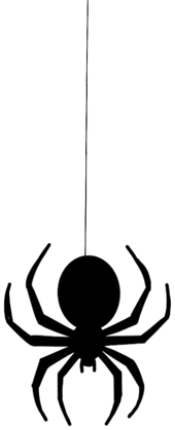
WEB APPLICATION

Penetration Testing Training

WWW.IGNITETECHNOLOGIES.IN

iGNITE Technologies



WEB PENTEST

Web Pentest program, also known as the Bug Bounty program, is a crowdsourcing initiative hosted by organizations to give a platform to security researchers and white hat hackers from across the globe to showcase their skills and discover any security holes in their infrastructure. Depending upon the severity level of the bug report and the details presented within the Proof of Concept (POC), they are either rewarded with remuneration or recognition as a token of appreciation.

While a large majority of the bug bounty programs are public, certain are private events and are strictly invite-based. Such programs have stringent terms and conditions that the invitees must always abide by

During this course, you will acquire knowledge in the fundamentals of application security vulnerabilities and penetration testing.

PREREQUISITES

In order to initiate the Bug Bounty Training, you should be aware of the basic concepts of the development web applications; frontend and backend.

COURSE DURATION: 25 to 30 HOURS

HOW WE FUNCTION

TRAINING TYPE

Type 1

A **GROUP SESSION** will have a maximum of 10 candidates.
Pros: 1) Less Expensive than Type2 & Type3.
2) Get a chance to build connections across the world.

Type 2

A **PERSONALISED SESSIONS** will one-on-one session
Pros: Flexible slot as per candidate availabilities.

Type 3

A **CUSTOMISED PERSONALISED** session will be a one-on-one session that can be finetuned as per the Candidate's requirement.
Pros: 1) Flexible slot as per candidate availabilities
2) Including **Live Website** Testing

iGNITE Technologies

COURSE OVERVIEW

1. Introduction to Web Pentesting and Types of Pentesting

- Black-box, White-box, Grey-box testing
- VAPT vs Bug Bounty vs Red Teaming
- Legal scope & responsible disclosure
- Recon methodology (passive vs active)
- OWASP Top 10 overview

2. Web Server Configuration

- Installation of Apache
- Installation of MySQL
- Installation of phpMyAdmin
- Installation of FTP server
- Installation of SSH service
- Installation of Git

3. Web Application Lab Setup

- Setting up DVWA
- Setting up bWAPP
- Practicing on PortSwigger Web Security Academy labs
- Browser setup (extensions for testing)
- Proxy configuration & intercepting traffic

4. Burp Suite (Installation + Usage)

- Burp installation & setup
- Proxy usage & traffic interception
- Repeater for manual testing
- Intruder for fuzzing
- Scanner basics
- Payload types & fuzzing techniques
- Session handling basics

5.HTTP Headers & Importance

- Security headers analysis
- CORS misconfiguration
- Cache control issues
- Header injection
- Host header attacks

6.HTTP Methods Exploitation

- PUT/DELETE method abuse
- Method override attacks
- TRACE method risks
- Verb tampering
- REST API method testing

7. Broken Authentication

- Credential stuffing & brute force
- Weak password policies
- MFA bypass techniques
- Session fixation

8. Broken Access Control

- IDOR (Insecure Direct Object Reference)
- Vertical vs Horizontal escalation
- Forced browsing
- API authorization flaws
- Role manipulation

9. Information Disclosure & Debug Leakage

- Verbose error messages
- Stack traces & debug endpoints
- Git/config file leaks
- API key exposure
- Metadata leakage

10. Encoding & Hashing

- Base64, URL encoding
- Hash identification (MD5, SHA1, bcrypt)
- Hash cracking basics
- Encoding bypass techniques
-

11. Source Code Disclosure

- Backup files (.zip, .bak, .old)
- .git exposure
- SVN leaks
- Misconfigured cloud storage

12.Session Hijacking

- Cookie stealing (XSS)
- Session fixation
- Predictable session IDs
- Token reuse

13. Error Messages & Cookie Manipulation

- Sensitive info in errors
- Cookie flags (HttpOnly, Secure)
- Tampering cookies
- JWT decoding & modification

14.Accessing Data & Privilege Escalation

- Parameter tampering
- Mass assignment
- Business logic flaws
- Chained exploitation

15. Directory Traversal & Bypass Techniques

- Path traversal basics
- Encoding bypass (%2e%2e/)
- Null byte injection
- Filter bypass techniques
- WAF bypass basics

16. LFI/RFI & Exploitation

- LFI basics & fuzzing
- Wrappers (php://filter)
- Log poisoning
- File inclusion to RCE
- Remote File Inclusion exploitation

17. OS Command Injection

- Basic command injection
- Blind injection (time-based)
- Out-of-band (OAST techniques)
- Command chaining operators
- Filter bypass

18. File Upload Vulnerabilities

- Multiple type bypass
- Double extension attacks
- Web shell upload
- Image-based payloads
- Upload to RCE

19. HTML Injection & Payloads

- HTML injection basics
- Payload crafting
- Leading to phishing attacks
- Obfuscation techniques

20. Open Redirect

- URL validation bypass
- Chaining with phishing
- Bypassing the restrictions

21. Regex Understanding

- Regex basics
- Input validation bypass

22. SQL Injection

- Union-based SQLi
- Boolean-based blind
- Time-based blind
- Error-based SQLi

23. XSS & CSP

- Reflected, Stored, DOM XSS
- Filter bypass techniques
- CSP misconfiguration
- CSP bypass techniques

24.CSRF

- CSRF token bypass
- SameSite cookie issues
- CSRF via JSON/API
- Clickjacking relation

25.Secure Design Principles

- OWASP secure design
- Least privilege
- Defense in depth

26. SSRF

- SSRF basics
- Internal service access
- Cloud metadata exploitation
- Blind 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

iGNITE Technologies

FOLLOW US ON *social media*

TWITTER

DISCORD

GITHUB

LINKEDIN

CONTACT US

FOR MORE DETAILS

+91 95993-87841

www.ignitetechnologies.in