Check Point
SOFTWARE TECHNOLOGIES LTD.

AppSec for Developers

2 days class

Penetration testing (security testing) as an activity tends to capture security vulnerabilities at the end of the SDLC and then it is often too late to influence fundamental changes in the way the code is written.
This class has being written due to 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 intentionally developed insecure web application 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 acquainted with some real-world breaches, for example, "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 within their own environments.

- **Covers industry standards such as OWASP top 10 with practical demonstration of vulnerabilities complemented with hands-on lab practice.**
- **Provides insights into the latest security vulnerabilities (such as host header injection, XML external entity injection,attacks on JWT tokens,known plaintext attacks, deserialization vulnerabilities).**
- **Offers thorough guidance on best security practices (Introduction to various security frameworks and tools and techniques for secure application development).**
- **Makes real-world analogies for each vulnerability explained (Understand and appreciate why Facebook would pay $33,000 for XML Entity Injection vulnerability?).**
- **Provides online labs for hands-on practice during and after the course (2 Days)**
- **Course material shared online.**

NOT SO SECURE
A Claranet Group Company

The class is 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 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 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 various real world issues such as the business logic and authorization flaws.

PREREQUISITES

The only requirement for this class is that you bring your own laptop with the latest version of Java (JDK) installed. Attendees will be provided with access to our online lab which has been built on the latest .NET ASPX framework and all the tools and materials required during the class.

CLASS CONTENT

The following topics will be covered:
- Application Security Basics
- Understanding the HTTP Protocol
- Security Misconfigurations
- nsufficient Logging and Monitoring
- Authentication Flaws
- Authorization Bypass Techniques
- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF)
- Server Side Request Forgery(SSRF)
- SQL Injection
- XML External Entity (XXE) Attacks
- Unrestricted File Uploads
- Deserialization Vulnerabilities
- Client-Side Security Concerns
- Source Code Review
- DevSecOps

WHO SHOULD TAKE THIS CLASS

Software/Web Developers, PL/SQL Developers, Penetration Testers, Security Auditors, Administrators, DBAs and Security Managers.
Prior pen-test experience is not mandatory, however, some knowledge of cloud services and a familiarity with common command line commands will be beneficial.