Application Security & Development: STIG Overview - TT8805

Learn to design, build, and secure applications using proven STIG-based best practices.

Duration: 3 Days
Skill Level: Intermediate
Available Format: Instructor-Led Online; Instructor-Led, Onsite In Person ; On Public Schedule

What You'll Learn

Overview

The course is a comprehensive four-day course that delves into the realm of Information Assurance, empowering you to enhance your cybersecurity skills, understand the essentials of STIGs, and discover cutting-edge web application security practices. This immersive experience is tailored for IT professionals, developers, project teams, technical leads, project managers, testing/QA personnel, and other key stakeholders who seek to expand their knowledge and expertise in the evolving cybersecurity landscape. The course focuses on the intricacies of best practices for design, implementation, and deployment, inspired by the diverse and powerful STIGs, ultimately helping participants become more proficient in application security.

The first half of the course covers the foundations of DISA's Security Technical Implementation Guides (STIGs) and learn the ethical approach to bug hunting, while exploring the language of cybersecurity and dissecting real-life case studies. Our expert instructors will guide you through the importance of respecting privacy, working with bug bounty programs, and avoiding common mistakes in the field.

The remainder of the course delves into the core principles of information security and application protection, as you learn how to identify and mitigate authentication failures, SQL injections, and cryptographic vulnerabilities. You'll gain experience with STIG walkthroughs and discover the crucial steps for securing web applications.

Throughout the course, you'll also explore the fundamentals of application security and development including checklists. You'll learn from recent incidents and acquire actionable strategies to strengthen your project teams and IT organizations.

Objectives

Working in an interactive learning environment, guided by our application security expert, you'll explore:

- the concepts and terminology behind defensive coding
- the spectrum of threats and attacks that take place against software applications in today's world
- the effectiveness of static code and dynamic application scanners in uncovering vulnerabilities in applications
- the vulnerabilities of programming languages as well as how to harden installations
- the basics of Cryptography and Encryption and where they fit in the overall security picture
- the requirements and best practices for program management as specified in the STIGS

Audience

This course is designed for:

- **IT professionals** who manage or secure systems and networks
- **Developers and engineers** who build or maintain web applications
- **Project managers and team leads** overseeing secure software projects
- **QA and testing personnel** verifying application security and performance
- **Technical decision-makers** who want to understand STIGs and application security principles

Pre-Requisites

Before attending this course, participants should have:

- **Basic cybersecurity awareness** — Know fundamental information security terms and concepts.
- **Familiarity with web applications** — Understand how websites and web apps are structured and function.

- **Basic networking knowledge** — Know common web/network protocols like HTTP, HTTPS, and TCP/IP.
- **Some programming exposure** — Experience with or understanding of programming languages such as JavaScript, Python, Java, or C# (helpful but **not required**).
- **General IT background** — Have a basic grasp of operating systems, databases, and web servers.

Agenda

Session: STIG Foundation

Lesson: DISA's Security Technical Implementation Guides (STIGs)

- The motivations behind STIGs
- Requirements that the various software development roles must meet
- Implementing STIG requirements and guidelines
- Lab: Exploring the STIG Viewer

Lesson: Why Hunt Bugs?

- The Language of Cybersecurity
- The Changing Cybersecurity Landscape
- The Human Perimeter
- Interpreting the 2021 Verizon Data Breach Investigation Report
- Starting Point for ALL Security Analysis of Web Applications
- Lab: Intro to Lab Environment
- Lab: Case Study in Failure

Session: Foundation for Securing Web Applications

Lesson: Unvalidated Data

- Applicable STIGs
- Buffer Overflows

- Integer Arithmetic Vulnerabilities
- Defining and Defending Trust Boundaries
- Rigorous., Positive Specifications
- Whitelisting vs Blacklisting
- Challenges: Free-Form Text, Email Addresses, and Uploaded Files
- Lab: Identifying and Defending Trust Boundaries
- Lab: Developer's Security Toolbox
- Lab: STIG Walk-Throughs

