Technology Ireland ICT Skillnet

itb Institute of Technology Blanchardstown
Institiúid Teicneolaíochta Baile Bhlainséir

Application Security (Penetration Testing)

Web applications are not just ubiquitous but carry an attraction and fascination for both user and developer alike. They have also become central to the commercial success of enterprises. They provide user-friendly interfaces, quick access to valuable business resources and seamless deployment to remote users. At the same time and for these very reasons web applications pose a major security risk for enterprises.

The frantic pace at which web applications are developed and deployed – often on tight budgets and with limited resources - means that security considerations often garner scant attention. It is hardly surprising then to see that web apps pose some of the easiest targets for hackers and because these apps are situated within websites across every industry and sector as well as state and government services, the consequences of a security breach can be devastating.

That's why this course is designed to create awareness of the need for the highest standards of security in developing web applications whether you are working as part of a team or alone. Effective security measures should be integrated into the web application development process. If your application is not tested and validated against security threats right from the initial stages of development, it may fail to protect valuable client data and resources from malicious attacks.

Certified Training Programme in Application Security (Penetration Testing)

This online practical course will develop the essential skills required to assess Application Security (Penetration Testing) and to apply an appropriate solution where necessary. Participants will gain an insight into the processes and models underpinning development of secure web applications and explore the adoption of secure web application practices.

INDICATIVE CONTENT

Introduction and Overview

Definition, Web Application Security Scenario, Common Security Mistakes, Why Security Mistakes Are Made, Need for Securing web applications, Types of Security Vulnerabilities, Types

Reconnaissance and Mapping

Discover the infrastructure within the application. Identify the machines and operating systems. SSL configurations and weaknesses. Explore virtual hosting and its impact on testing. Learn methods to identify load balancers. Software configuration discovery. Explore external information sources. Google hacking. Using tools to spider a Web site. Scripting to automate Web requests and spidering. Application flow charting. Relationship analysis within an application. JavaScript for the attacker

Server Side Discovery

Learn methods to discover various vulnerabilities. Information leakage. Username harvesting. Command injection. SQL injection. Blind SQL injection. Cross-Site Scripting (XSS). Cross-Site Request Forgery. Session issues. Explore differences between different data back-ends. Explore fuzzing and various fuzzing tools. Understand methods for attacking Web services

Client Side Discovery

Learn methods to discover various vulnerabilities. Information leakage. Username harvesting. Command injection. SQL injection. Blind SQL injection. Cross-Site Scripting (XSS). Cross-Site Request Forgery. Methods to decompile client-side code. Flash. Java. Explore malicious applets and objects. Discovery vulnerabilities in Web application through their client components.Understand methods for attacking Web services. Understand methods for testing Web 2.0 and AJAX based sites. AJAX and Web services. The attacker's perspective on Python and PHP. The ability to extend the tools we are using.

Exploiting

internal networks. Explore attack frameworks. AttackAPI. BeEF. XSS-Proxy Walk through an entire attack scenario. Exploit the various vulnerabilities discovered. Leverage the attacks to gain access to the system. Learn how to pivot our attacks through a Web application. Understand methods of interacting with a server through SQL injection. Exploit applications to steal cookies. Execute commands through Web application vulnerabilities

How You Will Learn

The course is delivered online over 12 weeks. Lectures are delivered one evening per week (streamed live from ITB) and are usually 3 hours long – they are recorded for playback. In addition you will need to spend about 3 hours per week on project work thought this may vary per student. During the course you will assessed based on two projects and the production of a written report in the subject matter.

What Award You Will Receive

The course is worth 10 ECTS credits at Level 8 on the NFQ. On successful completion you will be awarded a ***Certificate in Application Security – Penetration Testing***. Completion of the course entitles you to 250 Continuing Professional Development points with the Irish Computer Society.

It also completes part of the requirements to be awarded the BSc in Cyber Security from IT Blanchardstown under the Cybersecurity Skills Initiative. The BSc Degree course is mapped to the EU e-Competence Framework and will allow you on successful completion of the whole degree course, to be designated as a Certified IT Security Specialist.

What's in it for Companies

These accreditations ensure employees are qualified to properly configure your cloud servers and secure your data. Coupled with the proper amount of experience, certified employees can serve as a crucial resource towards helping your company defend against a data breach.

What are the Entry Requirements

Candidates should have at least a Level 7 NFQ qualification or alternatively may apply under a non-standard entry process which recognises their prior experiential learning and experience.

What does it cost?

The cost after applying the grant from Skillnet Ireland is €400.

How do I Apply

You must complete the online application form at this link
https://goo.gl/forms/PBayjA6Q1C7HLhKo1

Further Information

For further information and to enquire about payment options please email csi@ictskillnet.ie

Cybersecurity Skills Initiative (CSI)

Technology Ireland ICT Skillnet is co-funded by Skillnet Ireland and member companies. Skillnet Ireland is funded from the National Training Fund through the Department of Education and Skills.

An Roinn Oideachais agus Scileanna
Department of Education and Skills

Skillnet IRELAND