

Certificate Program in **ETHICAL HACKING AND CYBER SECURITY**

Class Room | Online | Corporate Training





5000+ Trainees | 20+ Countries
200+ Batches | 500+ Success Stories

Cyber Security FAQ's



DURATION

45 Days



ELIGIBILITY

Any Graduate



CERTIFICATIONS

Digital Nest Certificate



LAPTOP CONFIGURATION

OS: Windows X, I5 7th generation Processor, Ram: 8GB, HDD: 1 TB



ROLES

Security Architect, Security Consultant, Penetration Tester,
Chief Information Security Officer, Cryptographer, Security Analyst,
Security Engineer



AVG PACKAGES

3-13 Lakh p.a.



PRE REQUISITE

Familiarity with C, C++ , PHP, Linux, Unix, Windows,
Saas Model,etc



WHO CAN LEARN

IT Professionals, Administrators, Developers, Graduates,
Job Seekers, End users

KEY HIGHLIGHTS



Training by Real Time Experts



Material, Case Studies & Assignments



One-On-One with Industry Mentors



Dedicated Student Manager



100% Assured Placement Assistance



Hands on Training



Doubt Clarification Sessions



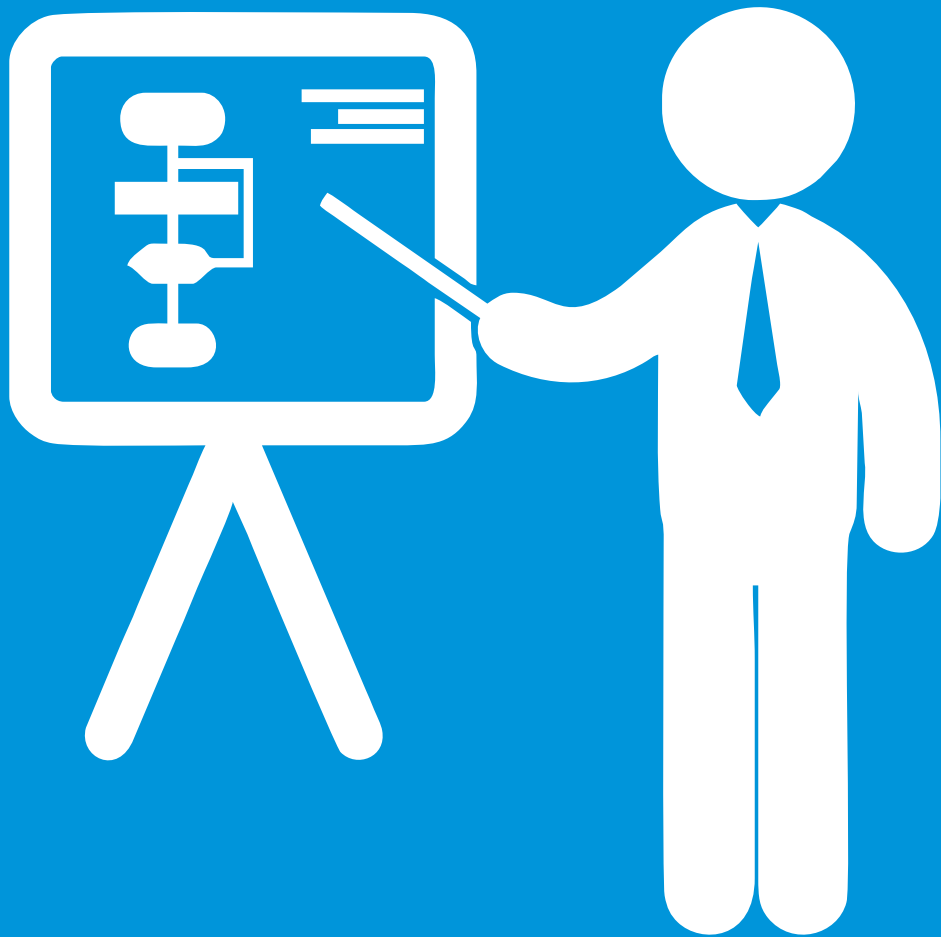
Limited Strength



Resume & Interview Prep Guidance



Course is curated by subject matter experts in Salesforce



COURSE STRUCTURE

PENETRATION TESTING :

Advanced In-detail Web & Mobile Application: Vulnerability Assessment & Penetration Testing: Application Security with Real Time Knowledge:

1. Introduction to the web Application Vulnerability Assessment & Penetration Testing

2. Standards to Follow

1. OWASP TOP 10 overview
2. OWASP Security testing methodology
3. SANS Top 25 overview

3. Intro to the Bug Bounty Program

1. Different Bug Bounty Platforms
2. Understanding In-Scope & Out-of-Scope
3. Understanding the Vulnerability Priority
4. Explanation about any one Bug bounty platform
5. About CTF in bug bounty (i.e. Hackerone)

4. Application Analysis

1. Understanding difference between Static & Dynamic Applications
2. Analysis of the application flow
3. Different categories of applications
4. Analysis of the application functionalities and their functional cycle

5. Authentication Testing

1. About Authentication Process Cycle
2. Understanding different login patterns
3. Introduction to Burp Suite
4. Authentication Bypass using SQL payloads
5. Login Brute force
6. User Enumeration
7. Hard Coded Credentials
8. Insecure Logout Implementation
9. Strict Transport Security Not Enforced

10. Testing OTP Length, Duration & Rate Limitation
11. Mobile/Email OTP Bombing
12. Leakage of OTP in Later Response
13. Response Tampering OTP Bypass
14. Testing IDOR - Token Based Authentication
15. Sending User Credentials using GET method

6. Testing the User Registration Process

1. About User Registration Process Cycle
2. Testing Input Validation - XSS
3. Verification of Email address / Mobile Number
4. Weak Username or un-enforced policies
5. Weak password policies

7. Testing Password Reset Functionality

1. About Password Reset Functionality Cycle
2. Testing authorization issue in-case of UID & Token
3. Testing Life time of reset link
4. Predictability of the token encryption (Base64 based encryption)
5. Testing password reset token expiration

8. Sensitive Data Exposure

1. About Sensitive Data Exposure depending on Application Category
2. Insecure Error Handling
3. Information disclosure via metadata
4. Insecure communication channel
5. Hidden/sensitive directories & files in robots.txt
6. Return of sensitive information in later responses (example: password, otp, other user's private/sensitive information)

9. API Communication

1. About API Communication
2. Authorization Header Analysis
 - Basic Authentication token
 - Barer Token
 - None
 - Custom
3. About JWT Token pattern
4. Un-Authenticated/Anonymous Access

10. Testing for Cookie Attacks

1. Understanding the cookie Life Cycle
2. Weakness in cookie life cycle
3. Cookie with sensitive data
4. XSS via cookie
5. Missing HTTP only Flag
6. Missing Secure Flag
7. Analysing authorization/privileges implementation through cookies

11. Headers & Policy Scrutiny

1. CRLF Injection
2. Host Header Injection
3. Cross Origin Resource Sharing
4. Click Jacking
5. URL Redirection

12. Session Management Issues

1. Testing for Insecure Logout Implementation
2. Testing for CSRF Vulnerability
3. Bypass Methods of CSRF Vulnerability

13. Testing for Authorization testing

1. Concept of Access Control & RBAC
2. Insecure Direct Object Reference (IDOR)
3. Testing for Vertical Privilege Escalation
4. Testing Horizontal Privilege Escalation
5. Directory Traversal

14. Data Validation Testing

1. Malicious file upload
2. Cross Site Scripting
3. CSV Injection
4. HTTP Parameter Solution

15. Injections (DAY 28-29)

1. Remote Code Execution
2. SQL Injection
3. XML Injection / XXE
4. OS Command Injection

16. Testing for Server Side Issues

1. Testing for SSRF
2. Template Injection

17. Business Logic Issues

1. About different payment methods Integration
2. About Payment Tampering Method
3. Straight Forward Payment Tampering
4. Add-on Based Payment Tampering
5. Coupon Based Payment Tampering
6. Longitude and Latitude based payment tampering (In Case of CAB booking, if validation process depends on Long & Lat)
7. Failure to Success Journey
8. HTTP Parameter pollution (In case of Amount parameter)
9. Getting High Benefits Features with Low Benefit cost (In case of Feature id)
10. Test with Fake DC/CC with CVV
11. Sensitive information Leakage
12. Insecure Direct Object Reference (Getting Booking & Billing Details, in case of E-Comers application)
13. Testing IDOR (In case QR Code generated based on ID value)
14. Bypassing Attaching Mandatory Entities

18. Cloud Misconfiguration

1. AWS S3 Bucket Misconfiguration

19. Testing for Security Misconfiguration

1. Outdated Framework /CRM/ Wordpress
2. Enabled Directory Listing
3. Default accounts with default passwords

20. Miscellaneous

1. Reflected File Download
2. Accessing Default Files (i.e: phpmyadmin)

21. Other Vulnerabilities

1. Web Cache Poisoning

22. Foot Printing & Information Gathering

1. About Red Team Assessment overview (RTA)
2. Foot Printing & Info Gathering Concepts

23. API testing

1. Introduction to postman Collection
2. Integrating burp proxy to the postman collection

ETHICALHACKING

Introduction to Ethical Hacking:

