# RECON

## CYBER SECURITY

DEFEND | DETECT | SECURE

OUR PARTNERS

cisco python EY Red Hat CompTIA Microsoft

## OVERVIEW

In this course, students will learn the about Bug Bounty Hunting techniques. Topics include BurpSuite, SQL injection, XML injection, Report Preparation and more.

## PRE-REQUISITES

Students should have Professional Knowledge about Web-Application Penetration Testing.

## 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.

# BUG HUNTING COURSE CONTENT

COURSE DURATION: 70 hrs

- Module 01: Introduction
  - Overview of Web Application Security
  - Importance of Ethical Hacking
  - Understanding OWASP Top 10
- Module 02: Information Gathering
  - Passive vs Active Reconnaissance
  - Tools for Information Gathering
  - Techniques for Gathering Target Data
- Module 03: BurpSuite Introduction
  - Setting up BurpSuite
  - Overview of BurpSuite Tools
  - Using Proxy, Spider, and Scanner
- Module 04: Cross Site Scripting (XSS)
  - Types of XSS: Reflected, Stored, DOM-based
  - Preventing XSS Attacks
  - Exploiting XSS with Examples
- Module 05: Host Header Injection
  - What is Host Header Injection?
  - Exploiting Host Header Injection Vulnerabilities
  - Mitigating Host Header Injection
- Module 06: URL Redirection
  - Open URL Redirection Attacks
  - Common Exploits of URL Redirection
  - Security Measures Against URL Redirection
- Module 07: Parameter Tempering
  - Exploiting Parameter Manipulation
  - Common Scenarios of Parameter Tampering
  - Defense Against Parameter Tampering
- Module 08: HTML Injection
  - Differentiating HTML Injection from XSS
  - Potential Consequences of HTML Injection
  - Mitigation Strategies
- Module 09: SQL Injection
  - Basics of SQL Injection
  - Types of SQL Injections: Error-based, Blind, and Union-based
  - Securing Applications Against SQL Injection
- Module 10: File Inclution
  - Local File Inclusion (LFI) vs Remote File Inclusion (RFI)
  - Exploiting File Inclusion Vulnerabilities
  - Preventive Measures for File Inclusion Attacks
- Module 11: Missing SRF Record
  - Understanding Sender Policy Framework (SPF)
  - Risks of Missing SPF Records
  - How to Set Up SPF Records
- Module 12: No rate Limiting
  - The Impact of Absence of Rate Limiting
  - Automated Attacks Due to No Rate Limiting
  - Implementing Effective Rate Limiting
- Module 13: Source Code Discloser
  - Causes and Effects of Source Code Disclosure
  - Techniques for Exploiting Source Code
  - Secure Coding Practices
- Module 14: Long Password Attack
  - Understanding Denial of Service via Long Password Inputs
  - Impact on Application Performance
  - Methods to Prevent Long Password DOS Attacks
- Module 15: IDOR
  - How IDOR Works
  - Risks Associated with IDOR
  - Preventing IDOR Vulnerabilities
- Module 16: Server Site Request Forgery (SSRF)
  - Common SSRF Exploits
  - Real-world Implications of SSRF
  - Mitigation Techniques
- Module 17: Cross Site Request Forgery (CSRF)
  - CSRF Attack Vectors
  - Identifying CSRF Vulnerabilities
  - Protection Against CSRF Attacks
- Module 18: Hostile Subdomain Takeover
  - Understanding Subdomain Takeovers
  - Steps to Identify and Prevent Takeovers
  - Secure Domain Management
- Module 19: S3 Bucket Takeover
  - How S3 Bucket Takeovers Happen
  - Securing Cloud Storage
  - Preventing Unauthorized Access to S3 Buckets
- Module 20: Command Injection (RCE)
  - Exploiting Command Injection Vulnerabilities
  - Remote Code Execution (RCE) Attacks
  - Defense Mechanisms for Command Injection
- Module 21: File Uploading
  - Risks Associated with File Uploading
  - Common File Upload Vulnerabilities
  - Secure File Upload Handling
- Module 22: XML External Entity Injection
  - XXE Attack Techniques
  - Risks of XML Parsing Vulnerabilities
  - Safeguarding Applications Against XXE
- Module 23: Buffer Overflow
  - How Buffer Overflow Occurs
  - Exploiting Buffer Overflow for Code Execution
  - Defenses Against Buffer Overflow Attacks
- Module 24: Wordpress Vulnerability
  - Common WordPress Vulnerabilities
  - Exploiting WordPress Weaknesses
  - Hardening WordPress Security
- Module 25: Joomla Vulnerability
  - Identifying Joomla Security Flaws
  - Typical Joomla Vulnerabilities
  - Protecting Joomla-Based Applications
- Module 26: Drupal Vulnerability
  - Exploiting Drupal Security Holes
  - Securing Drupal Installations
  - Recognizing and Patching Vulnerabilities
- Module 27: CMS Vulnerability Hunting
  - Tools for CMS Vulnerability Scanning
  - Popular CMS Platforms and Their Weaknesses
  - CMS Hardening Practices
- Module 28: HSTS ( HTTP Strict transport security)
  - Importance of HSTS in Secure Communication
  - Enforcing HSTS in Web Applications
  - Implementation Steps for HSTS