Lesson: Identification and Authentication Failures

- Applicable STIGs
- Quality and Protection of Authentication Data
- Proper hashing of passwords
- Handling Passwords on Server Side
- Session Management
- HttpOnly and Security Headers
- Lab: Identifying and Defending Authentication Assets
- Lab: STIG Walk-Throughs

Lesson: Injection

- Applicable STIGs
- Injection Flaws
- SQL Injection Attacks Evolve
- Drill Down on Stored Procedures
- Other Forms of Server-Side Injection
- Minimizing Injection Flaws
- Lab: Identifying and Defending Against SQL Injection
- Client-side Injection: XSS
- Persistent, Reflective, and DOM-Based XSS
- Best Practices for Untrusted Data
- Lab: Identifying and Defending Against XSS
- Lab: STIG Walk-Throughs

Lesson: Security Logging and Monitoring Failures

- Applicable STIGs
- Detecting Threats and Active Attacks
- Best Practices for Determining What to Log
- Safe Logging in Support of Forensics
- Lab: STIG Walk-Throughs

Lesson: Broken Access Control

- Applicable STIGs
- Elevation of Privileges
- Insufficient Flow Control
- Unprotected URL/Resource Access/Forceful Browsing
- Lab: Identifying and Defending Against Unsafe Direct Object References
- Metadata Manipulation (JWTs)
- CORS Misconfiguration Issues
- Cross Site Request Forgeries (CSRF)
- CSRF Defenses
- Lab: Spotlight: Verizon
- Lab: STIG Walk-Throughs

Lesson: Cryptographic Failures

- Applicable STIGs
- Identifying Protection Needs
- Evolving Privacy Considerations
- Options for Protecting Data
- Transport/Message Level Security
- Weak Cryptographic Processing
- Keys and Key Management
- Threats of Quantum Computing
- Steal Now, Crack Later Threat
- Lab: STIG Walk-Throughs

Lesson: Security Misconfiguration

- Applicable STIGs
- System Hardening
- Risks with Internet-Connected Resources (Servers to Cloud)
- Minimalist Configurations
- Application Whitelisting
- Secure Baseline
- Segmentation with Containers and Cloud
- Lab: Configuration Guidance
- Resolution of External References
- Safe XML Processing
- Lab: Identifying and Defending XML Processing

Lesson: Vulnerable and Outdated Components

- Vulnerable Components
- Software Inventory
- Managing Updates: Balancing Risk and Timeliness
- Software Bill of Materials (SBOM)
- AppSec Dissection of Ongoing Microsoft Exchange Exploits
- Lab: Spotlight: Equifax

Lesson: Software and Data Integrity Failures

- Serialization/Deserialization
- Issues with Consuming Vulnerable Software
- Using Trusted Repositories
- CI/CD Pipeline Issues
- Protecting Software Development Resources

Lesson: Server-Side Request Forgery (SSRF)

- Understanding SSRF
- Remote Resource Access Scenarios
- Complexity of Cloud Services

- SSRF Defense in Depth
- Positive Allow Lists

Lesson: Database Security

- Design and Configuration
- Identification and Authentication
- Computing Environment
- Database Auditing
- Boundary Defenses
- Continuity of Service
- Vulnerability and Incident Management
- Lab: STIG Walk-Throughs

Session: Moving Forward

Lesson: Applications: What Next?

- Common Vulnerabilities and Exposures
- Open Web Application Security Project (OWASP)
- OWASP Top Ten Overview
- CERT Secure Coding Standards
- Microsoft Security Response Center
- CWE/SANS Top 25 Most Dangerous SW Errors
- Strength Training: Project Teams/Developers
- Strength Training: IT Organizations

Session: Moving Forward with Application Security

Lesson: Application Security and Development Checklists

- Checklist Overview, Conventions, and Best Practices

- Leveraging Common AppSec Practices and Control
- Actionable Application Security
- Additional Tools for the Toolbox
- Strength Training: Project Teams/Developers
- Strength Training: IT Organizations
- Lab: Recent Incidents

For More Information

Please contact us or call 844-475-4559 toll free for more information about our training services (instructor-led, self-paced or blended), coaching and mentoring services, public course enrollment or questions, partner programs, courseware licensing options and more.