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
- Insufficient 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

Prior pen-test experience is not mandatory, however, some knowledge of cloud services and a familiarity with common command line commands will be beneficial.