Octogence Tech Solutions Pvt. Ltd.
Noida, ***India***
Email *| sudhanshu@octogence.com*
Phone*.| +91-9971658929*

Web Application Penetration Testing Training

www.octogence.com

WEB APPLICATION PENTRATION TESTING (WAPT)

Web Applications are everywhere. Every day we access a number of them, use them to share information, connect with people or simply read something. Modern technologies have added more features and functionalities to these applications. Are you aware how secure or should we say insecure they are? Would you like to learn how to perform a penetration test against them? If the answer is yes, then this is the course for you.

In this course on Web Application PenTesting we will learn about the technologies related to web applications, their architecture, what are the different segments that need to tested and what are the policies followed by them. We will dive deep into the applications and learn about various vulnerabilities that exist in them, how to find them and importantly how to exploit them. The testing process demonstrated would cover the automated as well as manual approach so that the participants could learn the industry practices and not just running another scanner. Attacks related to modern technologies such as **Ajax**, **HTML5**, **flash** etc. are also covered.

PARTICIPANTS ATTENDING THIS COURSE WOULD BE ABLE TO:

- Perform an in depth Web Application Penetration Test
- Create an actionable report

PREREQUISITES:

- Basic computer skills.
- Having basic web programming experience would be a plus.

TARGET AUDIENCE:

- Information Security Professionals
- Web Developers

TOPICS COVERED:

- **Basics of Web Applications**
  - Web application structure
  - HTTP basics
  - Cookies, headers, encoding
- **WAPT Process walkthrough**
  - Understanding the scope
  - Difference between black and gray box
  - Methodologies (OWASP, PTES, OSSTMM)
- **Introduction to the tools of the trade**
  - Identify the tools required and understanding their working
  - Application proxy and Automated scanners
- **Building the setup**
  - Setting up the tools for automated and manual testing
  - Tools covered Burp Suite, ZAP, AppScan, Netsparker etc.
- **Vulnerability classes**
  - OWASP top 10
  - WASC classes
- **Application overview**
  - Understanding the application and its flow
  - Identifying key components
- **Information gathering**
  - Application and Server fingerprinting
  - Crawling the application
  - Passive vulnerability identification
- **Authentication testing**
  - Testing for bugs in the authentication and associated modules
  - Username enumeration, authentication bypass etc.
- **Authorization testing**
  - Testing for privilege related issues
- **Session testing**
  - Attacking the session
  - Session fixation, Cross Site Request Forgery (CSRF), session prediction etc.
- **Input validation testing**
  - Attacking through client input
  - Cross Site Scripting (XSS), SQL Injection, XML Injection etc.

- **Automation attacks**
  - Testing the form automation
  - Brute force login, data flooding
- **Other common vulnerabilities**
  - Testing for other commonly found bugs
  - Clickjacking, Header Injection, Open Redirect etc.
- **Attacking advanced technologies**
  - Ajax, HTML based attacks
  - Vulnerability chaining
- **Process and Logical flaws**
  - Understanding the function logic
  - Identifying and exploiting the process
- **Configuration Issues**
  - Flaws related to technologies implemented
- **Web Service Testing**
  - Basics of web services
  - Testing web services
- **Reporting and Post-engagement**
  - Vulnerability Reporting and support

About Us

Octogence is an Information Security service provider which focuses on business centric security. Our aim is to help organizations to be more secure in the cyber space so that they stop worrying about data breaches and can focus on their business. Our qualified, experienced and motivated team aims at providing our clients the service and quality they expect. We have the expertise as well as the flexibility to provide customized solution depending upon the client requirements.