Developer Security Awareness Training 2024

Survey of Application Security in 2024 (AAA-101)

Overview

Building modern applications requires an understanding of security exploits, vulnerabilities, and defensive strategies. This course builds upon a developer's knowledge of software security by providing a security refresher course so students gain awareness of current security issues as well as re-visiting some fundamental issues in secure development. This is achieved through discussing and raising organizational awareness concerning latest security issues surrounding Authentication, Authorization, and Auditing (AAA) as well as Confidentiality, Integrity, and Availability (CIA). In the course, we also discuss how to apply these basic security principles to development. This training will help developers to identify flaws in running applications, as well as think about approaches used to fix some common flaws.

Requirements

Students will need a computer with a browser and wireless or internet connection.

Approach

Redpoint Security uses years of development experience to tailor training courses to developers. Each course features custom-developed intentionally-vulnerable applications used to demonstrate the exploitation and mitigation of vulnerabilities. This course takes a hands-on approach and requires developers to interact with vulnerable applications to better understand the topics.

Structure of Course

For the two-hour course, Redpoint Security will customize content through discussion with AppSec engineers or dev team leads to ensure exercises are relevant to technologies used by organizations as well as looking to raise awareness of common vulnerabilities found by prior application security reviews (We will work through NDAs to facilitate this level of detail on customizing the course content). The one-hour course covers the same topics but in a general approach regarding current issues in application security. The basic structure of the course is as follows:

- Training Introduction (5 minutes) – Overview of the importance of security in application development.
- Brief introduction to the key concepts: Authentication, Authorization, Auditing, Confidentiality, Integrity, and Availability. (10 minutes)
- Case Study 1: Secure Login System (30 minutes with organization-specific customization) (15 minutes general course) – applying AAA to the most basic functions of an application
    - Authentication: Discuss the creation of a secure login system.
    - Authorization: How to ensure users access only what they're permitted.
    - Auditing: Logging login attempts and access control decisions.

    - Wrap-up with a discussion on how Confidentiality, Integrity, and Availability relate to the login system, tease next discussion
- Case Study 2: Data Protection in a Web Application (30 minutes with organization-specific customization) (15 minutes general course)
    - Confidentiality: Encrypting sensitive data and protecting user privacy.
    - Integrity: Ensuring data hasn't been tampered with.
    - Availability: Keeping the service up and preventing unauthorized access during maintenance.
- Interactive Exercise: Threat Modeling (25 minutes with organization-specific customization) (10 minutes general course) – Divide participants into small groups.
    - Present a hypothetical or special component or function of the organization's application.
    - Have each group identify potential threats related to Authentication, Authorization, Auditing, Confidentiality, Integrity, and Availability.
    - Groups present their findings.
- Q&A and Conclusion (5-10 minutes)
    - Review of key points.
    - Address any remaining questions.
    - Share additional resources.

Outline of Covered Topics

- **Authentication**
    - Definition and importance.
    - Best practices (e.g., strong passwords, multi-factor authentication).
    - Common pitfalls and attacks (e.g., brute force, phishing).
- **Authorization**
    - Difference between Authentication and Authorization.
    - Role-based access control (RBAC) and least privilege.
    - Real-world examples and common vulnerabilities.
- **Auditing**
    - Importance of logging and monitoring.
    - What to audit: authentication attempts, data access, configuration changes.
    - Tools and techniques for effective auditing.
- **Confidentiality**
    - Encryption in transit and at rest.
    - Data masking and anonymization.
    - Protecting sensitive information in code and storage.
- **Integrity**
    - Ensuring data is accurate and untampered.
    - Hashing and checksums.
    - Common threats like data corruption or unauthorized alterations.
- **Availability**
    - Ensuring systems are up and running.
    - DOS – whether by malicious attacker or insider mistakes

Training Costs

Select option	Item Description		Price/student
☐ Recommended	2-hour course with customization		$200

Select option	Item Description		Price/student
☐	1-hour course, no customization		$100