QAAPPSEC: Application Security for Developers 2 Days

2-Day hands-on training covering the most common application security vulnerabilities and how to build secure applications that avoid these issues.

Finding security vulnerabilities at the end of the SDLC is often too late to influence fundamental changes in the way the code is written, and many security issues could be avoided from the outset.

This class has been written by developers turned pentesters who can help developers to code in a secure manner and introduce security into the development cycle.

Throughout this class, developers will be able to get on the same page with security professionals, understand how exploitable vulnerabilities are created in code, learn how to fix or mitigate vulnerabilities and get acquainted with the root causes behind some real-world breaches. 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 generic and developers from any language background can easily grasp and implement the knowledge learned within their own environments. In the class, .NET, Java and NodeJS are used in the workshop examples as this range provide lessons that can be used in a wide range of applications.

Students will also participate in a 'capture the flag' exercise where they'll be challenged to identify vulnerabilities in code snippets derived from real-world applications.

Delegate 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.

Delegates Should Bring

A Laptop with minimum 4 GB RAM and 1 GB of extra space.

Audience Skill Level

Intermediate

Course Objectives

- Offers thorough guidance on best security practices for secure application development (Introduction to various security frameworks and tools and techniques).
- Covers industry standards such as OWASP top 10 application vulnerabilities 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, deserialization vulnerabilities).
- Uses real-world stories for each vulnerability explained (Understand and appreciate why Facebook would pay $33,000 to the person who found a XML Entity Injection vulnerability?).
- Provides online labs for hands-on practice during and after the course (7 Days)

Delegates 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.

Who Should Attend

This class is ideal for front end and back end Web/API developers who work day-in-day out building full-stack web applications or web APIs. This course will however benefit anyone who is looking to develop a skill-set into web application security and identify web application flaws.

NotSoSecure part of claranet cyber security

For more information:

UK: +44 (0)1223 653 193
US: +1 (628)200-3053/3052
Email: contact@notsosecure.com
Visit: notsosecure.com

QAAPPSEC: Application Security for Developers 2 Days *Continued*

Course Outline

- 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
- 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

Course Takeaway

- Learn to code more securely and build more secure applications.
- Identify and fix security vulnerabilities much earlier in the SDLC process saving time and effort.
- Understand OWASP Top 10 common application vulnerabilities with practical demonstrations and deeper insight.
- Understand the financial and wider repercussions of different vulnerabilities.
- Get on the same page with the security team while discussing vulnerabilities.

NotSoSecure part of claranet cyber security

For more information:
UK: +44 (0)1223 653 193
US: +1 (628)200-3053/3052
Email: contact@notsosecure.com
Visit: notsosecure.com