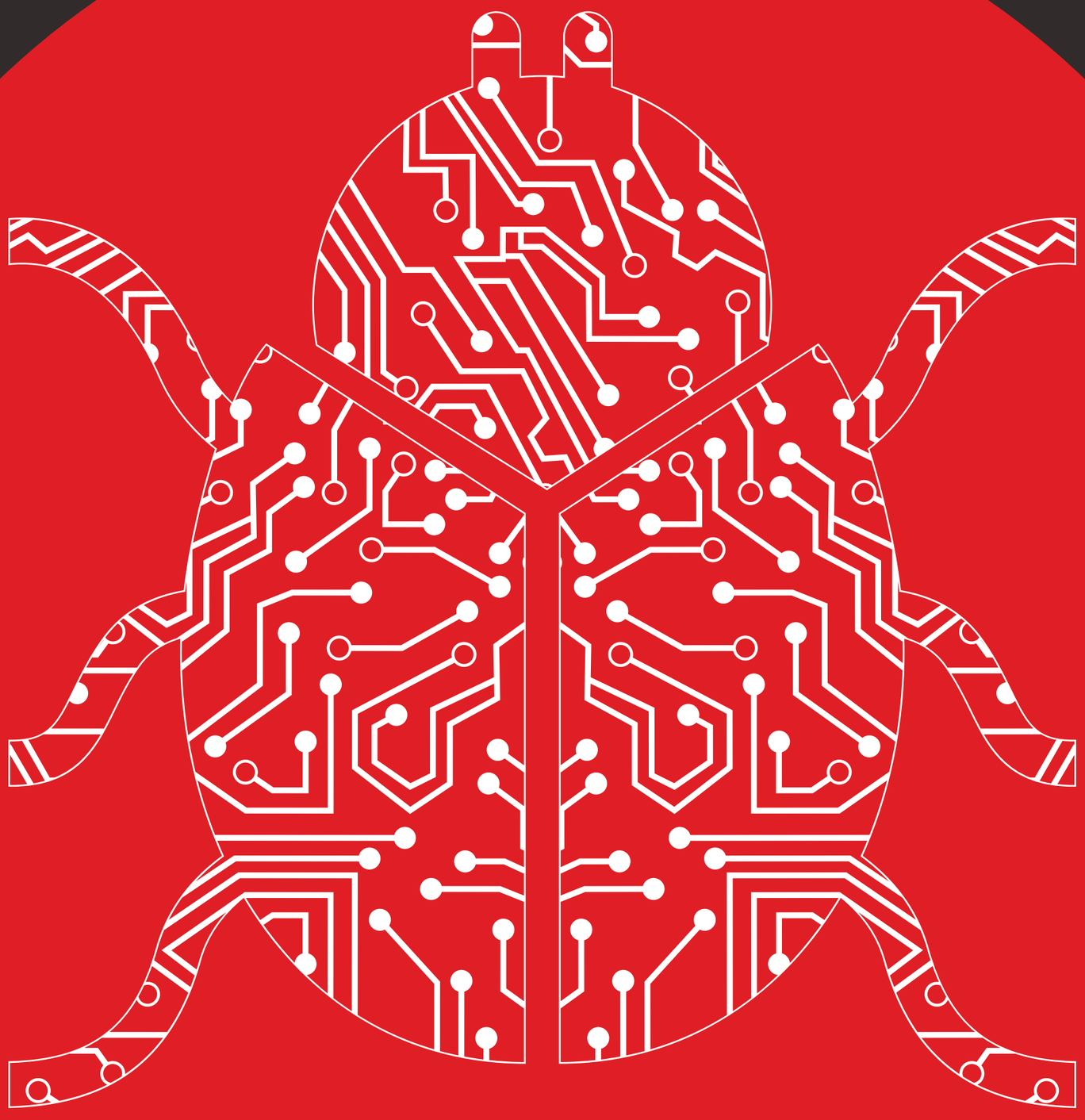
iGNITE Technologies

BURP SUITE



for

PENTESTER

www.ignitetechnologies.in

ABOUT

Well-Known Entity for Offensive Security

{Training and Services}

ABOUT US

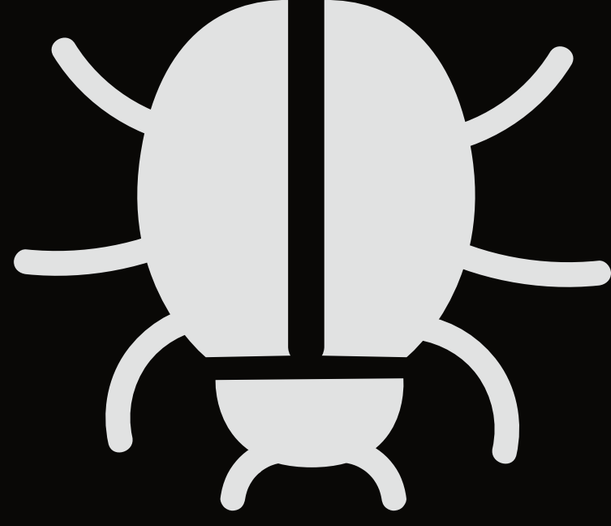
With an outreach to over a million students and over thousand colleges, Ignite Technologies stood out to be a trusted brand in cyber security training and services.

WHO CAN ?

- College Students
- IS/IT specialist, analyst, or manager
- IS/IT auditor or consultant
- IT operations manager
- Network security officers and
- Practitioners
- Site administrators
- Technical support engineer
- Senior systems engineer
- Systems analyst or administrator
- IT security specialist, analyst, manager,
- Architect, or administrator
- IT security officer, auditor, or engineer
- Network specialist, analyst, manager,
- Architect, consultant, or administrator

WHY US ?

- Level up each candidate by providing the fundamental knowledge required to begin the Sessions.
- Hands-on Experience for all Practical Sessions.
- Get Course PDF and famous website links for content and Tools
- Customized and flexible training schedule.
- Get recorded videos after the session for each participant.
- Get post-training assistance and backup sessions.
- Common Platform for Group discussion along with the trainer.
- Work-in Professional Trainer to provide realtime exposure.
- Get a training certificate of participation.



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. *iOS Penetration Testing*
2. *Ethical Hacking*
3. *Bug Bounty*
4. *Network Penetration Testing*
5. *Windows for Pentester*
6. *Linux for Pentester*
7. *Burp Suite For Pentester*
8. *CTF*
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 500 walkthrough (Solutions) of CTFs of the various platform on our reputed website "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*

iGNITE Technologies

CAREER IN IT SECURITY DOMAIN

- Chief Information Security
