Course Outline

OWASP Programming

Course Summary

Description

OWASP.org is a well-known community for securing web applications. They post documents, top-ten security lists, and host major events and conferences. OWASP is recognized worldwide for making invaluable contributions towards keeping both web applications and users safe.

Each year, OWASP publishes top-ten lists of current security vulnerabilities. The lists are a roadmap for common vulnerabilities that developers should be familiar. In this class, you will learn to mitigate the vulnerabilities in the latest list to assure an adequate defense for your applications.

OWASP has expanded their focus beyond web applications to include operating system (API), cloud, and hardware applications. Some of these other domains are reviewed in class.

This course also instructs on how to classify and prioritize vulnerabilities. For this reason, STRIDE, DREAD, and other initiatives are reviewed.

Cryptography is a major component in defending many of the problems OWASP identifies. This class includes an introduction to crypto concepts.

Topics

- Security Concepts
- OWASP - Web
- OWASP - API
- Adversarial Prospective
- OWASP – Cloud

Audience

This course is designed for professional developers.

Prerequisites

Students should have one year of development experience.

Duration

Three days

Course Outline

OWASP Programming

Course Outline

I. Security Concepts
- A. CIA Triad
- B. STRIDE
- C. DREAD
- D. Cryptography
- E. Token authentication
- F. Oauth2

II. OWASP - Web
- A. Injection
- B. Cross-Site Scripting (XSS)
- C. Broken Authentication and Session Management
- D. Insecure Direct Object References
- E. Cross-Site Request Forgery (CSRF)
- F. Security Misconfiguration
- G. Insecure Cryptographic Storage
- H. Failure to Restrict URL Access
- I. Insufficient Transport Layer Protection
- J. Unvalidated Redirects and Forwards

III. OWASP - API
- A. OWASP - API
- B. Broken object level authorization
- C. Broken user authentication
- D. Excessive data exposure
- E. Lack of resources and rate limiting
- F. Broken function level authorization

IV. Adversarial Prospective
- A. Phishing attacks
- B. Injection attacks
- C. Zero-day attacks
- D. Heartbeat attacks
- E. Birthday attacks
- F. Rowhammer attacks
- G. Threat intelligence

V. OWASP – Cloud
- A. Accountability and data ownership
- B. User identity
- C. Regulatory compliance
- D. Business continuity and resiliency
- E. User privacy and secondary usage of data