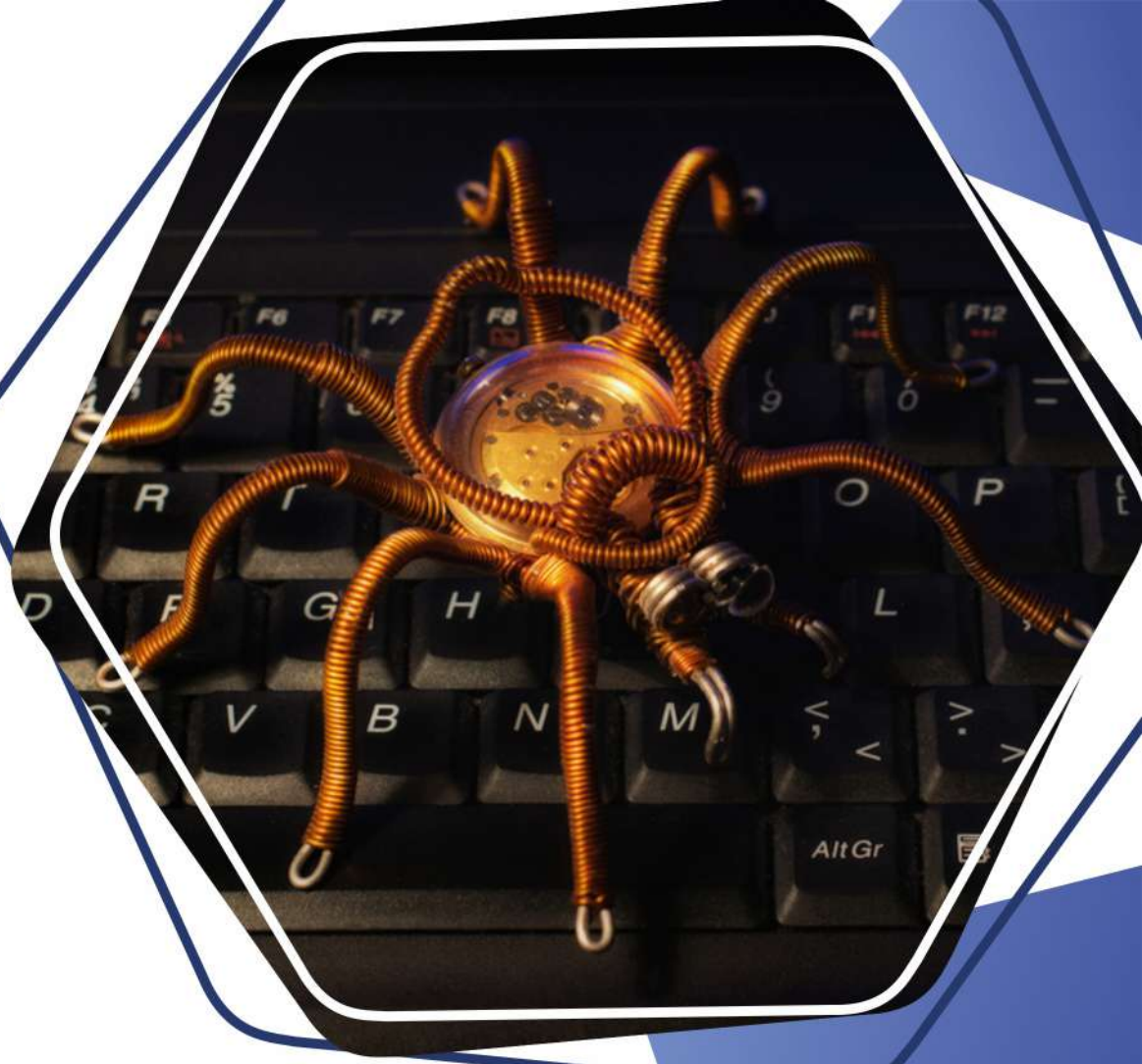
RECON CYBER SECURITY

BUG HUNTING

DURATION 2.5 MONTHS

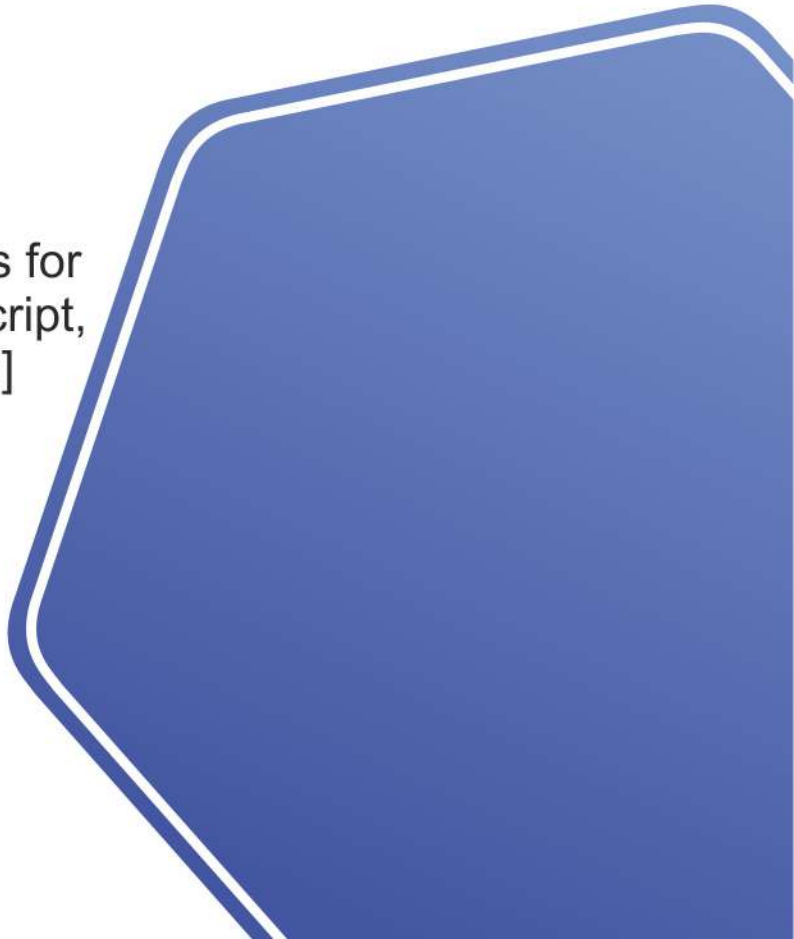


OVERVIEW

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?

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 cybersecurity 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.

COURSE SYLLABUS

WWW.RECONFORCE.IN

Bug Hunting Course Module

01. Introduction
02. Information Gathering
03. BurpSuite Introduction
04. Cross Site Scripting (XSS)
05. Host Header Injection
06. URL Redirection
07. Parameter Tempering
08. HTML Injection
09. SQL Injection
10. File Inclusion
11. Missing SPF Record
12. No rate Limiting
13. Source Code Discloser
14. Long Password Dos Attack
15. IDOR
16. Server Site Request Forgery (SSRF)
17. Cross Site Request Forgery (CSRF)
18. Hostile Subdomain Takeover
19. S3 Bucket Takeover
20. Command Injection (RCE)
21. File Uploading
22. XML External Entity Injection
23. Buffer Overflow
24. Wordpress Vulnerability
25. Joomla Vulnerability
26. Drupal Vulnerability
27. CMS Vulnerability Hunting
28. HSTS (HTTP Strict transport security)
29. Session Fixation
30. Account Lookout
31. Password Reset Poisoning
32. Identity Management test Testing
33. Authentication Testing
34. Cryptographic Vulnerability
35. Session Management Testing
