



ADVANCED

Bug Bounty

ABOUT

This course will help the candidate to understand the basic function of the web application and HTTP protocol and their security Assessment.

VISION

This course will provide a complete understanding of OWASP's top 10 and the candidate will be able to complete security assessments for any web application by finding loopholes in them and creating the technical report for their client delivery as per Industry standards.

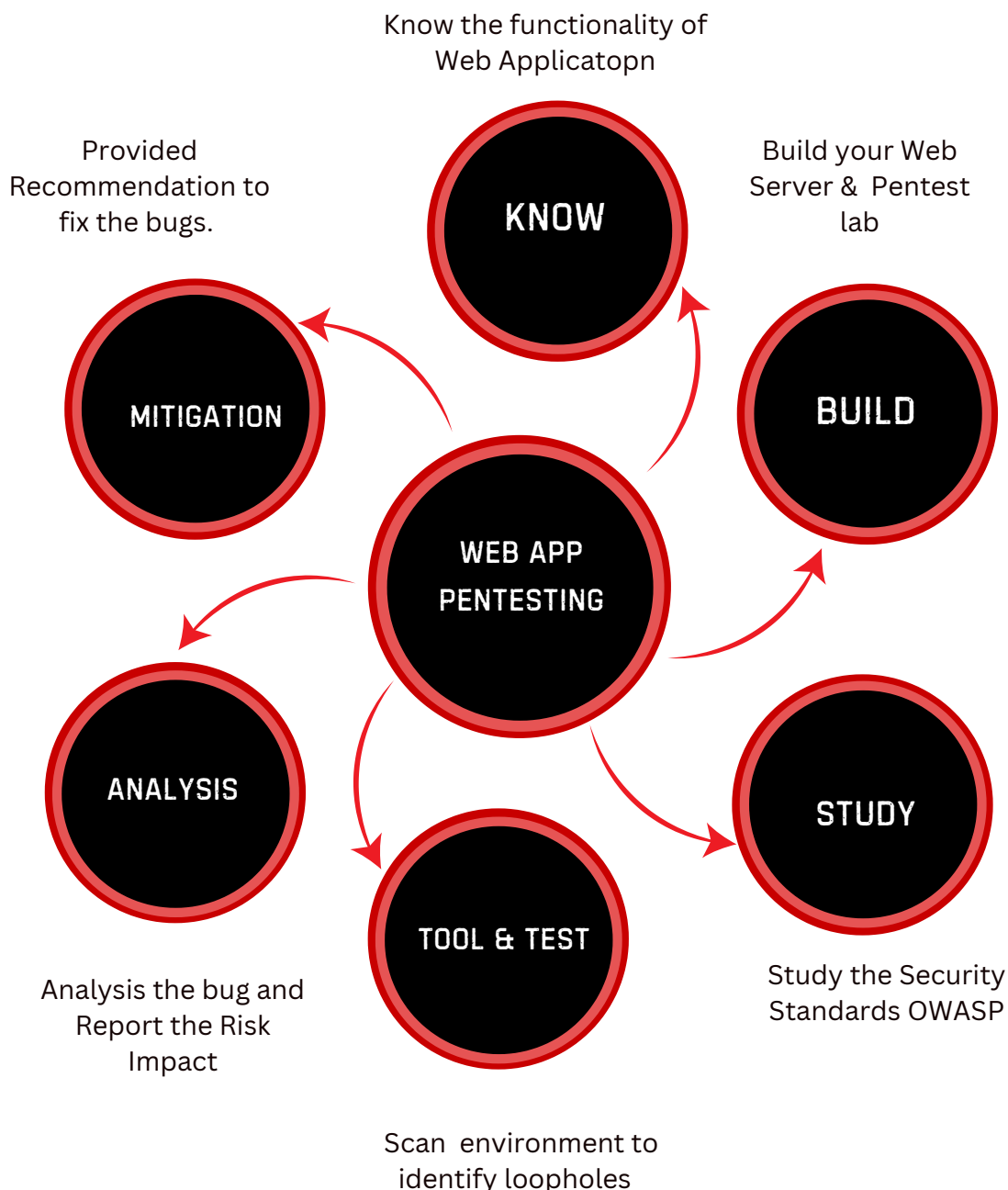
HOW WE FUNCTION

Ignite Trainers

Ignite Trainers are **industry-experienced professionals** and have vast experience with real-time threats thus they provide proactive training by delivering **hands-on practical sessions**.

Had working exposure in Big Fours and MNCs and Fortune 500 companies and clients such as Tata, Facebook, Google, Microsoft, Adobe, Nokia, Paypal, Blackberry, AT&T and many more.

Certified Trainers: CEH, OSCP, OSAP, Iso- Lead Auditor, ECSA, CHFI, CISM



COURSE OUTLINE

1. INFORMATION GATHERING
2. CONFIGURATION AND DEPLOYMENT MANAGEMENT TESTING
3. IDENTITY MANAGEMENT TESTING
4. AUTHENTICATION TESTING
5. AUTHORIZATION TESTING
6. SESSION MANAGEMENT TESTING
7. INPUT VALIDATION TESTING
8. TESTING FOR ERROR HANDLING
9. TESTING FOR WEAK CRYPTOGRAPHY
10. BUSINESS LOGIC TESTING
11. CLIENT SIDE TESTING
12. MITIGATION
13. STANDARD REPORT WRITING

TABLE OF CONTENT

- 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



CONTACT US



PHONE

☎ +91-9599387841 | +91 11 4510 3130

WHATSAPP

💬 <https://wa.me/message/HIOPPNENLOX6F1>

EMAIL ADDRESS

✉ info@ignitetechnologies.in

WEBSITE

🌐 www.ignitetechnologies.in

BLOG

📝 www.hackingarticles.in

LINKEDIN

🌐 <https://www.linkedin.com/company/hackingarticles/>

TWITTER

🐦 <https://twitter.com/hackinarticles>

GITHUB

🐙 <https://github.com/Ignitetechnologies>