- Basics of Ethical Hacking
- Types of Hackers

Reconnaissance:

- Information Gathering
- Foot Printing

Kali Linux Basics:

- Basic Commands of Kali Linux
- Configuration of Kali Linux

Password Cracking:

- Password Guessing
- Default passwords
- Password Dictionary Creation

Brute Force Attacks:

- OTP Brute Forcing
- Password Brute Forcing
- Login Brute Forcing

Injection Attacks:

- CSV Injection
- SQL Injection
- XXS Injection

Phishing attacks:

- Account Take over

Privilege Escalation:

- Low privilege & High privilege Escalation

Cryptography:

- Encryption
- Decryption

• Web Application Hacking Basics:

• Mobile Application Hacking:

• Vulnerability Analysis:

• Vulnerability Scanning:

• OWASP Top 10:

• Proxies & VPN:

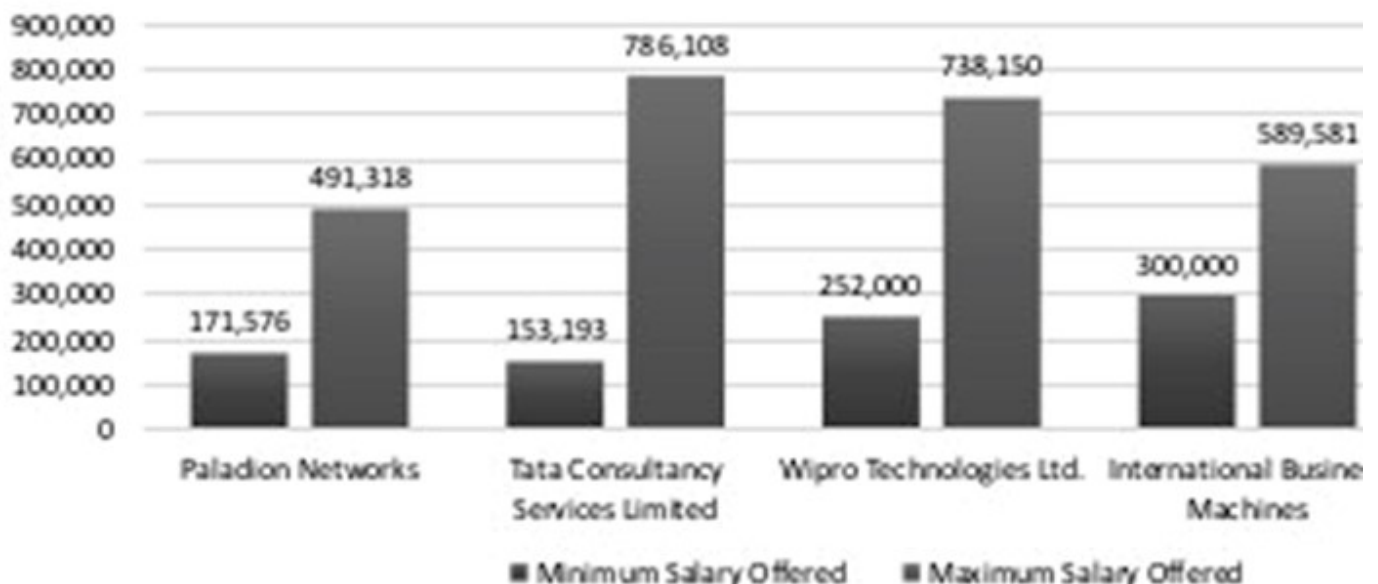
• HTTP parameter pollution Attack:

• User & Password Enumerations:

Salary Ranges

TOP RECRUITERS IN IN

The figures as depicted by the graph below will provide an insight into the salary ranges for Security professionals which the companies are ready to pay. This will also provide reasons why Ethical Hacking programs have become the most demanded skill set.



Country: India

Currency: INR

Source: www.Payscale.com

Our Trainees Hail from

Ready to get
incubated in
**ETHICAL HACKING
AND
CYBER SECURITY**
Lets Start

Reach Us:

📍 1st Floor, SNR Towers,
Beside BVRIT
City Center bus stop,
PANJAGUTTA, Hyderabad.

📍 2nd Floor,
Above Karnataka Bank,
Silicon Valley Road,
HITECH-CITY, Hyderabad.

☎ +91 80889 98664 @ info@digitalnest.in 🌐 www.digitalnest.in

Follow us on



/digitalnest



/digitalnesthyd



/digitalnest



/digitalnesthyd