36. Exposed Source Code Control System
37. Apache Structs RCE Hunting
38. Web Cache Deceptions
39. Server Side Includes Injection
40. Ticket Tricks Bug Bounty
41. Multi-Factor Authentication
42. HTTPoxy Attact
43. Webmin Unauthentication RCE
44. HeartBleed
45. Appweb Authentication bypass
46. Ngnix
47. MySQL Authentication Bypass
48. DMS Zone Transfer
49. Log Injection
50. Black (Jinja-2) SSTI to RCE
51. Handloop Vulnerability
52. CSRF Same Site Bypass
53. Jwt Token Attack
54. Email Bounce Resource
55. IVR Call Request Crash
56. Weak Password Reset
57. Business Logic Vulnerability
58. RPC Ping Back Attack
59. WAF / MOD Security Bypass
60. Broken Authentication
61. Open Redirection
62. Null Byte Injection
63. CORS Vulnerability

Tools and Benefits of the Diploma course

- Online and Offline classes
- Networking Certificate after completion
- Training by experienced trainers
- Checkpoint based training
- Live Hunting
- 1 Year Membership
- Class session recordings
- 24x7 Support

Contact Us:

Call or WhatsApp

+91-8595756252 | +91-8800874869

Email Id

Info@reconforce.in

enquiry@reconforce.in

Branch 1:

Street No. 08, Plot No.308,
Main Market Sant Nagar
Burari - 110084

Branch 2:

D-64, Main Vikas Marg, Laxmi Nagar
Delhi - 110092

www.reconforce.in | www.reconcybersecurity.com