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 Penetration Testing techniques. Topics include Reconnaissance, Scanning, Exploitation, Post Exploitation and more.

PRE-REQUISITES

Students should have prior knowledge with Operation System such as : Windows 7, 8, 10, or 11 etc.

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.

WEB APP PEN-TESTING COURSE CONTENT

COURSE DURATION: 40 hrs

- Lesson 1 : Introduction to Web-application Penetration-Testing
  - ⊙ Understanding the Purpose of Penetration Testing:

  Learn why penetration testing is crucial for web applications.
  - ⊙ Types of Web Vulnerabilities:

  Explore common security flaws targeted in web apps.
  - ⊙ Tools for Web Penetration Testing:

  An overview of popular tools like Burp Suite, OWASP ZAP, and more.

- Lesson 2 : Finding Subdomains
  - ⊙ Introduction to Subdomain Enumeration:

  Why subdomains are vital for security analysis.
  - ⊙ Tools for Subdomain Discovery:

  Techniques and tools such as Sublist3r, Amass, and DNS recon.
  - ⊙ Practical Guide to Subdomain Enumeration:

  Step-by-step approach to discovering and analyzing subdomains.

- Lesson 3 : Understanding HTTP
  - ⊙ Overview of HTTP Protocol:

  Structure and workings of HTTP requests and responses.
  - ⊙ Common HTTP Methods and Their Impact on Security:

  GET, POST, PUT, DELETE, and other HTTP methods.
  - ⊙ Security Implications of HTTP Headers:

  How headers like CORS, HSTS, and Content-Security-Policy affect web security.

- Lesson 4 : Access Control Flaws
  - ⊙ Understanding Access Control:

  What is access control, and why is it critical?
  - ⊙ Types of Access Control Issues:

  Insecure Direct Object References (IDOR), broken access control.
  - ⊙ Exploiting and Mitigating Access Control Flaws:

  Real-world examples and remediation techniques.

- Lesson 5 : Ajax Security
  - ⊙ What is Ajax?: Introduction to Ajax and its role in web apps.
  - ⊙ Security Risks with Ajax Requests: Common vulnerabilities like CSRF and improper data handling.
  - ⊙ Securing Ajax Implementations: Techniques to ensure safe Ajax usage in web apps.

- Lesson 6 : Authentication Flaws
  - ⊙ Introduction to Authentication Mechanisms: Passwords, tokens, and multifactor authentication.
  - ⊙ Common Authentication Vulnerabilities: Brute force attacks, session fixation, weak password policies.
  - ⊙ Securing Authentication: Best practices for strong authentication mechanisms.

- Lesson 7 : Buffer overflaws
  - ⊙ What is a Buffer Overflow?: An overview of how buffer overflows occur.
  - ⊙ Exploiting Buffer Overflow Vulnerabilities: Techniques and real-world examples.
  - ⊙ Preventing Buffer Overflows: Defensive programming techniques to mitigate these flaws.

- Lesson 8 : Code Quality
  - ⊙ The Importance of Secure Coding Practices: Understanding how code quality impacts security.
  - ⊙ Common Coding Mistakes Leading to Vulnerabilities: Examples of poor coding practices.
  - ⊙ Improving Code Quality for Security: Best practices in secure software development.

- Lesson 9 : Concurrency Flaws
  - ⊙ What are Concurrency Issues?: Explanation of race conditions and deadlocks.
  - ⊙ How Concurrency Flaws Impact Security: Real-world implications of concurrency vulnerabilities.
  - ⊙ Mitigating Concurrency Vulnerabilities: Techniques to handle concurrency safely.
- Lesson 10 : Cross Site Scripting
  - ⊙ Types of XSS Attacks: Reflected, stored, and DOM-based XSS.
  - ⊙ Exploiting XSS Vulnerabilities: How attackers use XSS to compromise web apps.
  - ⊙ Preventing XSS Attacks: Implementing proper input validation and sanitization.

- Lesson 11 : Improper Error Handling
  - Understanding Error Handling in Web Applications: Why proper error handling is important.
  - Common Flaws in Error Handling: How revealing error messages can lead to information leakage.
  - Best Practices for Error Handling: Techniques to secure error management.

- Lesson 12 : Injection Flaws
  - Overview of Injection Attacks: SQL injection, command injection, and LDAP injection.
  - Exploiting Injection Vulnerabilities: Real-world examples and techniques.
  - Mitigating Injection Flaws: Secure coding practices and input validation techniques.

- Lesson 13 : Denail of Service
  - What is a Denial of Service Attack?: How DoS attacks disrupt web services.
  - Common DoS Techniques: Flood attacks, slow attacks, and resource exhaustion.
  - Preventing DoS Attacks: Strategies to detect and mitigate DoS attacks.

- Lesson 14 : Insecure Communication
  - Understanding Secure Communication Protocols: TLS, HTTPS, and their importance.
  - Vulnerabilities in Web Communication: Man-in-the-middle attacks, SSL stripping.
  - Securing Communication Channels: Best practices for secure communication in web apps.

- Lesson 15 : Insecure Configuration
  - What is Insecure Configuration?:
    How misconfigurations lead to vulnerabilities.
  - Common Misconfiguration Issues:
    Exposed admin panels, weak file permissions.
  - Securing Web Application Configurations:
    Steps to harden configurations for better security.

- Lesson 16 : Insecure Storage
  - Risks of Insecure Data Storage:
    Sensitive data exposure due to poor storage practices.
  - Common Storage Vulnerabilities:
    Unencrypted databases, weak cryptography.
  - Best Practices for Secure Data Storage:
    Encryption techniques and secure storage mechanisms.

- Lesson 17 : Malicious File Execution
  - Understanding File Upload Vulnerabilities:
    How attackers exploit file uploads.
  - Exploiting Malicious File Execution Flaws:
    Real-world examples of file execution attacks.
  - Mitigating File Upload Risks:
    Techniques to secure file upload mechanisms.

- Lesson 18 : Parameter Tampering
  - What is Parameter Tampering?:
    Understanding how attackers manipulate input parameters.
  - Exploiting Parameter Tampering Vulnerabilities:
    Real-world examples.
  - Preventing Parameter Tampering:
    Implementing secure input validation and handling.

- Lesson 19 : Challenge Online Platform
  - Overview of Web Penetration Testing Challenges:
    Introduction to online testing platforms.
  - Using Platforms like Hack The Box and TryHackMe:
    Practical penetration testing in a simulated environment.
  - Improving Skills with Online Challenges:
    Benefits of participating in web security challenges.

- **10 gb toolkit**
- **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