- Module 29: Session Fixation
  - Understanding Session Fixation Attacks
  - Mitigating Session Fixation Risks
  - Secure Session Management
- Module 30: Account Lookout
  - Protecting Accounts from Brute-Force Attacks
  - Implementing Account Lockout Mechanisms
  - Best Practices for Account Security
- Module 31: Password Reset Poisoning
  - What is Password Reset Poisoning?
  - Attack Techniques for Password Reset Poisoning
  - Prevention Strategies for Secure Password Reset
- Module 32: Identity Management test Testing
  - Testing Identity and Access Management (IAM) Systems
  - Common IAM Vulnerabilities
  - Secure Identity Management Best Practices
- Module 33: Authentication Testing
  - Importance of Authentication in Web Security
  - Common Authentication Flaws
  - Techniques for Testing Authentication Mechanisms
- Module 34: Cryptographic Vulnerability
  - Identifying Cryptographic Weaknesses
  - Real-World Impacts of Cryptographic Flaws
  - Secure Cryptographic Practices
- Module 35: Session Management Testing
  - Importance of Secure Session Management
  - Testing Session Expiry and Hijacking Vulnerabilities
  - Best Practices for Session Security
- Module 36: Exposed Source CCS
  - Risks of Publicly Exposed Version Control Systems
  - Detecting Leaked Source Code
  - Securing Code Repositories
- Module 37: Apache Structs RCE Hunting
  - What is Apache Struts RCE?
  - Exploiting Apache Struts Vulnerabilities
  - Hardening Apache Struts Applications
- Module 38: Web Cache Deceptions
  - Understanding Web Cache Deception Attacks
  - Exploiting Caching Mechanisms
  - Preventing Cache-Based Exploits
- Module 39: Server Side Includes Injection
  - How SSI Injection Attacks Work
  - Impact of SSI Injection
  - Mitigating SSI Injection Vulnerabilities
- Module 40: Ticket Tricks Bug Bounty
  - Common Ticketing System Vulnerabilities
  - Exploiting Ticket-Based Bugs in Applications
  - Securing Ticketing Systems from Exploits
- Module 41: Multi-Factor Authentication
  - Importance of Multi-Factor Authentication
  - Testing for MFA Vulnerabilities
  - Best Practices for Implementing MFA
- Module 42: HTTPoxy Attact Module
  - What is an HTTPoxy Attack?
  - Identifying and Exploiting HTTPoxy
  - Protection Against HTTPoxy Attacks
- Module 43: Webmin Unauthentication RCE
  - Exploiting Webmin Authentication Flaws
  - Real-World Scenarios of Webmin Bypass
  - Strengthening Webmin Authentication
- Module 44: HeartBleed
  - Understanding the HeartBleed Vulnerability
