RECON
CYBER SECURITY

Call Now:
+91-8595756252
+91-8800874869

SEC_RITY IS NOT COMPLETE WITHOUT U!

The security light made me feel safe, though I know that was an illusion. If there is light, you can just see what's coming for you a little more clearly.

Details for BUG Hunting **Duration: 2.5 to 3 Months**

Overview

In this course, students will learn about **Advance Web-Application Exploiting** techniques. Like: Buffer Overflow, CMS hunting, Sever Hijacking, CORS, etc.

Pre-Requisites

Students should already know about web development languages for code reading and modification. (Like: HTML, CSS, JAVA, Java-Script, etc.) **[Note: Students should already know about OWASP TOP 10]**

Who We Are?

Recon Force is a Training and Consulting company and adheres to training standards. We are bringing it to improve its security training and services through technology-enabled IT content. Prepares for an important role as a Penetration Testing expert, instrument analyst, service analyst, network security program manager, and other related roles.

Why Choose Recon Cyber Security?

Recon Force is the best accredited Ethical Hacking training classes in Delhi that offers the best Ethical Hacking training in Delhi on practical exams that help aspirants gain professional skills. The institute offers practical and career-based Ethical Hacking training in Delhi to help students find their dream job at various MNCs. Students are given the opportunity to gain practical experience of participating in real Ethical Hacking projects and 100% placement assistance. The Recon Ethical Hacking Course in Delhi is run under the highly experienced industry professionals. It is recognized among the leading Ethical Hacking Center in Delhi, as it operates on a mix of practical learning and learning theory. This type of comprehensive behavioral training with good exposure facilitates the complete transition of the student into a professional.

- **BUG Hunting toolkit**
- **24x7 Online Classes Available**
- **BUG Hunting Certificate**
- **Interview Preparation**
- **1 Year Membership**
- **Training by experienced trainers**
- **Live Hunting**
- **Checkpoint based training**
- **Class recording**
- **24x7 Support**

BUG Hunting Course Content

- Module 1 : Cross Site Scripting (XSS)
- Module 2 : Host Header Attack
- Module 3 : URL Redirection
- Module 4 : Command Injection
- Module 5 : Critical File Found
- Module 6 : File inclusion
- Module 7 : Source code disclosure
- Module 8 : File Upload
- Module 9 : Parameter Tampering
- Module 10 : SPF attack
- Module 11 : SQL Injection
- Module 12 : No Rate Limiting
- Module 13 : Long Password DOS
- Module 14 : Insecure Direct Object Reference
- Module 15 : Joomla Security vulnerabilities
- Module 16 : Account Lockout
- Module 17 : Apache HTTP server byte range DOS
- Module 18 : Apache struts RCE Hunting
- Module 19 : Application Server Vulnerabilities
- Module 20 : Authentication Testing
- Module 21 : Buffer Overflow
- Module 22 : CMS Hunting
- Module 23 : Comprehensive Command Injection

- **Module 24 : Cryptographic Vulnerabilities**
- **Module 25 : CSRF**
- **Module 26 : Drupal Security Vulnerabilities**
- **Module 27 : Account takeover through support service**
- **Module 28 : Exposed Source Control**
- **Module 29 : Extraction Information and GEO location through uploaded images**
- **Module 30 : Heart bleed**
- **Module 31 : HSTS**
- **Module 32 : HTTPOXY Attack**
- **Module 33 : Identity Management Testing**
- **Module 34 : Advanced Indirect Object reference**
- **Module 35 : Multi Factor Authentication (2FA) Security Testing**
- **Module 36 : Password Reset Poisoning**
- **Module 37 : Server Side Injection (SSI)**
- **Module 38 : Session Fixation**
- **Module 39 : Shell Shock RCE Testing**
- **Module 40 : SSRF**
- **Module 41 : Testing for Session Management**
- **Module 42 : Ticket Security Testing**
- **Module 43 : Web cache deception Attack**
- **Module 44 : WebMin unauthentic RCE**
- **Module 45 : Word Press Security testing**
- **Module 46 : Application Logic Vulnerabilities**
- **Module 47 : Broken Authentication**
- **Module 48 : Browser cache weakness**

- Module 49 : Cache Testing
- Module 50 : CAPTCHA Security Testing
- Module 51 : Code Injection
- Module 52 : Cookies Testing
- Module 53 : CORS
- Module 54 : CRLF Injection
- Module 55 : CSS Injection
- Module 56 : Dangerous HTTP Methods
- Module 57 : Testing for default Configuration
- Module 58 : Directory listing testing
- Module 59 : DOM clobbering
- Module 60 : HTTP Parameter Pollution
- Module 61 : Identity Management Testing
- Module 62 : LDAP Injection
- Module 63 : Log injection
- Module 64 : Null Byte Injection
- Module 65 : OAUTH Security Testing
- Module 66 : Open redirection
- Module 67 : Web Application Firewall Testing
- Module 68 : Parameter Modification Testing
- Module 69 : PHP Object Injection
- Module 70 : RACE condition Vulnerability
- Module 71 : Relative Path Overview
- Module 72 : Remote Code Injection
- Module 73 : HTTP Headers Testing

- Module 74 : HTTP Headers Testing
- Module 75 : SSL Security Testing
- Module 76 : SSTI Testing
- Module 77 : Template Injection
- Module 78 : Virtual Host Misconfiguration
- Module 79 : Vulnerable Remember me Testing
- Module 80 : Weak Password Reset
- Module 81 : XML Quadratic Blowup
- Module 82 : XML RPC Pingback
- Module 83 : XXE Injection
- Module 84 : Advanced Training About Burp Suite

Contact Details:

- ✓ Phone : +91-8595756252
  +91-8800874869
- ✓ Emai : Training@reconforce.in
  Enquiry@reconforce.in
- ✓ Website : www.reconforce.in
  www.reconcybersecurity.com
- ✓ Address : D-64, Ground floor, Gali no-3 Laxmi Nagar
  Near Metro Exit Gate no-5
  Delhi- 110092