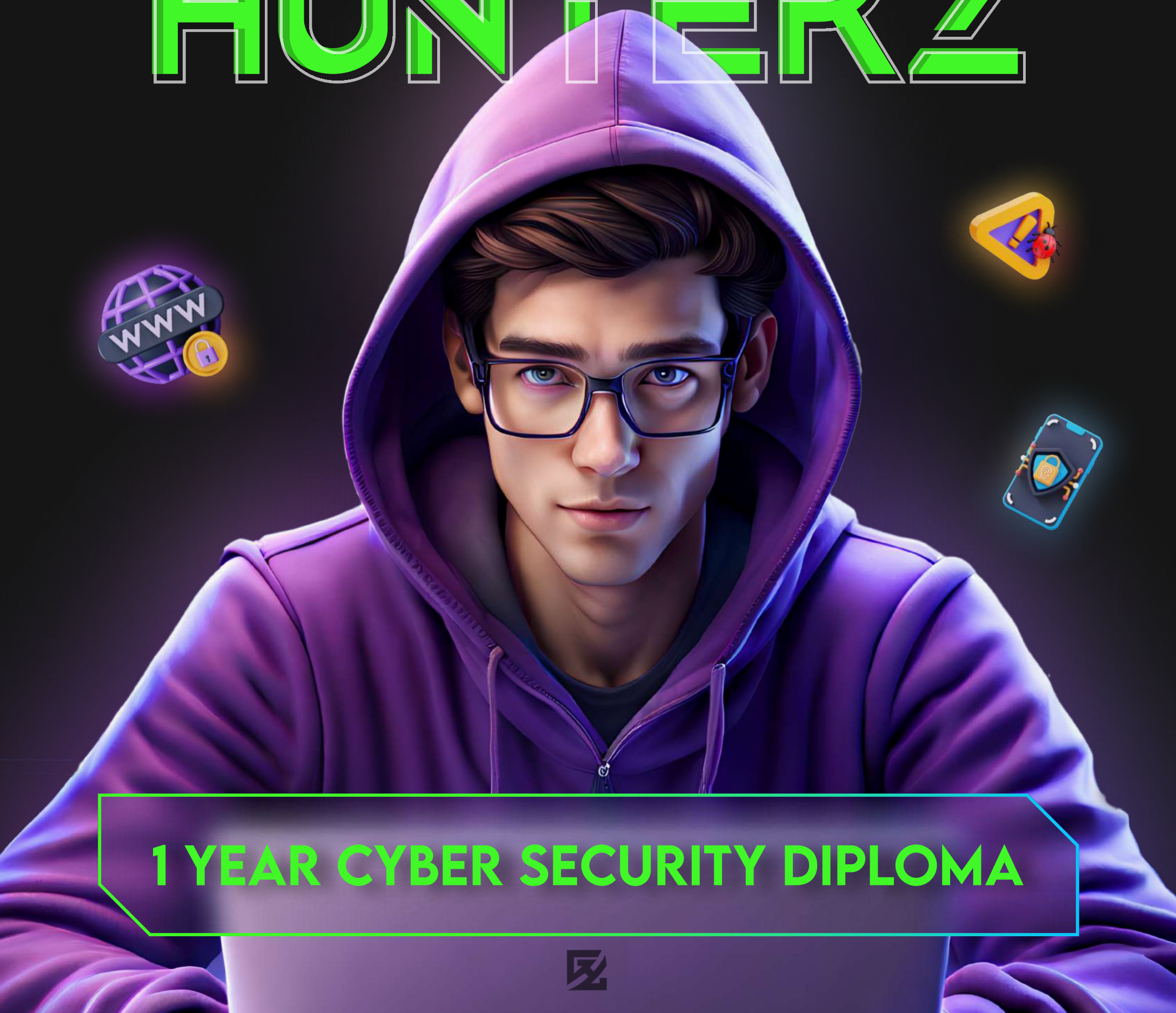
CYBER HUNTERZ



1 YEAR CYBER SECURITY DIPLOMA

1 YEAR DIPLOMA

LEVEL 1
ADVANCED NETWORKING

Module 01: Introduction to Networking
Module 02: Networking Fundamentals
Module 03: OSI Model
Module 04: TCP/IP Model
Module 05: Concept of Layers
Module 06: Lab Configuration
Module 07: Network Devices Fundamentals
Module 08: Internet Protocols
Module 09: Difference between IPv4 & IPv6
Module 10: Subnetting
Module 11: Router Fundamentals
Module 12: Routing Protocols
Module 13: WAN Protocols
Module 14: PPP/ NAT & NAT PAT
Module 15: SSH
Module 16: DHCP
Module 17: BGP

