

# **Engineering Staff College of India**

Autonomous Organ of The Institution of Engineers (India) Old Bombay Road, Gachi Bowli, Hyderabad – 500 032. Telangana, India



INFORMATION TECHNOLOGY DIVISION

# CONTINUING PROFESSIONAL DEVELOPMENT PROGRAMME Web Application Penetration Testing



and Web Security

05 - 07 February 2024

(Classroom / Online Training)



### Introduction

Web applications play a vital role in every modern organization. But, if your organization does not properly test and secure its web apps, adversaries can compromise these applications, damage business functionality, and steal data. Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems.

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. The penetration tester exhibits/fabricates attacks and environment from an attacker's perspective, such as using SQL injection tests. The web application penetration testing key outcome is to identify security weakness across the entire web application and its components (source code, database, back-end network). It also helps in prioritizing the identified vulnerabilities and threats, and possible ways to mitigate them.

#### **Objectives**

- Training provides knowledge and skills Web application penetration testing & Web Security
- The instructor-led course will provide knowledge and skills on automated penetration tests to identify any vulnerability, security flaws or threats in a web application.

## **Course Coverage**

- Information Gathering & Basic Terminology
- Introduction of Burpsuite
- Comprehensive XSS
- Host Header Injection
- URL Redirection
- Parameter Tampering
- HTML Injection
- File Inclusion
- Missing/insufficient SPF record

- XML External Entity Injection.
- Insecure CORS Configuration
- Server Side Request Forgery
- Critical File Found
- Source Code Disclosure
- Cross Site Request Forgery
- Hostile Subdomain Takeover
- SQL Injection
- Command Injection
- File Uploading

## Methodology

Methodology of the programme includes

- Learning prerequisites skill through ESCI LMS Platfom
- Online Video Interactive sessions with Cloud based Hand-on Practical,
- Online case studies, Sharing of experiences.

# (An ISO 9001:2015 Certified, AICTE & CEA Recognized Institution) Centre for Promotion of Professional Excellence

#### **Target Participants**

- Information Security Manager, Information Technology Manager, Chief Information Security Officer, and Technical Team.
- Web Developers, Programmers, Software Testers, IT Managers, System Engineers in Government, Public & Private sector Companies.
- Scientiests & Executives of DRDO & Defence Involved in Web development & Testing Activities
- Faculty & Technical shtaff of Engineering Colleges.
- All the Managers / Executives who are using Computer, Mobiles & Internet and looking for Web Security.

#### Benefits to the participants

- After completing this course, the Participant will be able to prevent Web Attacks using new trends & techniques.
- A rare opportunity to experience sharing among numbers of guest speakers and experts from various organizations from all over India.

#### **Programme Dates & Timings**

Venue : Engineering Staff College of India, GachiBowli, Hyderabad
Dates: 05 - 07 February 2024
session timings will be from 10:00 – 17:00 hrs with 1 Hour Lunch Break & 15 Minutes Tea break.

#### **Course Director**

Mr. Syed Azgar , MBA(IT), RHCE, MCSA Sr Faculty & Head IT, Information Technology Division, Engineering Staff College of India, Hyderabad.

#### **Course Fee for Classroom Training**

₹ 15,000/- (Residential Fee) per participant. Fee includes course material, course kit, twin-sharing / single AC accommodation as per availability, Breakfast, Lunch, Dinner, Tea / Coffee and Snacks during the actual days of training programme.

#### **Course Fee for Online Training**

₹ 9,000/- per Participant. Fee includes LMS Platform Access for Digital Learning , 30 Hours Live Interactive Sessions, Experts Online Support and Reading Material Softcopy

**GST** @18% is to be paid extra and above the training fee as training. **PAN Card No.** AAATT3439Q. **GST No: 36AAATT3439Q1ZV, HS No.: 999293** (under commercial training or coaching services – clause 65(105) (ZZC) of Finance act – 1994).

Programme fee is to be paid in in favour of **"THE INSTITUTION OF ENGINEERS (INDIA) – ENGINEERING STAFF COLLEGE OF INDIA"** by **Electronic Fund Transfer (EFT)** to ESCI – **Axis Bank** A/c No. **912010049234564** with The Axis Bank Ltd, Old Mumbai Hwy, Cyberhills Colony, P Janardhan Reddy Nagar, GachiBowli Hyderabad-500032 by NEFT/ RTGS/ IFSC Code No. UTIB 0000733 – MICR No.500211020. **While using EFT method of payment, please ensure to communicate us your company name, our invoice reference and programme title.** 

#### Registration

Online registration shall be available on ESCI web portal http://www.escihyd.org/index.php/it-upcoming-trainings

**To register manually** please send your nominations giving details of name, designation, contact address, email address, mobile no, telephone and fax number of the participant along with the details of mode of payment of fee, addressed to : <u>it@escihyd.org</u>

A Certificate of participation will be awarded to each participant on conclusion of the programme.

Information Technology Division, Engineering Staff College of India Gachi Bowli, Hyderabad – Telangana 500 032 Phone: 040 – 66304100 (EPABX) 66304123/24/25 (Direct), 8886661060 Fax: 040 – 66304103 Email: it@escihyd.org, web portal: www.escihyd.org