CHAITANYA CYBER STRIX
TECHNOLOGIES

ADVANCED WEB APPLICATION SECURITY

WEB APPLICATION PENETRATION TESTING

Web application penetration testing works by using manual or automated penetration tests to identify any vulnerability, security flaws or threats in a web application. The tests involve using/implementing any of the known malicious penetration attacks on the application.

WEB APPLICATION SECURE CODING (PYTHON)

Secure coding makes it easier for developers and programmers to weed out common vulnerabilities in their software by following certain best practices. Defects, bugs and logic flaws are consistently the primary cause of commonly exploited software vulnerabilities.

CONTACT US

+91 81251 30203

www.chaitanyacyberstrix.com

H.No : 10-15/59/1, Surya Nagar Colony, Vajpaypee Road,
R.L Nagar, Medchal, Hyderabad, Telangana, India, 501301

COURSE PREREQUISITES

Basic knowledge of HTML ,JS ,Python or any backend programming languages like PHP, Java, etc..
One year in an information security role or equivalent experience is recommended.
Ability to read and understand python code will help, although it is not mandatory.

WHO SHOULD TAKE THIS COURSE?

Bug Bounty Hunters
Penetration Testers
Application Developers
IT Security professionals with a technical background

CLASSROOM TRAINING

When it comes to quality instruction in a classroom training experience a more stimulating learning environment with our optimized mix of lecture, hands-on practice, when you have doubts our instructors are available to clear and ensure you comprehend the course and knowledge.

ONLINE TRAINING

We are providing training through Online LIVE with a real time live instructor. The live instructor teaches the course and provides the opportunity for students to ask live questions via voice or instant message during the live training event with practicals

WORKSHOPS

We conduct workshops and seminars in Information Security. Ethical Hacking & Information Security Workshop will teach you how to protect yourself from the cyber attacks and make yourself come to know how to secure your organization from hackers.

WEB APPLICATION PENETRATION TESTING

10 HRS
DURATION

Linux For Hackers
Basic commands
Standards of Unix
Advanced way of using Linux for pentesters

Basic Reconnaissance
Recon with tools
Shodan
Crawling and gathering the info

Advanced Reconnaissance & Asset Discovery
Fuzzing
Collecting word-list
Preparing word-list
GitHub Recon (Python)
Basics of python
Understanding the use cases of code
Developing basic scripts
Using python as a hacker

Broken Cryptography
Types of cryptography
Encoding
Encryption
Hashing
Difference between them

Broken Authentication
Password Reset link poisoning
Bypassing password
OTP bypass
Reseting victims password
Tab-nabbing/Advanced Phishing attacks

Improper Session Management
Week session management
Session takeover

Creating Session Tokens

Injection Attacks

SQL injection
Command Injection
Server Side Template Injection
Server Side inclusions

Authentication Bypass

Response tampering
Injecting malicious scripts to bypass Authentication
CSRF

Cross-Site Scripting (XSS)

Reflected XSS
Stored XSS
Dom XSS
Escalating attacks with XSS
Injecting advertisements with XSS
Taking full session control using XSS

Sensitive Data Exposure

Smart ways to Identify data exposure in Source code
GitHub data/sensitive keys leak
Data leaks in logs
Looking for sensitive information with tools

Broken Access Control

IDOR
Looking for Admin panels
Deleting other user contents
Accessing other user data

Business logic Flow

Parameter tampering
Logic attacks
Functionality to bug convertion.

WEB APPLICATION SECURE CODING (PYTHON)

25 HRS
DURATION

Understanding Standards of Protocols and Browser Behavior.

- HTTP
- HTTP stateless
- HTTPS
- TLS
- Cookies,Session,Tokens
- Headers
- Browser Behavior

Understanding how Front End Codes and Frameworks can affect a web application

- HTML,css,js and Frameworks (jquery) nature
- Dynamic web page creation
- Possible attack on dynamic web pages
- Securing the frontend

Understanding Cryptography

- Encryption, Encoding, and Hashing
- Understanding Secure Radom
- Why, Where and When to use them
- Possible attacks on cryptography
- Implementing the security best practices

Understanding Backend Code Issues

- Authentication bypass and reason behind the bypass (with detailed debugging in code) & Applying them on similar kinds of areas
- Fixing the code to protect from Authentication bypass
- Direct object reference Issue and Fix in code level
- What is the issue of using If else improperly in the program
- White listing and black listing, When and where to apply each
- Backend directory info leaks and keeping them safe from attackers

Advanced:

Understanding 3rd party vulnerabilities and How to secure our application from that.

- Command Injection and Fixing in code level
- RCE issues and Best practices to follow in code
- Understanding Business logic issues/Fixes
- Understanding SQL attacks and Handing the SQL queries securely
- What is a CVE and how to protect our application in case it is a ZERO day issue.
- Checks to be performed while configuring a server and firewalls
- To what extent a fire wall or IDPS can help us and what could be a better approach to keep the application safe
- Understanding Frontend server, Backed server and cache servers
- Understanding secure design architecture importance and steps to process it.
- Steps to take while integrating 3rd party services like OAUTH, Payment gateways etc