NOT SO SECURE
A Claranet Group Company

claranet cyber security

Application Security for Developers

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 been written due to the increasing need for developers to code in a secure manner as it is critical to introduce security as a quality component into the development cycle. 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 get acquainted with some real-world breaches, for example, "The Equifax" breach in September 2017. Various bug bounty case studies from popular websites like Facebook, Google, Shopify, Paypal, Twitter etc will be discussed explaining the financial repercussions of application security vulnerabilities like SSRF, XXE,SQL Injection, Authentication issues etc...

The techniques discussed in this class are mainly focused on .NET,Java and NodeJS 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 learned within their own environments.

Course Objectives

- Covers industry standards such as OWASP top 10 with a 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)

Audience Skill Level

Intermediate

Class Outline

Day 1

- Application Security Basics
- Understanding the HTTP Protocol
- Security Misconfigurations
- Insufficient Logging and Monitoring
- Authentication Flaws
- Authorization Bypass Techniques
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery Scripting

Day 2

- 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

Class Takeaway

- Understand OWASP Top 10 2017 with practical demonstrations and deeper insight.
- Understand the financial repercussions of different vulnerabilities.
- Get on the same page with the security team while discussing vulnerabilities.
- Identify and Fix security vulnerabilities much earlier in the SDLC process saving time and efforts.

Who Should Attend

This class is ideal for Web/API developers who work day-in-day out building full-stack web applications or web APIs. Anyone who is looking to develop a skill-set into web application security and identify web application flaws can also benefit from this course.

Student Requirements

Students need to have a basic understanding of how web applications work with an added advantage for those who currently develop web applications. This training is a programming language agnostic.

What Students Should Bring

A Laptop with minimum 4 GB RAM and 1 GB of extra space. Currently the tools provided by us support only Windows and MacOS operating systems.

What Students Receive

Apart from the various tools and content around the training Students will also be provided with a 7-day lab access where they can practice all the exercises/demos shown during the training.

For more information contact
+44 1223 653193
contact@notsosecure.com