JAV201 - DEFENDING JAVA

Course Learning Objectives

- Identify threats that affect modern java applications and how they work.
- Recognize types of security risks that are inherently mitigated by java.
- Implement defensive coding techniques to manage the security of your java application and its dependencies.

Description

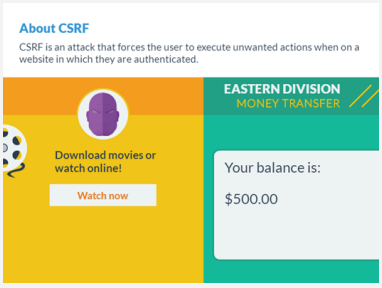
This course will build upon high-level application security concepts and how they relate to the java environment. We will cover various threats and their defenses that are relevant to java applications in SDK 6 through 10, including many common frameworks like java EE / jakarta EE and Spring. The material is intended for junior to mid-level java developers on their way to becoming senior engineers and architects.

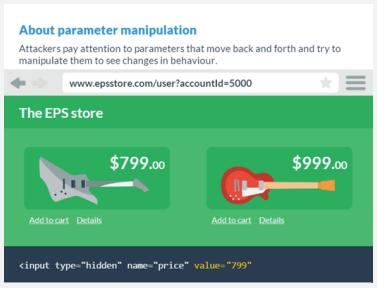
Audience

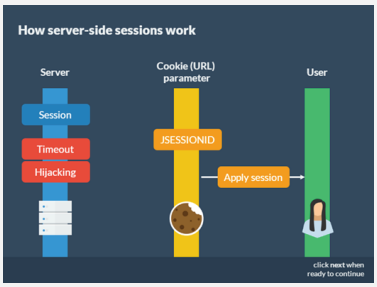
Java Developers
Java Architects

Time Required

Tailored learning - 90 minutes total







JAV201 - DEFENDING JAVA

Course Outline

1. Introduction

- Types of Java
- Application: The sum of all code
- Security benefits of Java
- STRIDE
- Java STRIDE for managing dependencies
- Java upgrade strategy

2. Authentication

- About authentication
- How SAML works
- How OAuth works
- SAML vs OAuth
- Two Factor Authentication
- How account enumeration works
- Account enumeration defense
- Storing passwords
- Attacks on hashed passwords
- Salting
- MessageDigest
- Listing MessageDigest algorithms

3. Authorization

- About authorization
- Attacks against authorization
- Privilege escalation
- Elevation through tampering
- Forcible browsing
- The problem with JAAS
- Apache Shiro
- Annotation-based system
- Shiro authentication
- Configuration
- Shiro – WebFilter
- Role based access control
- Example: Blocking Forced Browsing
- How Shiro works
- Imperative programming
- Aspect Oriented Programming

4. Web defenses

- Java web development
- Cookie handling
- Cookie hijacking
- Cookie hijacking defense
- Server-side sessions
- How server-side sessions work
- Session timeouts
- Session max timeout
- Session max age
- Session fixation – Security risk
- Session fixation – Defense
- Web filters
- Servlet Filters
- Creating a WebFilter
- Cross-Site Request Forgery
- REST endpoints
- Token system
- HTTP request referrers
- CORS
- Prevention through Servlet Filters

5. Input validation

- About input validation
- Types of validation
- Attack types
- SQL Injection
- JDBC and JPA
- About Cross-Site Scripting
- Reflected XSS
- Stored XSS
- XXS defenses
- Parameter manipulation
- Server-side controls
- Deserialization attacks
- Serialization defenses
- Marshalling and unmarshalling
- Memory overflow
- How HTTP response splitting works
- Whitelisting
- Race Conditions
- What are race conditions?
- Race conditions in Java Web Applications
- Race conditions example

6. File handling

- Java file APIs
- Local file inclusion
- Poison Null Byte
- Indirect selection
- Malicious file contents
- Polyglot VM
- File size validations
- Enforcing file size
- File size defense
- File performance
- File access blocking

SecurityCompass

JAV201 - DEFENDING JAVA

Course Outline

7. Cryptography

- JCA file APIs
- Random numbers
- Locations of core cryptography
- Symmetric encryption driver
- Encrypt function
- Decrypt function
- Symmetric encryption test
- Asymmetric encryption driver
- Encrypt function
- Decrypt function
- Asymmetric encryption test
- Benefits of Cipher streams
- Wrapping a stream
- Chained streams

8. Secret management

- Java certificate management
- Diagnosing certificate issues
- Trust stores for certificates
- Key locations
- KeyStore
- Listing aliases
- Certificates
- OpenSSL
- KeyTool
- Generating keys
- Signed code
- Validating code
- Signing JARs
- Timestamped signatures

9. Logging and auditing

- Java logging
- Logging frameworks
- Centralized logs
- Unifying log frameworks
- Logging sensitive data
- Handling sensitive information
- Logging levels
- Logger performance

SecurityCompass