RECON
CYBER SECURITY

DEFEND | DETECT | SECURE

OUR PARTNERS

cisco python EY Red Hat CompTIA Microsoft

OVERVIEW

In this course, students will learn the about Web Application based API Penetration Testing techniques. Topics include Lab Setup, Postman, XXE exploitation, File path traversal and more.

PRE-REQUISITES

Students should have prior knowledge with Penetration Testing, Bug Bounty Hunting and Hands On Experience with Burp Suite.

WHO WE ARE

We promise to offer the best training and certification programs to our students. We provide the programs and resources you need to succeed if you are just beginning your Cyber security career or are an experienced expert wishing to develop your skills. Contact us today to learn more about our training and certification options!

WHY CHOOSE US

Welcome to our Cyber Security Training Institute, where we are committed to giving individuals and organisations who want to protect their digital assets thorough training and certification programmes. Our knowledgeable Trainers will bring you through the complexities of cyber security with their cutting-edge expertise and practical experience. You will learn useful methods and abilities to protect yourself from online dangers, such as ethical hacking, network security, incident response, and other things. Our programmes give you the opportunity to hone your skills and grow your profession through practical lab experiences and individualised coaching.

API TESTING COURSE CONTENT

COURSE DURATION: 40 hrs

- Module 12: Mass Assignment attack
  - What is mass assignment in APIs
  - Exploiting mass assignment vulnerabilities
  - Preventing mass assignment attacks
- Module 01: introduction to API
  - Definition of APIs
  - Types of APIs: REST, SOAP, GraphQL
  - How APIs work
  - Understanding API endpoints and requests
- Module 02: Postman Lab setup
  - Installing and configuring Postman
  - Introduction to API testing with Postman
  - Creating your first API request
  - Managing API environments in Postman
- Module 03: Preparation for API Pen-Testing
  - Tools required for API penetration testing
  - Understanding API documentation
  - Identifying potential API vulnerabilities
  - Setting up a testing environment
- Module 04: Lab Setup
  - Setting up a local API testing environment
  - Introduction to API simulation tools
  - Creating mock APIs for testing purposes
- Module 05: OWASP API TOP 10
  - Overview of the OWASP API Security Top 10 risks
  - Deep dive into each of the OWASP Top 10
  - How to identify and mitigate these risks
- Module 06: SQL injection
  - Understanding SQL Injection in APIs
  - Testing for SQL Injection vulnerabilities
  - Preventing SQL Injection attacks in API endpoints
- Module 07: Command Injection
  - Basics of command injection
  - Identifying and exploiting command injection vulnerabilities
  - Best practices to prevent command injection
- Module 08: Offensive XXE Exploitation
  - Introduction to XML External Entities (XXE) vulnerabilities
  - Exploiting XXE in APIs
  - Mitigation techniques to prevent XXE attacks
- Module 09: Server Side Request Forgery
  - Understanding SSRF and its impact
  - Detecting SSRF vulnerabilities in APIs
  - Exploiting SSRF in real-world scenarios
- Module 10: Cross site scripting
  - Types of XSS attacks in APIs
  - Testing API responses for XSS vulnerabilities
  - Mitigating XSS vulnerabilities in API responses
- Module 11: Transport layer security issues
  - Importance of Transport Layer Security (TLS)
  - Identifying insecure transport layer configurations
  - How to secure transport layers in API communication

- **Weekend / weekdays classes**
- **Online and offline classes**
- **1 year membership**
- **Certificate after completion**
- **Interview preparation**
- **Live hacking training**
- **Class session recordings**
- **Ebooks tutorials**
- **24x7 support**

- Module 13: Broken Object Level Authorization Issues
  - Understanding object-level authorization
  - Identifying broken object-level authorization vulnerabilities
  - Securing APIs against BOLA vulnerabilities
- Module 14: File Path Traversal
  - What is file path traversal in APIs
  - Exploiting file path traversal vulnerabilities
  - Best practices to secure against file path traversal
- Module 15: User Enumeration
  - Identifying user enumeration in APIs
  - Techniques for preventing user enumeration attacks
  - Case studies of real-world user enumeration attacks
- Module 16: Information Disclosure
  - How APIs unintentionally disclose sensitive information
  - Testing for information disclosure vulnerabilities
  - Securing APIs to prevent information leakage
- Module 17: JSON web token
  - Introduction to JWT and its use in API authentication
  - Exploiting vulnerabilities in JWT implementations
  - Best practices for securing JWT in AP
- Module 18: Unauthorized password change
  - Understanding unauthorized password change vulnerabilities
  - Testing for improper password change implementations
  - Securing APIs to prevent unauthorized password changes
- Module 19: Excessive data exposure
  - How APIs expose excessive data
  - Detecting excessive data exposure vulnerabilities
  - Limiting data exposure through best practices
- Module 20: Lack of Resource & Rate Limiting
  - Importance of rate limiting in APIs
  - Identifying APIs with no resource or rate limiting
  - Implementing rate limiting to prevent abuse
- Module 21: Regular Expression DOS attack
  - Understanding ReDoS (Regular Expression Denial of Service)
  - Detecting ReDoS vulnerabilities in APIs
  - Securing APIs against ReDoS attacks
- Module 22: BFLA Issues
  - What is Broken Function Level Authorization (BFLA)
  - Identifying and exploiting BFLA vulnerabilities
  - Mitigating BFLA issues in API functions
- Module 23: Billion laugh attack
  - Introduction to XML DoS attacks, specifically Billion Laughs
  - Exploiting Billion Laughs vulnerabilities in APIs
  - Best practices to prevent Billion Laughs attacks
- Module 24: Hidden API Functionality Exposure
  - Understanding hidden API functionality
  - Identifying and exploiting hidden or undocumented API features
  - Securing APIs by removing or hiding unnecessary functionality
- Module 25: RCE Via Deserilization in API
  - Introduction to remote code execution (RCE) via deserialization
  - Exploiting deserialization vulnerabilities in APIs
  - Mitigation techniques to prevent RCE through deserialization