LEVEL 2
ETHICAL HACKING

Module 01: Ethical Hacking Introduction
Module 02: Building Custom lab for hacking
Module 03: Reconnaissance
Module 04: Scanning
Module 05: System Hacking
Module 06: Malware Generation And analysis
Module 07: Trojans and Ransomwares
Module 08: Bots and Botnets
Module 09: MITM with Kali Linux
Module 10: MITM with windows
Module 11: Email security
Module 12: Social Engineering tools and Technique
Module 13: Open source for social engineering
Module 14: Denial of service
Module 15: Basics of Web App Security
Module 14: Denial of service
Module 15: Basics of Web App Security
Module 16: Mastering session hijacking
Module 17: SQL Injection Manual Testing
Module 18: SQL Injection Automated Tool Based Testing
Module 19: Bypassing firewall in sql injection
Module 20: Web servers hacking
Module 21: Hacking wireless networks
Module 22: Evading IDS, Firewalls, Honey pots
Module 23: Buffer Overflow
Module 24: Cryptography
Module 25: Mobile hacking
Module 26 : Carrier in Information security as Ethical hacker

LEVEL 3
PENETRATION TESTING

Module 01: Introduction to penetration testing
Module 02: Roping your penetration testing
Module 03: Network and web application scanning techniques
Module 04: Advance social engineering offensive methodology and email security
Module 05: In-depth password attacks
Module 06: System & network exploitation
Module 07:Wireless and browser exploitation
Module 08: Web application penetration testing
Module 09: CTF of a vulnerable machine
Module 10: Report generation best practices

LEVEL 4

WEB APPLICATION SECURITY EXPERT

Module 01: Introduction to application security
Module 02: OWASP Top 10
Module 03: Modern Attacks of Web Application
Module 04: Automated approach of Vulnerability Assessment
Module 05: API security Testing
Module 06: Mitigation Strategy for Web Application loopholes
Module 07: Cloud Introduction
Module 08: Cloud Migration Challenges
Module 09: Cloud Infrastructure Security
Module 10: Cloud Data Security
Module 11: Identity and Access Management
Module 12: Cloud Application Security
Module 13: Cloud Compliance. Policy, Governance
Module 14 : Cloud Incident Response & Intrusion Detection & BCP/DR

LEVEL 5

MOBILE APPLICATION PENETRATION TESTING

Module 1: Android architecture and permission model
Module 2: Android app components
Module 3: Android Debug Bridge (ADB)
Module 4: Setting up an testing lab
Module 5: Reversing application using (jadxs,apktooL,dex2jar)
Module 6: Application vulnerabilities
Module 7: Insecure logging
Module 8: Leaking content provider
Module 9: Insecure data storage
Module 10: Client side injection (sqli)
Module 11: API hooking
Module 12: DOS
Module 13: Pentesting DIVA
Module 14: Drozer
Module 15: MobSF

LEVEL 6

DIGITAL FORENSIC

Module 1: Introduction of CHFI
Module 2: Computer Forensics
Module 3: Investigation Process
Module 4: Searching and Seizing
Module 5: Digital Evidence
Module 6: First Responder Procedures
Module 7: Understanding CHFI Lab
Module 8: Understanding File systems HDD and Windows
Module 9: Windows os Forensics
Module 10: Data Acquisition and Duplication
Module 11: (TOOLS: FTK Imager EnCase)
Module 12: Data Recovering
Module 13: Steganography Image forensics
Module 14: Password Cracking
Module 15: Emails Investigation
Module 16: Logs Analysis
Module 17: Web Attack Investigation
Module 18: Mobile Forensics
Module 19: Data Analysis With (Autopsy)
Module 20: Investigation Report

