Overview of OWASP Top 10 Vulnerabilities

Course Summary

Description

The objective of this course is to go over the most common and critical vulnerabilities, as described in the *Open Web Application Security Project (OWASP) Top Ten* list. The *OWASP Top Ten* list represents a broad consensus regarding what are the most critical web application security flaws.

The course will include explanations and demonstrations of the vulnerabilities and their causes, as well as discuss ways to securely avoid each of these vulnerabilities.

The course is rich in live demos and code examples, and the selection of programming languages, operating systems, frameworks, and technologies can be customized according to a client's needs.

Objectives
By the end of this course, students will be able to:

- Understand the risks imposed to Web applications
- Learn about common developer bugs and how to avoid them
- Identify weaknesses in web applications
- Learn to develop web applications with security in mind

Topics

- A1-Injection
- A2-Broken Authentication and Session Management
- A3-Cross-Site Scripting (XSS)
- A4-Insecure Direct Object References
- A5-Security Misconfiguration
- A6-Sensitive Data Exposure
- A7-Missing Function Level Access Control
- A8-Cross-Site Request Forgery (CSRF)
- A9-Using Components with Known Vulnerabilities
- A10-Unvalidated Redirects and Forwards

Audience

Experienced web application developers

Prerequisites

There are no prerequisites for this course**.**

Duration

One day

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically