AppSec for Developers

2 DAY CLASS

SPECIALIST TRACK

Covers latest industry standards such as OWASP Top 10 with practical demonstrations of vulnerabilities complemented with Hands-on Lab practice

Insight into the latest security vulnerabilities (such as Host Header Injection, XML Entity Injection,Web-Services and API Security, Deserialization Vulnerabilities)

Thorough guidance on the best security practices (Introduction to various Security Frameworks and tools and techniques for Secure Development)

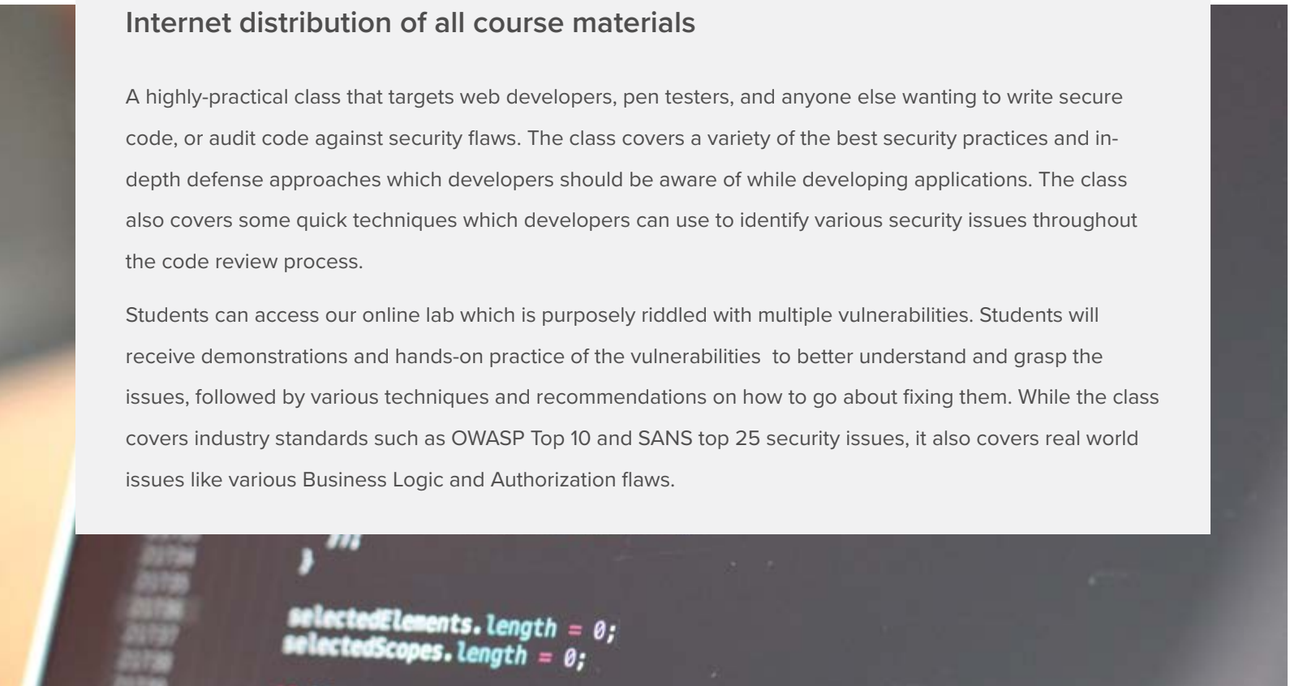
References to real world analogy for each vulnerability (Understand and appreciate why Facebook would pay $33,000 for XML Entity Injection Vulnerability?)

Online Lab available for practicing during and after the course (2 Days)

Internet distribution of all course materials

A highly-practical class that targets web developers, pen testers, and anyone else wanting to write secure code, or audit code against security flaws. The class covers a variety of the best security practices and in-depth defense approaches which developers should be aware of while developing applications. The class also covers some quick techniques which developers can use to identify various security issues throughout the code review process.

Students can access our online lab which is purposely riddled with multiple vulnerabilities. Students will receive demonstrations and hands-on practice of the vulnerabilities to better understand and grasp the issues, followed by various techniques and recommendations on how to go about fixing them. While the class covers industry standards such as OWASP Top 10 and SANS top 25 security issues, it also covers real world issues like various Business Logic and Authorization flaws.



WHO SHOULD TAKE THIS CLASS?

This training is ideal for: Software/Web developers, PL/SQL developers, Penetration Testers, Security Auditors, Administrators, DBAs and Security Managers.

NOT SO SECURE
A Claranet Group Company

Security testing (Pen Testing) as an activity tends to capture security vulnerabilities at the end of the SDLC and is often too late to be able to influence fundamental changes in the way code is written.

We wrote this class because of the increasing need for developers to code in a secure manner. It is critical to introduce security as a quality component into the development cycle. This class aims at educating developers about various security vulnerabilities through hands-on practice using our purposely developed insecure web application which is built on Microsoft .NET platform. Throughout this class developers will be able to get on the same page with security professionals, understand their language, learn how to fix or mitigate vulnerabilities learnt during the class and also get introduced to some real world breaches For ex: The Equifax breach in September 2017 and application vulnerabilities from popular websites like Facebook, Google, Instagram, Paypal etc.

The techniques discussed in this class are mainly focused on .NET and JAVA technologies owing to their huge adoption in various enterprises in building web applications. However, the approach is generic and developers from other language backgrounds can easily grasp and implement the knowledge learnt in within their own environments.

DAY 1

Module 1.
Application Security Basics

Module 2.
Understanding HTTP protocol

Module 3.
Security Misconfigurations

Module 4.
Insufficient Logging and Monitoring

Module 5.
Authentication Flaws

Module 6.
Authorization Bypass

Module 7.
Cross Site Scripting (XSS)

DAY 2

Module 8.
Cross Site Request Forgery (CSRF)

Module 9.
SQL Injection

Module 10.
XML External Entity (XXE) Attacks

Module 11.
Insecure File Uploads

Module 12.
Deserialization Vulnerabilities

Module 13.
Client Side Security

Module 14.
Source Code Review