AppSecOps 3 Days

A Holistic Approach to Application Security

A 3-Day practical hands-on training to understand application security vulnerabilities and how to automate the defenses for the same.

AppSecOps is a 3-Day practical hands-on training to understand application security vulnerabilities and how to automate the defenses for the same. Provides insights into the latest security vulnerabilities such as host header injection, XML external entity injection, attacks on JWT tokens, SSRF Attacks, deserialization vulnerabilities etc... Attendees will learn how to defend themselves against such attacks and learn how to integrate the defenses by creating a DevSecOps environment.

The DevSecOps environment will be shown implemented by injecting security into Continuous Integration (CI), Continuous Delivery (CD), Continuous Monitoring (CM) and Infrastructure as Code (IaC) . A Short preview of the DevSecOps portion of the course is available for viewing here https://www.youtube.com/watch?v=_iGCZ4NPDqY

As part of the class attendees will be provided access to an online lab for 7 days where they can practice their application security skills and be provided with our custom developed DevSecOps-Lab VM containing all the tools and code which are used for demonstrating the DevSecOps pipeline.

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 skillset into web application security and identify web application flaws can also benefit from this course.

DevOps engineers, security and solutions architects, system administrators and anybody who is a fan of automation will also strongly benefit from this course as it'll give them a holistic approach towards application security.

Delegate Requirements

Anybody with a background in IT or related to software development whether a developer or a manager can attend this course to get an insight about Web Application Security vulnerabilities, DevOps and DevSecOps

Delegates Receive

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

They shall also be provided with our custom built DevSecOps-Lab VM containing all the code, scripts and tools that are used for building the entire DevSecOps pipeline.

Course 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.
- Understand how to tackle security issues in a fast-moving DevOps environment
- Identify tools/solutions and develop processes to create a secure by default infrastructure
- Utilize the integration scripts and tools provided in the DevSecOps Lab to create your own DevSecOps pipeline

Delegates Should Bring

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

NotSoSecure part of
claranet cyber security

AppSecOps 3 Days (Continued)

A Holistic Approach to Application Security

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 (7 Days)
- Create a security culture/mindset amongst the already integrated “DevOps” team.
- Find and fix security bugs as early in SDLC as possible i.e. understand the “Shift Left” methodology.
- The culture promotes the philosophy “Security is everyone’s problem”.
- Integrate all security software centrally and utilize the results more effectively.
- Measure and shrink the attack surface.

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

Introduction to DevOps

Introduction to DevSecOps

Continuous Integration

Continuous Delivery

Infrastructure As Code

Continuous Monitoring

DevSecOps in AWS

DevSecOps Challenges and Enablers