- Officer Incident Analyst | Responder
- Information Security Analyst
- Senior Security Consultant
- Software Code Analyst
- Digital Forensic Expert
- Cryptographer
- Risk Controller
- International Trainer
- Penetration Tester
- Security Architect
- Security Engineer
- Researcher
- Exploit Developer
- Ethical Hacker

iGNITE Technologies

COURSE OVERVIEW

Introduction To Burp Suite

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

- Manual Configuration
- Using Browser's Extension Configuring Burp Proxy for Android Applications

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 Collaborator

Introduction to Burp Collaborator Detecting vulnerabilities with Collaborator Client

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

iGNITE Technologies

The Burp's Hack Bar

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

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

Burp Suite As A Vulnerability Scanner

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

iGNITE Technologies

Advanced Fuzzing

Introduction to Fuzzing Burp Suite as a Fuzzer Fuzzing with built-in payloads

- Fuzzing for Login credentials.
- Fuzzing for SQL Injection
- Fuzzing to find Hidden Files
- Fuzz to find Restricted File Upload Extensions
- Fuzzing for Cross-Site Scripting
- Fuzzing for OS Command Injection
- Fuzzing for Hidden Directories
- Fuzzing for HTTP Verb Tampering
- Manipulate Burp Suite's predefined payloads
- Injecting our customized payload lists

Fuzzing with the Attack Type

- Cluster Bomb
- Battering ram
- Pitchfork

Fuzzing with the Payload Types

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

iGNITE Technologies

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
- Turbo Intruder
- CSRF Scanner
- CMS Scanner
- CO2
- Bypass WAF

Engagement Tools

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

CONTACT US

Phone No.

+91 9599 387 41 | +91 1145 1031 30

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