation
20)- Directory Traversal
21)- Bypassing Absolute Path Restriction
22)- Bypassing Hard-coded Extensions
23)- Bypassing Filtering
24)- Bypassing Advance Filtering
25) Learning LFI with automation
26) LFI to Remote code Execution
27) LFI to Apache log poisoning
28) SSH log poisoning
29) RFI and its exploitation
30)- OS Command Injection
31)- Blind OS command Injection with time delays
32)- Understanding OS with out-of-band exfiltration
33)- Different types of File Upload
34)- HTML Injections and their types
35)- Creating different types of web payloads
36) Open Redirect Attack
37) Understanding of Regex
38) SQL Injection and its types
39) Cross Site Scripting
40) Reflected XSS
41) DOM XSS
42) Stored XSS
43) CSP Bypass
44)-CSRF
45)- Violation of secure designed principles
46)- SSRF

iGNITE
Technologies