  - Exploiting HeartBleed in SSL/TLS Implementations
  - Mitigation Steps for HeartBleed Vulnerabilities
- Module 45: Appweb Authentication bypass
  - Identifying Weaknesses in Appweb Authentication
  - Exploiting Authentication Bypass in Appweb
  - Strengthening Appweb Security
- Module 46: Ngnix
  - Common Security Flaws in Nginx Servers
  - Exploiting Nginx Vulnerabilities
  - Hardening Nginx Configurations
- Module 47: MySQL Authentication Bypass
  - Understanding MySQL Authentication Vulnerabilities
  - Exploiting Authentication Bypass in MySQL
  - Securing MySQL Authentication Mechanisms
- Module 48: DMS Zone Transfer
  - What is DNS Zone Transfer?
  - Exploiting Insecure DNS Zone Transfers
  - Preventing Unauthorized Zone Transfers
- Module 49: LOG Injection
  - Exploiting Log Injection Vulnerabilities
  - Detecting Log Manipulation Attacks
  - Mitigation Techniques for Log Injection
- Module 50 : Cache Testing
  - Testing Web Application Cache Behavior
  - Identifying Cache-Related Security Issues
  - Secure Cache Configuration Practices
- Module 51 : Black (Jinga-2) SSTI to RCE
  - Server-Side Template Injection (SSTI) Basics
  - Exploiting Jinja-2 SSTI to Achieve RCE
  - Preventing SSTI in Web Applications
- Module 52 : Handloop Vulnerability
  - Understanding Handloop Vulnerabilities
  - Exploiting Handloop for DoS and Other Attacks
  - Mitigating Handloop Vulnerabilities
- Module 53 : CSRF Same site bypass
  - How Same-Site Attribute Works in CSRF Protection
  - Exploiting Weaknesses in Same-Site Enforcement
  - Strengthening CSRF Defenses
- Module 54 : JWT Token Attack
  - Common Attacks on JSON Web Tokens (JWT)
  - Exploiting JWT Misconfigurations
  - Securing JWT Implementation in Applications
- Module 55 : Email bounce resource
  - Exploiting Email Bounce Mechanisms
  - Common Vulnerabilities in Email Systems
  - Securing Email Bounce Handlers
- Module 56 : IVR Call Request Crash
  - Understanding Interactive Voice Response (IVR) Systems
  - Exploiting Call Request Handling in IVR Systems
  - Mitigation Strategies for IVR Vulnerabilities
- Module 57 : Weak Password Reset
  - Identifying Weaknesses in Password Reset Processes
  - Exploiting Password Reset Vulnerabilities
  - Best Practices for Secure Password Resets
- Module 58 : Business Login Vulnerabilities
  - Understanding Business Logic Attacks
  - Identifying and Exploiting Flaws in Business Logic
  - Securing Application Logic Against Exploits