LEVEL 7

BUG BOUNTY HUNTING

Module 1: XSS
Module 2: Host Header
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
Module 11: SQL
Module 12: No Rate limiting
Module 13: Long Password Dos
Module 14: IDOR
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: Web Cache Deception Attack
Module 22: Webmin Unauthentic RCE
Module 23: WordPress Security testing
Module 24: Application Logic Vulnerabilities
Module 25: Broken Authentication
Module 26: Browser Cache Weakness
Module 27: Cache Testing
Module 28: CAPTCHA Security Testing
Module 29: Code Injection
Module 30: Cookies Testing
Module 31: CORS
Module 32: CRLF Injection
Module 33: CSS Injection
Module 34: DANGEROUS HTTP Methods
Module 35: Testing For Default Configuration
Module 36: Directory Listing Testing
Module 37: DOM Clobbering
Module 38: HTTP Parameter Pollution
Module 39: Identity Management Testing
Module 40: LDAP Injection
Module 41: Blind XSS
Module 42: Buffer Overflow
Module 43: CMS Hunting
Module 44: Comphrensive Command Injection
Module 45: Cryptographic Vulnerabilities
Module 46: CSRF
Module 47: Drupal Security Vulnerabilities
Module 48: Account takeover Through Support Service
Module 49: Exposed Source Control
Module 50: Extraction Information And Geo Location Through Uploaded images
Module 51: Heartbleed
Module 52: HSTS
Module 53: HTTPOXY Attack
Module 54: Identity Management Testing
Module 55: Advanced Indirect object Reference
Module 56: Multi Factor Authentication (2FA) Security Testing
Module 57: Password Reset Poisoning
Module 58: Server side injection (SSI)
Module 59: Session Fixation
Module 60: Shell Shock RCE Testing
Module 61: SSRF
Module 62: Testing For Session Management
Module 63: Ticket Security Testing
Module 64: LOG Injection
Module 65: Null Byte Injection
Module 66: Oauth Security Testing
Module 67: Open Redirection
Module 68: Web Application Firewall Testing
Module 69: Parameter Modification Testing
Module 70: PHP Object Injection
Module 71: RACE Condition Vulnerability
Module 72: Relative Path Overview
Module 73: Remote Code Injection
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: Web Application Firewall Testing
Module 82: XML Quadratic Blowup
Module 83: XML RPC Pingback
Module 84: XXE Injection
Module 85: Advanced Training About Burpsuite

LEVEL 8

PYTHON PROGRAMMING

Module 1: PYTHON AN OVERVIEW
Module 2: PYTHON VARIABLES & DATA TYPES
Module 3: OPERATORS
Module 4: PYTHON CONDITIONAL STATEMENTS
Module 5: PYTHON LOOPING CONCEPT
Module 6: PYTHON CONTROL STATEMENTS
Module 7: PYTHON DATA TYPE CASTING
Module 8: PYTHON NUMBER
Module 9: PYTHON STRING
Module 10: PYTHON LIST
Module 11: PYTHON TUPLE
Module 12: PYTHON DICTIONARY
Module 13: PYTHON SETS
Module 14: PYTHON SYS MODULE
Module 15: PYTHON OS MODULE
Module 16: PYTHON FUNCTION
Module 17: MODULE
Module 18: FILE HANDLING (INPUT / OUTPUT)
Module 19: EXCEPTION HANDLING
Module 20: OOPS CONCEPTS
Module 21: MULTITHREADING
Module 22: PYTHON MAIL SENDING
Module 23: REGULAR EXPRESSION
Module 24: PYTHON WEB SCRAPING
Module 25: PYTHON DATA SCIENCE
Module 26: INTRODUCTION WITH PYTHON ML

LEVEL 9

MALWARE ANALYSIS

Module 1: Introduction
Module 2: Everything you need to know
Module 3: Types of Malware
Module 4: Methodology of Malware
Module 5: Setting Up Lab
Module 6: Dynamic Malware Analysis
Module 7: All about debuggers
Module 8: Static Malware Analysis

WHY CYBERHUNTERZ?

- Global Certification
- 100% Placement Assistance
- CEH | OSCP Certified Mentors
- Hands-On Live Projects
- Real Time Practical Training
- Gamified Security CTFs

OUR STUDENTS AT TOP SECURITY COMPANIES

ABOUT US

Cyber Hunterz: Premier Cyber Security Services and Training in India

Cyber Hunterz is one of India's most trusted providers of comprehensive cyber security services, products, and training. Our offerings include strategic planning, vulnerability assessment, risk assessment, 24/7 Security Operations Center (SOC) support, incident response, and forensic investigation, helping organizations effectively address internal and external threats.

We empower our clients to develop robust security strategies that protect their businesses and enhance operations. We understand that an organization's trust and credibility rely on the strength of its security measures.

