NOT SO SECURE
A Claranet Group Company

claranet cyber security

AppSecOps

Application Security testing (Also known as whitebox 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. This class is geared towards:

- **Understanding what application security vulnerabilities are and their trends**
- **Gain an insight into their impact through practical demonstrations**
- **How to fix/avoid them by discussing various strategies, best practices, code snippets and tools (Hackers/ application security tester's view)**
- **How to inject Security into your DevOps pipeline to automate security and develop a DevSecOps pipeline**

If you are a developer who requires mitigation strategies or fails to understand issues like Cross-Site Scripting, XML, External Entity attacks, Deserialization issues, Content-Security Policy and many more application security vulnerabilities and their remediation then this class is for you!

If you are Manager responsible for handling a development team and would like to give a good dose of security knowledge so that you can avoid application security bugs in your code, then you are at the right place!

If you are a DevOps engineer wondering how to automate security into your pipeline, then this course will teach you on how to metamorphose your DevOps to DevSecOps. If you would like to avoid breaches like that of Equifax in September 2017, then sign up now!

Class Outline

This class covers the following modules:

Day 1

- Application Security Basics
- Understanding HTTP protocol
- Security Misconfigurations
- Insufficient Logging and Monitoring
- Authentication Flaws
- Authorization Bypass
- Cross Site Scripting (XSS)

Day 2

- Cross Site Request Forgery (CSRF)
- Server-Side Request Forgery
- SQL Injection
- XML External Entity (XXE) Attacks
- Insecure File Uploads
- Deserialization Vulnerabilities
- Client-Side Security
- Source Code Review

Day 3

- Introduction and overview of DevOps
- What and Why of DevSecOps?
- Integrating Security in CI/CD
- Vulnerability Management using Archerysec
- Secret Management using Vault, Jenkins and Docker Secrets
- Security in Developer Workstations: Pre-Commit Hooks using Talisman
- Software Composition Analysis using Dependency-Checker
- SAST - Static Application Security Testing using FindSecBugs
- DAST - Dynamic Application Security Testing using ZAP
- Security in Infrastructure as a Code using Clair
- Automated Vulnerability Assessment using OpenVAS
- Compliance as Code using Inspec
- Monitoring and Feedback using Modsecurity WAF
- DevSecOps in AWS
- Challenges in DevSecOps
- DevSecOps Enablers

Who Should Attend

- Any person who wishes to learn about application security vulnerabilities and understand more about their impact
- Developers who create web applications in any language can attend
- Any technical person having a basic knowledge of how web applications work or is responsible for Implementing, managing or protecting web applications
- Any DevOps engineer looking to automate security

You Will be able to

- Obtain a hands-on introduction to application security vulnerabilities like Cross-Site Scripting, SQL Injection, XXE, Authentication & authorization flaws on our purposely built vulnerable web applications to help you understand the vulnerabilities better. Thereby enabling you to defend your organization's website or assets
- Identify application security bugs in code and fix them before deploying it into production
- Identify vulnerable libraries and avoid their usage
- Develop secure web applications so that you don't waste your time later in fixing security issues
- Understand the methodology that can be used to automate and integrate security

What Students Receive

- 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.
- Students will also receive our state-of-the-art DevSecOps Tool-chest VM comprising of all the tools and scripts being discussed in the course.

Prerequisites

The only requirement for this class is that you bring your own laptop with minimum version JDK 8.0 installed with administrator rights and lots of caffeine!

Trainers

Anant Shrivastava is an information security professional with 11+ yrs of corporate experience with expertise in Network, Mobile, Application and Linux Security. He is Regional Director - Asia Pacific for NotSoSecure Global Services. He has trained ~800 delegates at various conferences (Black Hat (USA, ASIA, EU), Nullcon, c0c0n, Ruxcon to name a few). He has also been a speaker at various conferences such as Nullcon, c0c0n, Rootconf. Anant also leads Open Source project Android Tamer (www.androidtamer.com) and CodeVigilant (www.codevigilant.com). He is active in various open security communities like OWASP, null, G4H. He is chapter leader for local null community chapter and is an avid open source contributor. He is a contributing author for OWASP Web Testing Guide v4.0 and a reviewer for Mobile Testing Guide and Mobile ASVS standard documents by OWASP. His work can be found at anantshri.info

Rohit Salecha is a technology enthusiast who loves to dive deep into the world of technology. His current expertise revolves around finding interesting bugs in Web Applications and also loves doing Android and iOS app security assessments. Through his learning, he also loves to deliver talks and training on various subjects related to Web and Mobile Applications. He delivered training on Basic Web Hacking and Basic Infrastructure Hacking at Blackhat USA 2017 and 2018 to more than 80 students. He is also passionate about architecting IT solutions with the focus on Information security.

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