- Module 59 : RPC Ping Back Attack
  - How RPC Pingback Vulnerabilities Work
  - Exploiting RPC Systems for Attacks
  - Preventing Pingback Exploits

- Module 60 : WAF/ MOD Security Bypass
  - Techniques for Bypassing Web Application Firewalls (WAF)
  - Understanding ModSecurity and Its Weaknesses
  - Strengthening WAF Configurations

- Module 61 : Broken Authentication
  - Identifying Authentication Flaws
  - Exploiting Insecure Authentication Mechanisms
  - Best Practices for Authentication Security

- Module 62 : Open redirection
  - What is Open Redirection?
  - Exploiting Open Redirection Vulnerabilities
  - Mitigation of Open Redirection Risks

- Module 63 : Null Byte Injection
  - Understanding Null Byte Injection Attacks
  - Exploiting Null Byte Vulnerabilities
  - Defenses Against Null Byte Injection

- Module 64 : CORS Vulnerabilities
  - Cross-Origin Resource Sharing (CORS) Basics
  - Identifying CORS Misconfigurations
  - Securing Web Applications Against CORS Exploits

“

- **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

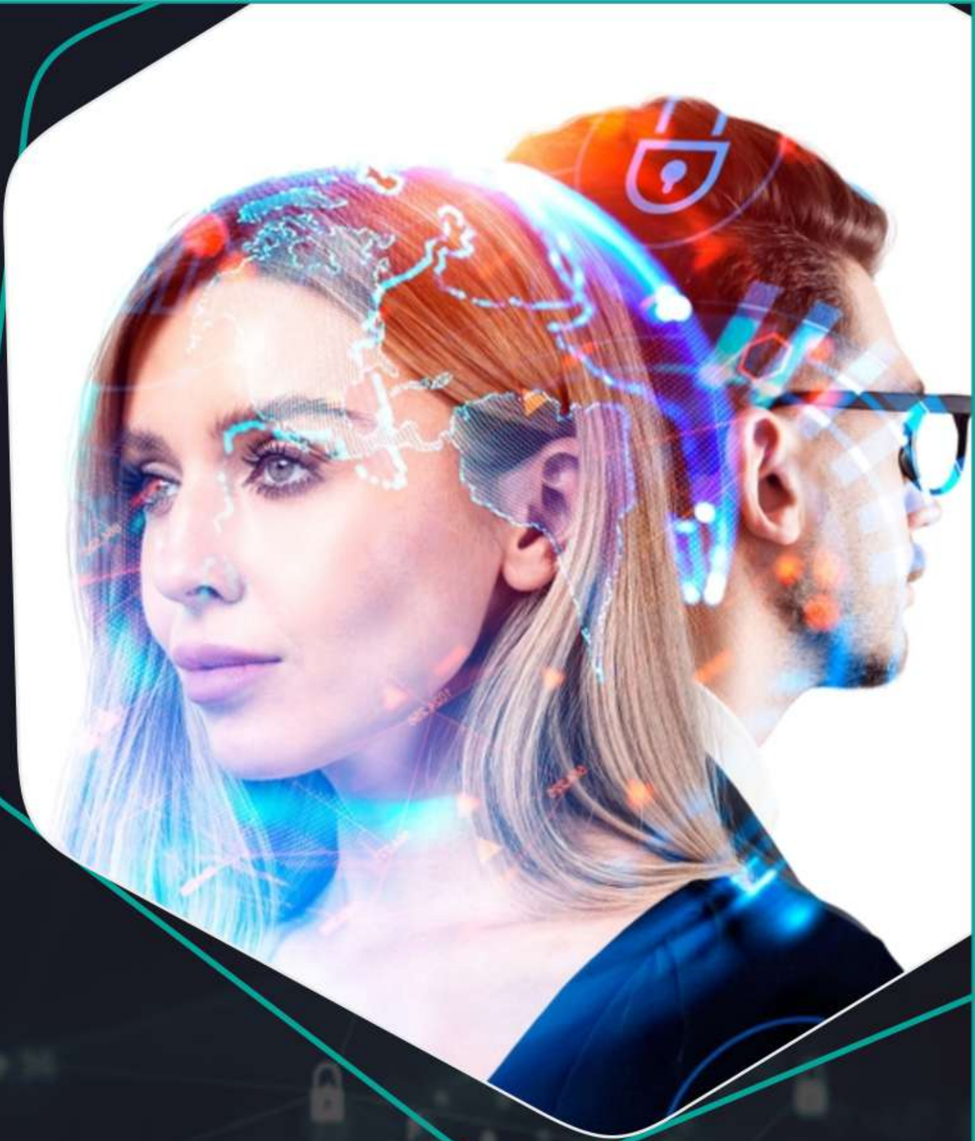
Easy Repetations

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