Application Security and Development (STIG)

Course Summary

Description

This lab intensive, hands on application security training course essential for developers, designers, architects, QA, Testing, and other personnel who need to deliver secure applications within the DoD. In addition to teaching basic programming skills, this course digs deep into sound processes and practices that apply to the entire software development lifecycle. In this course, students thoroughly examine best practices for defensively coding applications, including XML processing and web services. Students will repeatedly attack and then defend various assets associated with a fully functional application. This hands on approach drives home the mechanics of how to secure applications in the most practical of terms.

Objectives

At the end of this course, students will be able to:

- Understand potential sources for untrusted data
- Understand the consequences for not properly handling untrusted data such as denial of service, cross- site scripting, and injections
- Be able to test web applications with various attack techniques to determine the existence of and effectiveness of layered defenses
- Prevent and defend the many potential vulnerabilities associated with untrusted data
- Understand the vulnerabilities of associated with authentication and authorization
- Be able to detect, attack, and implement defenses for authentication and authorization functionality and services
- Understand the dangers and mechanisms behind Cross- Site
- Scripting (XSS) and Injection attacks
- Be able to detect, attack, and implement defenses against XSS and Injection attacks
- Understand the concepts and terminology behind defensive, secure, coding
- Understand the use of Threat Modeling as a tool in identifying software vulnerabilities based on realistic threats against meaningful assets
- Perform both static code reviews and dynamic application testing to uncover vulnerabilities in Java- based web applications
- Design and develop strong, robust authentication and authorization implementations within the context of application framework
- Understand the fundamentals of Cryptography and Encryption and where they fit in the overall security picture
- Understand the fundamentals of XML Digital Signature and XML Encryption as well as how they are used within the webservices arena
- Be able to detect, attack, and implement defenses for XMLbased services and functionality
- Understand techniques and measures that can used to harden web and application servers as well as other components in your infrastructure
- Understand and implement the processes and measures associated with the Secure Software Development (SSD)
- Acquire the skills, tools, and best practices for design and code reviews as well as testing initiatives
- Understand the basics of security testing and planning
- Work through a comprehensive testing plan for recognized vulnerabilities and weaknesses

Topics

- Foundation
- Top Security Vulnerabilities
- Additional Measures
- Defending XML Processing
- Secure Software Development (SSD)
- Application Development
- Application Security and Development Checklist

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

Application Security and Development (STIG)

Course Summary (cont'd)

Audience

This is an intermediate - level programming course, designed for developers who wish to get up and running on developing well-defended software applications. This course may be customized to suit your team's unique objectives.

Prerequisites

Familiarity with a programming language is required and real world programming experience is highly recommended. Ideally students should have approximately 6 months to a year of working knowledge.

Duration

Four days

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

Application Security and Development (STIG)

Course Outline

I. Foundation

A. Misconceptions
1. Thriving Industry of Identify Theft
2. Dishonor Roll of Data Breaches
3. TJX: Anatomy of a Disaster
4. Heartland: What? Again?

B. Security Concepts
1. Terminology and Players
2. Assets, Threats, and Attacks
3. OWASP
4. CWE/SANS Top 25 Programming Errors

C. DISA's Security Technical Implementation Guides (STIGS)
1. Purpose
2. Process
3. Areas Covered
4. Checklists
5. Scripts (SRRs)
6. Resources

D. Defensive Coding Principles

E. Reality
1. Recent, Relevant Incidents
2. Find Security Defects In Web Application

II. Top Security Vulnerabilities

A. Unvalidated Input
1. Description With Working Example
2. Defenses
3. Identifying Trust Boundaries
4. Qualifying Untrusted Data
5. Implementing An Effect, Layered Defense
6. Designing An Appropriate Response
7. Testing Defenses And Responses

B. Overview Of Regular Expressions
1. Regular Expressions
2. Working with Regular Expressions in Java

C. Broken Access Control
1. Description With Working Example
2. Defenses
3. Authorization Security Overview
4. Defending Special Privileges Such As Administrative Functions
5. Application Authorization Best Practices

D. Broken Authentication And Session Management
1. Description With Working Example
2. Defenses
3. Multi-Layered Defenses Of Authentication Services
4. Password Management Strategies
5. Password Handling With Hashing Using JCE/JCA
6. Mitigating Password Caching
7. Testing Defenses And Responses For Weaknesses
8. Alternative Authentication Mechanisms
9. Best Practices For Session Management in J2EE
10. Defending Session Hijacking Attacks
11. Best Practices For Single Sign-On (SSO)

E. Cross Site Scripting (XSS) Flaws
1. Description With Working Example
2. Defenses
3. Character Encoding
4. Complications
5. Blacklisting
6. Whitelisting
7. HTML/XML Entity Encoding
8. Trust Boundary Definition
9. Implementing An Effective Layered Defense
10. Designing An Appropriate Response
11. Cross-Site Request Forgeries (CSRF)
12. Understanding CSRF
13. Defending Against CSRF
14. Output Encoding – Why
15. Output Encoding – How
16. Output Encoding – Best Practices

F. Injection Flaws
1. Description With Working Example
2. Defenses
3. Qualifying Untrusted Data
4. JDBC, Prepared Statements, and Stored Procedures
5. Hibernate Best Practices
6. XML Best Practices
7. Third Party API's
8. Implementing An Effective Layered Defense
9. Designing An Appropriate Response

G. Error Handling And Information Leakage
1. Description With Working Example
2. Defenses
3. J2EE Application Exception Handling

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

Application Security and Development (STIG)

Course Outline (cont'd)

4. Error Response Best Practices
5. Error, Auditing, And Logging Content Management
6. Error, Auditing, And Logging Service Management
7. Best Practices For Supporting Web Attack Forensics

H. Insecure Storage
1. Description With WorkingExample
2. Defenses
3. Data Leakage
4. Risk Minimization
5. Cryptography Overview
6. JCS/JCE
7. Data Encryption
8. Partial/Complete
9. Property/Deployment/Configuration Files

I. Insecure Management Of Configuration
1. Description With Working Example
2. Defenses
3. System Hardening
4. Server Configuration "Gotchas!"
5. Hardening Software Installation

J. Direct Object Access
1. Description With Working Example
2. Defenses
3. Java Byte Code Verifier
4. XML/DTD/Schema/XSLT Best Practices

K. Spoofing
1. Description With Working Example
2. Defenses
3. Protecting Your Clients
4. Defending Against Cross Site Request Forgeries
5. Phishing Defenses

III. Additional Measures

A. Cryptography Overview
1. Cryptography defined
2. Strong Encryption
3. Ciphers and algorithms
4. Message digests
5. Types of keys
6. Key management
7. Certificate management
8. Encryption/Decryption

B. Auditing
1. Auditing Mechanics and Best Practices

C. Third Party Software

D. Mobile Code

IV. Defending XML Processing

A. Defending XML
1. Understanding Common Attacks And How To Defend
2. Operating In Safe Mode
3. Using Standards-Based Security
4. XML-Aware Security
5. Infrastructure
6. JAXP Safe Mode

B. Defending Web Services
1. Security Exposures
2. Transport-Level Security
3. Message-Level Security
4. WS-Security
5. Attacks And Defenses

C. Defending Ajax
1. Ajax Security Exposures
2. Attack Surface Changes
3. Injection Threats And Concerns
4. Effective Defenses And Practices

V. Secure Software Development (SSD)

A. SSD Process Overview

B. Asset, Boundary, and Vulnerability Identification

C. Threat Modeling and Analysis

D. Process, Design, and Code Reviews

E. Applying Processes and Practices

F. Configuration Specification and Compliance

G. Testing as Lifecycle Process

H. Testing Planning and Documentation

I. Testing Tools And Processes
1. Principles
2. Reviews
3. Testing
4. Tools

J. Static and Dynamic Analysis

K. Testing Practices
1. Authentication Testing
2. Data Validation Testing

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

Application Security and Development (STIG)

Course Outline (cont'd)

3. Denial Of Service Testing
4. Web Services Testing
5. Ajax Testing

VI. Application Deployment

A. Documentation
B. Best Practices
C. Update and Patch Management
D. Incident Response
E. Auditing

VII. Application Security and Development Checklist

A. Checklist Overview, Conventions, and Best Practices
B. Generic Application Checks and Procedures
C. .Net Framework Checks and Procedures (Optional)
D. Web/Java Checks and Procedures (Optional)

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically