Ducara Info Solutions (P) Ltd.

C|OWASP

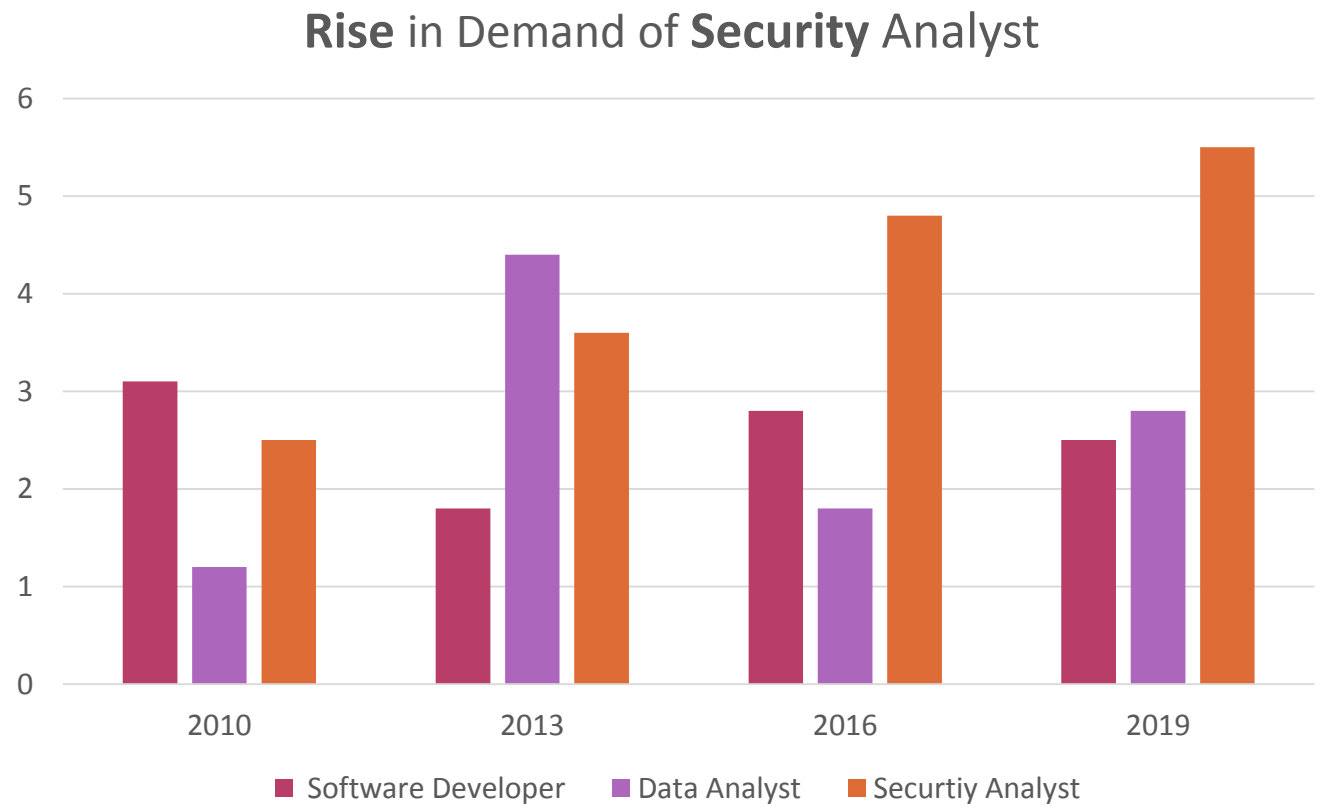
Certified OWASP Pen Tester

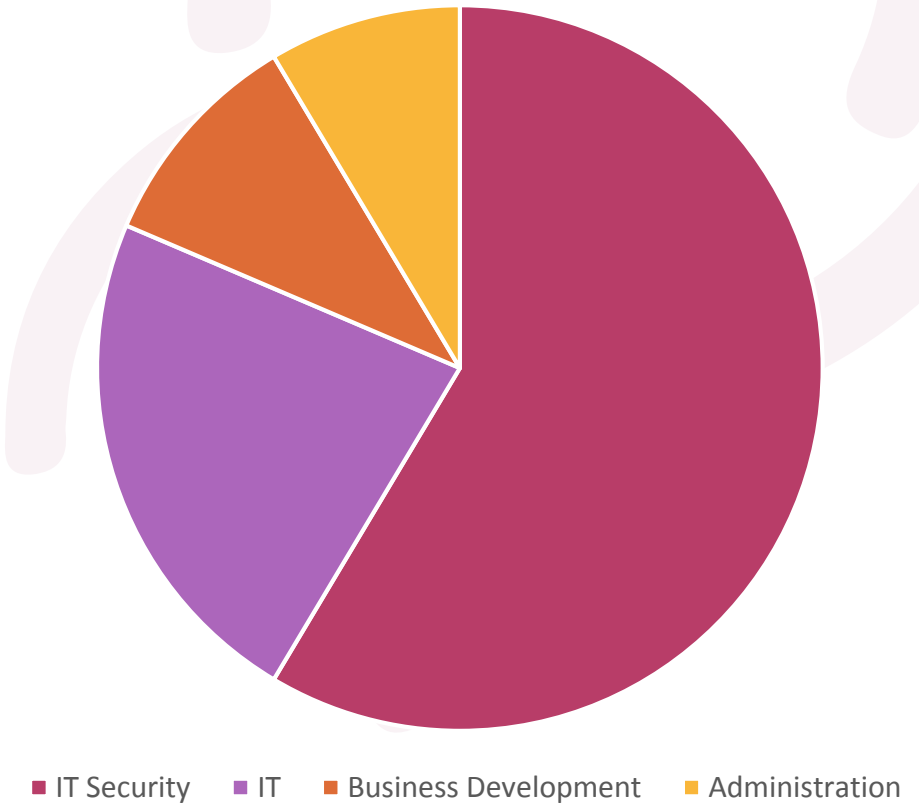
WHY C|OWASP?

Web application **Penetration** testing is the practice of testing a Computer System, Network or Web Application to find security vulnerabilities that an attacker can exploit.

WHAT TREND SAYS?

With the **Increasing** focus on WebApps and websites over the last several years, IT security expert are in great demand worldwide. Many organizations have moved to web services platforms for **Better** scalability, mobility, and availability of the services they provide or use. Pen-testers are among the **Highest** paid professionals in the IT industry.





TARGET AUDIENCE

DURATION: 40 HRS

FRAMEWORK DESIGNER

APPLICATION ARCHITECTS

TECHNOLOGY ARCHITECTS

SYSTEM ARCHITECTS

The Certified OWASP **Pen-tester** program is designed to make you an **Expert** in scanning web applications for vulnerabilities. It will enable you to **Master** the core skill-sets required for testing and managing dynamically scalable, **Highly** available, fault-tolerant, and reliable applications.

WHAT IS THE OBJECTIVE?

Individuals **certified** at this level will have a demonstrated **understanding** of:

- Serve as the central point of contact for **Enterprise Security** for other Technology teams within the organization.
- **Scan** and test security architectures for various information systems.
- Design and implement architectures that will allow business requirements to be met with a minimal degree of **Risk** to the organization.
- Represent security **Platform** in development and implementation of the overall global enterprise architecture.
- Works with Engineering, **Infrastructure** services, and application development organizations to choose appropriate technology solutions.
- Leads **Initiatives** designed to share knowledge across Security Platforms and Technology teams.
- Identifies, recommends, coordinates, and delivers timely knowledge to support teams regarding technologies, processes or **Tools**.
- Gather information, check web based applications and follow **OWASP** Reference testing guides.

Become an **Expert** with Ducara, the stage is all set, get **Certified** with our best OWASP **Penetration** testing program.

C|OWASP PEN-TESTER

SCAN YOUR WEB APPLICATIONS FOR VULNERABILITIES

DUCARA

WHAT YOU WILL LEARN IN THE COURSE?

MODULE	TOPIC	MODULE	TOPIC
01	**Introduction** and Objectives	07	**Session** Management Testing
02	Information **Gathering**	08	Input **Validation** Testing
03	Configuration and Deployment **Management** Testing	09	**Error** Handling
04	**Identity** Management Testing	10	Crypto**graphy**
05	Authentication **Testing**	11	Business **Logic** Testing
06	**Authorization** Testing	12	**Client** Side Testing

MODULE 1

INTRODUCTION AND OBJECTIVES

1. **What** is Web Application Security Testing?
2. **What** is a Vulnerability?
3. **What** is a Test?
4. **The** Approach in Writing this Guide
5. **What** is the OWASP testing methodology?

MODULE 2
INFORMATION GATHERING

1. **Conduct** Search Engine Discovery and Reconnaissance for Information Leakage
2. **Fingerprint** Web Server
3. **Review** Webserver Metafiles for Information Leakage
4. **Enumerate** Applications on Webserver
5. **Review** Webpage Comments and Metadata for Information Leakage
6. **Identify** application entry points
7. **Map** execution paths through application
8. **Fingerprint** Web Application Framework
9. **Fingerprint** Web Application
10. **Map** Application Architecture

MODULE 3

CONFIGURATION AND DEPLOYMENT MANAGEMENT TESTING

1. **Network/Infrastructure** Configuration
2. **Application** Platform Configuration
3. **File** Extensions Handling for Sensitive Information
4. **Review** Old, Backup and Unreferenced Files for Sensitive Information
5. **Enumerate** Infrastructure and Application Admin Interfaces
6. **HTTP** Methods
7. **HTTP** Strict Transport Security
8. **RIA** cross domain policy
9. **File** Permission

MODULE 4

IDENTITY MANAGEMENT TESTING

1. **Role** Definitions
2. **User** Registration Process
3. **Account** Provisioning Process
4. **Account** Enumeration and Guessable User Account
5. **Weak** or unenforced username policy

MODULE 5

AUTHENTICATION TESTING

1. **Credentials** Transported over Encrypted Channel
2. **Default** credentials
3. **Weak** lock out mechanism
4. **Bypassing** authentication schema
5. **Test** remember password functionality
6. **Browser** cache weakness
7. **Weak** password policy
8. **Weak** security question/answer
9. **Weak** password change or reset functionalities
10. **Weaker** authentication in alternative channel

MODULE 6

AUTHORIZATION TESTING

Directory traversal/file

Bypassing authorization schema

Privilege Escalation

Insecure Direct Object References

MODULE 7

SESSION MANAGEMENT TESTING

Bypassing Session Management

Cookies attributes

Session Fixation

Exposed Session Variables

Cross Site Request Forgery (CSRF)

