APEC

transforming careers...

301, Annapurna Block,
Aditya Enclave, Ameerpet,
Hyderabad – 500016
Ph:+91 7671043906

https://www.apectraining.com

CYBER SECURITY

Duration:2M

NETWORK & SYSTEM ESSENTIALS

- Different Operating Systems and their commands
- Comparison of Windows, Linux, UNIX
- What is IP? Why We Use?
- What is A Port? Why We Use It?
- Different Types of Ports
- What Is A Protocol > Types of Protocols / About
- Every Protocol for Network Transmission
- What Are Different Layers Of Network?
- What type of attacks can be performed on each layer of network?
- What Is Data Transmission or Info Transmission on Network

INTRODUCTION TO WEB APPLICATION

- Vulnerability assessment & penetration testing
- Standards to follow OWASP TOP 10 overview
- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- CrossSite Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging & Monitoring
- OWASP Security testing methodology

APPLICATION ANALYSIS

- Understanding difference between Static & Dynamic Applications
- Analysis of the application flow
- Different categories of applications
- Analysis of the application functionalities and their functional cycle

TESTING THE USER REGISTRATION PROCESS

- About User Registration Process Cycle
- Testing Input Validation XSS
- Verification of Email address / Mobile Number
- Weak Username or unenforced policies we Weak password policies

AUTHENTICATION TESTING

- About Authentication Process Cycle
- Understanding different login patterns
- Introduction to Burp Suite
- Authentication Bypass using SQL payloads
- Login Brute force
- User Enumeration
- Hard Coded Credentials
- Insecure Logout Implementation
- Strict Transport Security Not Enforced
- Testing OTP Length, Duration & Rate
- Limitation
- Mobile/Email OTP Bombing
- Leakage of OTP in Later Response
- Response Tampering OTP Bypass
- Testing IDOR Token Based
- Authentication
- Sending User Credentials using GET method

TESTING PASSWORD RESET FUNCTIONALITY

- About Password Reset Functionality Cycle
- Testing authorization issue incase of UID & Token
- Testing Life time of reset link
- Predictability of the token encryption (Base64 based encryption)
- Testing password reset token expiration

SENSITIVE DATA EXPOSURE

- About Sensitive Data Exposure depending on Application Category
- Hidden/sensitive directories & files in robots.txt
- Return of sensitive information in later responses (example: password, OTP, other user's private/sensitive information)

API COMMUNICATION

- About API Communication
- Authorization Header Analysis
- Basic Authentication token
- Barer Token
- None
- Custom
- About JWT Token pattern

SESSION MANAGEMENT ISSUES

- Testing for CSRF Vulnerability
- Bypass Methods of CSRF Vulnerability
- Testing for Insecure Logout Implementation

TESTING FOR AUTHORIZATION TESTING

- Concept of Access Control & RBAC
- Insecure Direct Object Reference (IDOR)
- Testing for Vertical Privilege Escalation
- Testing Horizontal Privilege Escalation

DATA VALIDATION TESTING

- Malicious file upload
- Cross Site Scripting
- HTTP Parameter Solution

INJECTIONS

- Remote Code Execution
- SQL Injection
- OS Command Injection

TESTING FOR SERVER SIDE ISSUES

- Testing for SSRF
- Template Injection

BUSINESS LOGIC ISSUES

- About different payment methods Integration
- About Payment Tampering Method
- Straight Forward Payment Tampering
- Addon Based Payment Tampering
- Coupon Based Payment Tampering 6
- Longitude and Latitude based payment tampering (In Case of CAB booking, if validation
- Process depends on Long & LAT)
- Failure to Success Journey
- HTTP Parameter pollution (In case of Amount parameter)
- Getting High Benefits Features with Low Benefit cost (In case of Feature id)
- Test with Fake DC/CC with CVV
- Sensitive information Leakage
- Insecure Direct Object Reference (Getting
- Booking & Billing Details, in case of Ecommerce application

CLOUD MISCONFIGURATION

- AWS S3 Bucket Misconfiguration

TESTING FOR SECURITY MISCONFIGURATION

- Outdated Framework /CRM/Wordpress
- Enabled Directory Listing
- Default accounts with default passwords

FOOT PRINTING & INFORMATION GATHERING

ABOUT RED TEAM ASSESSMENT

- OVERVIEW (RTA)
- Foot Printing & Info Gathering Concept

API TESTING

- Introduction to postman Collection
- Integrating burp proxy to the postman collection

INTRODUCTION TO ETHICAL HACKING

- Basics of Ethical Hacking
- Types of Hackers
- RECONNAISSANCE
- Information Gathering
- Foot Printing
- Scanning
- Enumeration
- 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

CRYPTOGRAPHY:

- Encryption
- Decryption

INJECTION ATTACKS

- CSV Injection
- SQL Injection
- XXS Injection
- PHISHING ATTACKS
- Account Take over
- DOS & DDOS
- PRIVILEGE ESCALATION AS ATTACK
- Low privilege & High privilege Escalation

aws

JAVA / PYTHON / .NET
FULL STACK

DEV OPS

DATA SCIENCE

python

Azure
(ADMIN, DEVOPS & DATA ENGINEERING)

React

ANGULAR

Power BI

UiPath

Office

Advanced
Excel
Training

Tally
POWER OF SIMPLICITY
Tally Prime

301, Annapurna Block,
Aditya Enclave, Ameerpet,
Hyderabad – 500016

Ph:+91 7671043906

https://www.apectraining.com

APEC
transforming careers...