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 already be familiar with how to operate the Linux Operating system and Bug Hunting.

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 01: introduction to API
- Module 02: Postman Lab setup
- Module 03: Preparation for API Pen-Testing
- Module 04: Lab Setup
- Module 05: OWASP API TOP 10
- Module 06: SQL injection
- Module 07: Command Injection
- Module 08: Offensive XXE Exploitation
- Module 09: Server Side Request Forgery
- Module 10: Cross site scripting
- Module 11: Transport layer security issues
- Module 12: Mass Assignment attack
- Module 13: Broken Object Level Authorization Issues
- Module 14: File Path Traversal
- Module 15: User Enumeration
- Module 16: Information Disclosure
- Module 17: JSON web token
- Module 18: Unauthorized password change
- Module 19: Excessive data exposure
- Module 20: Lack of Resource & Rate Limiting
- Module 21: Regular Expression DOS attack
- Module 22: BFLA Issues
- Module 23: Billion laugh attack
- Module 24: Hidden API Functionality Exposure
- Module 25: RCE Via Deserilization in API

“

- **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**

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