Every Class Recordings

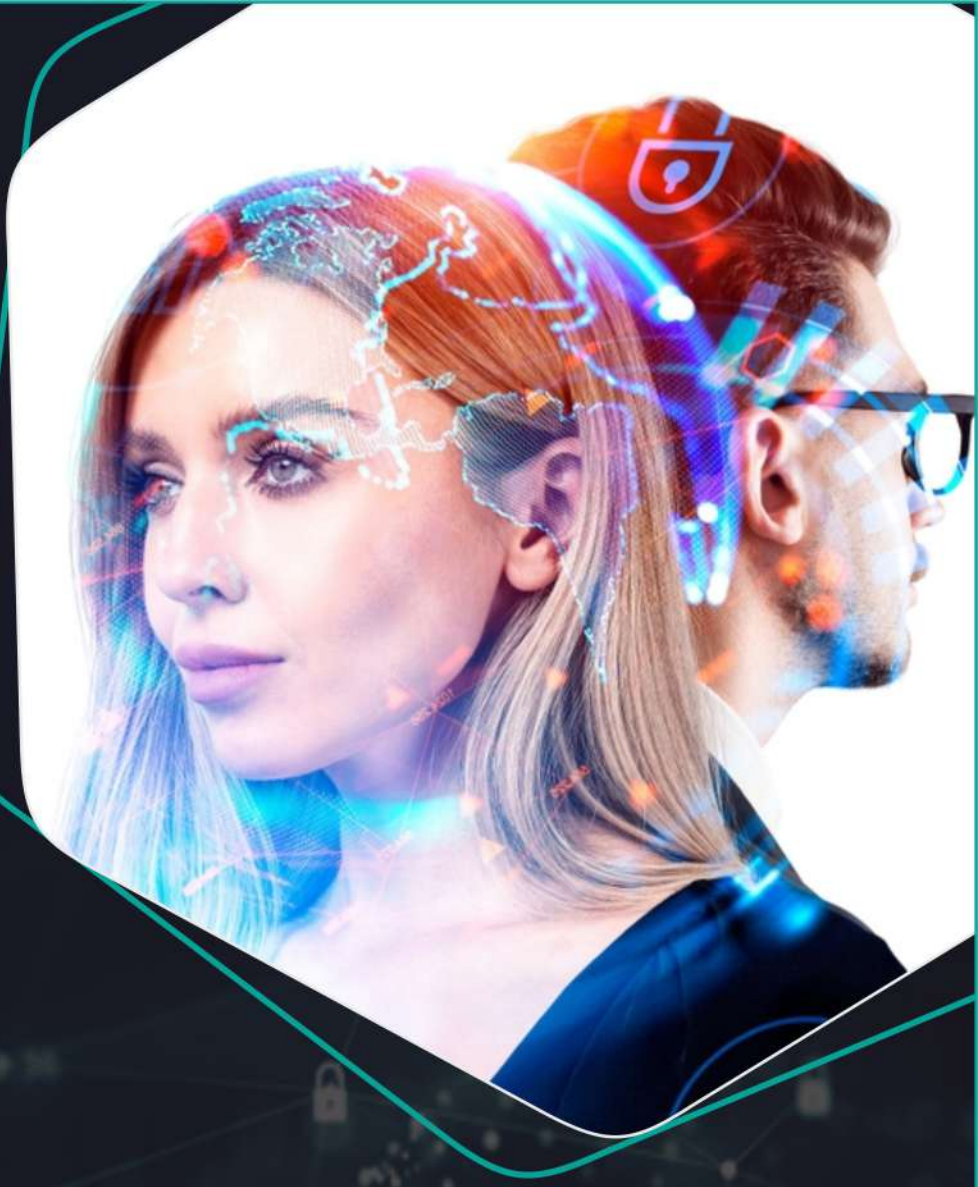
Easy Repetations

Shareable Content

Hybrid Classes

Checkpoint Based Training

24x7 Support



RECON CYBER SECURITY PVT. LTD

(HEAD OFFICE | LAXMI NAGAR, NEW DELHI)

2nd Floor, Gali no 1, Shakarpur, Laxmi Nagar New Delhi 110092

WhatsApp or Call : +91-8595756252, +91-8800874869

Training@reconforce.in, Info@reconforce.in

RECON CYBER SECURITY PVT. LTD

(BRANCH OFFICE | SANT NAGAR BURARI, NEW DELHI)

Ground Floor, Gali no 8, Main Market, Sant Nagar, Burari, New Delhi 110092

WhatsApp or Call : +91-8595756252, +91-8800874869

Training@reconforce.in, Info@reconforce.in

#RECON CYBER SECURITY