In addition to advisory services, we offer world-class practical training to individuals and corporate professionals globally. Our experienced mentors deliver industry-relevant content, enabling students to achieve excellence.

Our focus is on equipping students for the industry from day one, with hands-on training led by certified experts. Our programs are tailored to meet industry demands, ensuring participants can effectively showcase their skills.

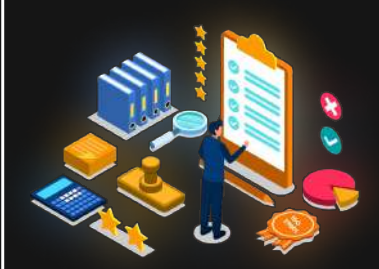
We proudly collaborate with prestigious institutions, including top IITs and NITs, and engage in faculty development programs, workshops, and partnerships across India, fostering a strong cyber security education ecosystem.

SERVICES

SECURITY ASSESSMENT SERVICES 1

RED TEAMING 2

SOURCE CODE REVIEW 3

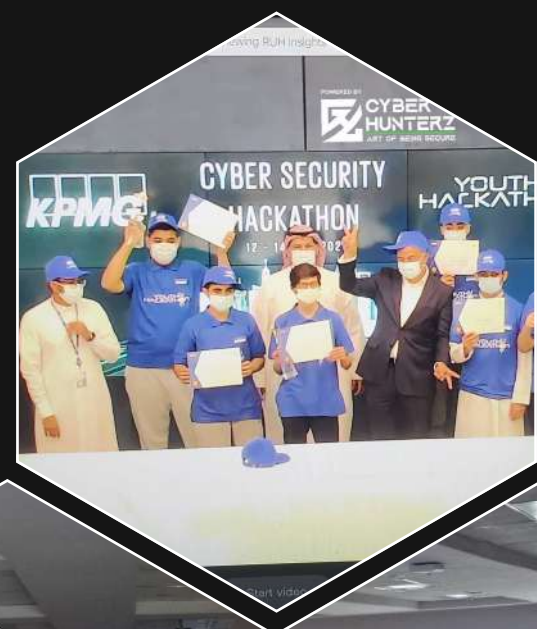


GOVERNANCE RISK & COMPLIANCE 4

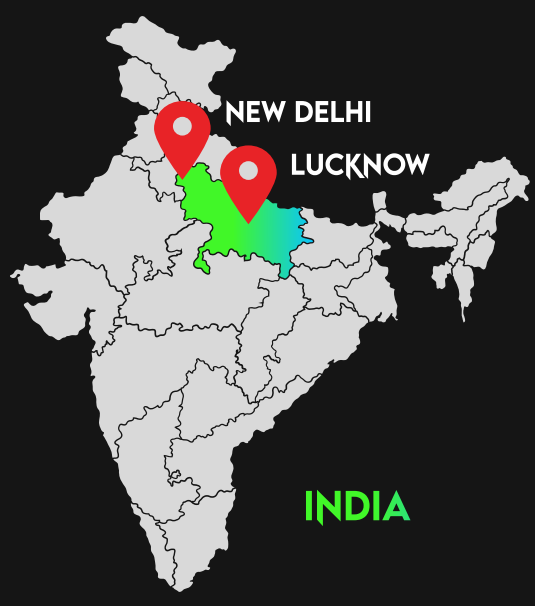
EMAIL SECURITY 5

SECURITY OPERATION CENTER 6

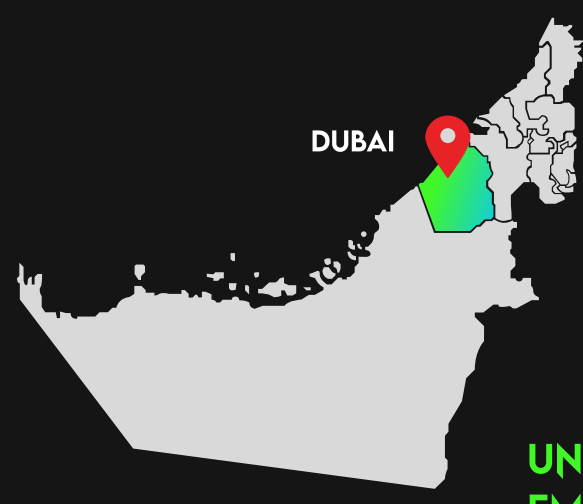
SEMINARS & WORKSHOPS



OUR PRESENCE

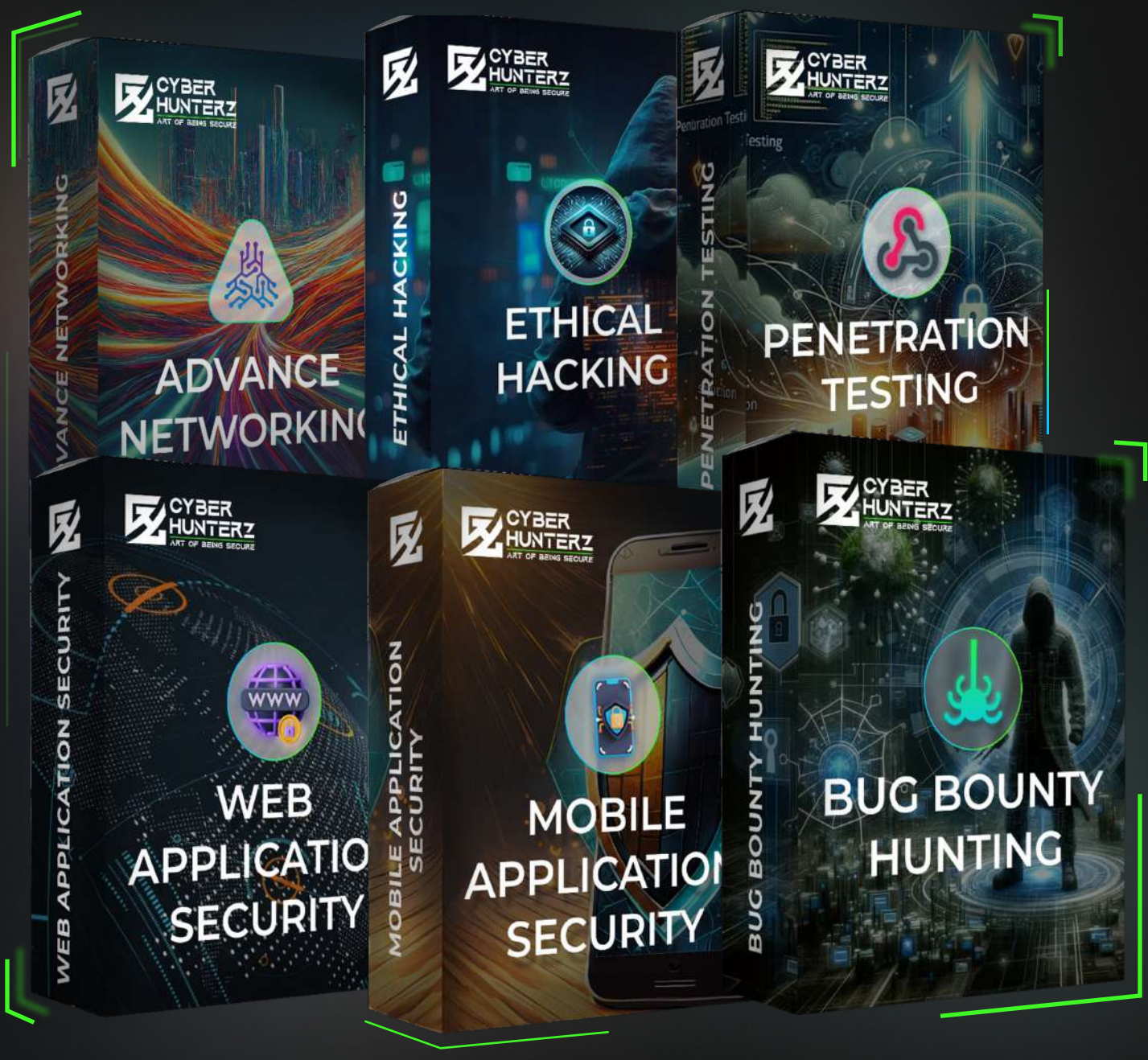


INDIA



UNITED ARAB EMIRATES

SHORT TERM COURSES



CONTACT US

LUCKNOW | DELHI | DUBAI

B-96, 1st floor, Vibhutikhand,
Gomti Nagar, Lucknow, U.P. -226010

cyberhunterz.com

+91 88106 52253
+91 81783 95155

enquiry@cyberhunterz.com

Scan QR to download brochure