## Description

The Professionally Evil Application Security (PEAS) course is designed to teach developers, IT professionals, and penetration testers of all skill levels. This course focuses on the techniques used to assess and exploit applications; including web and mobile applications, APIs, and HTTP-based systems. We combine these techniques with explanations of the risks exposed and defenses required to improve the security of your organizations.

The course uses a large number of hands-on exercises to reinforce the techniques and understanding an attendee will gain so that they benefit on the very first day back to work. The course focuses on manual techniques for discovery and exploitation while teaching an industry-standard methodology of reconnaissance, mapping, discovery, and exploitation. This methodology provides a comprehensive standard for assessing applications and APIs.

Students use the SamuraiWTF project environment to learn both attacks and defenses while in class. This environment provides realistic targets and tools which enables the attendees to understand how the techniques taught are used in the real world.

Completing this course meets all of the requirements for developer training as part of PCI-DSS.

## Agenda

- Introduction
- Standards & Guidelines
    - PCI
    - HIPAA
    - OWASP
    - Other
- Preparation
    - How the web works
    - Tools used in assessing application
    - Test Lab & Class Targets
- Testing Methodology Overview
    - Reconnaissance
        - Recon Overview
        - Recon Tools
    - Mapping

        - Mapping Overview
        - Mapping Tools
        - Mapping walkthrough of dojo-basic
        - Critical Skills: Search Mapping Results - what to look for
    - Discovery
        - Discovery Overview
        - Discovery Tools
    - Exploitation
        - Exploitation Overview
        - Exploitation Tools
- Server-Side Vulnerabilities
    - Authentication and Session Management Issues
    - Access Control Flaws
    - Sensitive Data Exposure
    - Injection Flaws
        - Command Injection
        - SQL Injection
        - Buffer Overflows
- Fuzzing
    - Tool Set
    - Attack Sources
    - Context Understanding
- Testing Web Services
    - Web Services Overview
    - Tools for testing Web Services
    - Critical Skills: Running Web Services
    - Web Service Vulnerabilities
        - XML External Entity (XXE)
- Client-Side Vulnerabilities
    - Cross-Site Scripting (XSS)
    - Open Redirects and Forwards
    - Cross-Site Request Forgery (CSRF)
- Logic Flaws
    - Business Logic Issues
    - Race conditions and TOC/TOU issues
- Defenses
    - Logging and Monitoring