Logout functionality

Session Timeout & Puzzling

MODULE 8

CLIENT SIDE TESTING

Cross site scripting

HTTP Verb Tampering

Parameter Pollution

MODULE 9

ERROR HANDLING

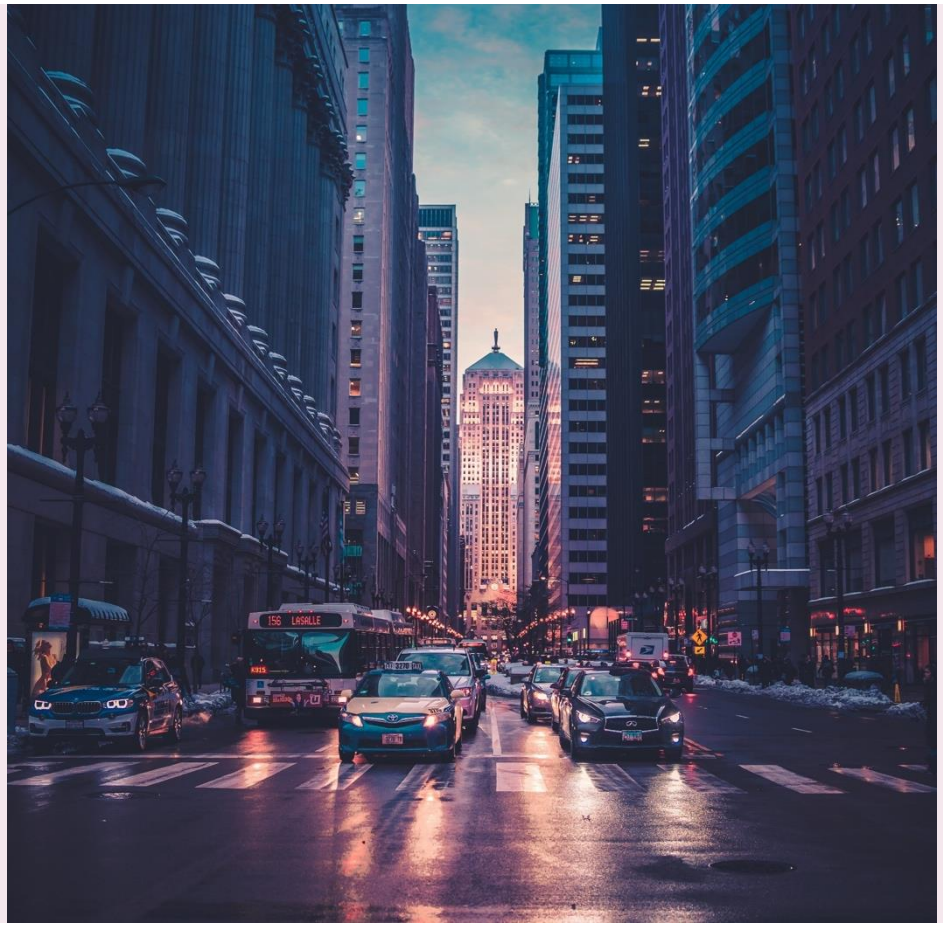
Error, Exception handling & Logging

Generic error messages

Locate the potentially vulnerable code

Vulnerable Patterns

Best Practices



MODULE 10

CRYPTOGRAPHY

Cryptographic Algorithms

Algorithm Selection

Key Storage

Insecure Transmission

Reversible Authentication Tokens

Safe UUID generation

MODULE 11

BUSINESS LOGIC TESTING

- Business logic **DATA** validation
- **INTEGRITY** Checks
- Process **TIMING**
- Number of Times a Function Can be Used **LIMITS**
- **CIRCUMVENTION** of Work Flows
- Defenses Against **APPLICATION** Mis-use
- **UPLOAD** of Unexpected File Types
- Upload of **MALICIOUS** Files

MODULE 12

CLIENT SIDE TESTING

- DOM based **CROSS** Site Scripting
- **JAVASCRIPT** Execution & HTML Injection
- Client Side URL Redirect & **CSS** Injection
- Client Side **RESOURCE** Manipulation
- **CROSS** Origin Resource Sharing
- Cross Site Flashing & **CLICKJACKING**
- **WEBSOCKETS** & Web Messaging
- Test **LOCAL** Storage

DUCARA

THE TECHNOLOGY IS CHANGING EVERY DAY AND WE AT DUCARA ARE COMMITTED TO DEMONSTRATING VALUES. EMBRACING A DIGITAL TRANSFORMATION STRATEGY WHICH DRIVE RETURNS ON IT SECURITY INVESTMENT.

CONNECT US!

INFO@DUCARAINFO.COM

WWW.DUCARAINFO.COM