ProTech *"Charting the Course ...*

protechtraining.com

... to Your Success!"

Secure Coding in Java Serialization

Course Summary

Description

Our secure coding training courses help developers establish a security mindset and prevent them from making secure coding errors that lead to deploying vulnerable systems.

The one-day instructor-led Java Serialization course provides developers with practical guidance for securely implementing Java serialization. Serialization is widely used both directly by applications and indirectly by Java subsystems such as RMI (Remote Method Invocation), JMX (Java Management Extension), and JMS (Java Messaging System). Java deserialization is an insecure language feature included in the OWASP Top 10 Application Security Risks – 2017. Deserialization of untrusted streams can result in remote code execution (RCE), denial-of- service (DoS), and a range of other exploits. Applications can be vulnerable to these attacks even when no coding defects are present.

This course explains and demonstrates these attacks while showing developers how to securely code their systems to support Java serialization. Developers will learn how Java serialization/ deserialization works under the covers, how to determine if your systems are vulnerable to Java deserialization exploits, and how to securely implement Java Serialization.

The course consists of lecture (40%), demonstrations (30%), and labs (30%). Participants should come away from the course with a working knowledge of Java Serialization. Moreover, the course encourages programmers to adopt security best practices and develop a security mindset that can help protect software from tomorrow's attacks, not just today's.

Topics

- Implement Java object serialization
- Implement Java object externalization
- Identify serialization security risks
- Exploit deserialization vulnerabilities
- Assign versions to serializable classes
- Implement a customized serialized form
- Use the proper signatures of serialization methods
- Write readObject methods defensively
- Use serialization proxies
- Sign and seal objects
- Mitigate vulnerabilities using serialization filtering in Java 9

Audience

The course is designed primarily for Java SE 8 developers, but some course demonstrations will use Java SE 9 features.

Prerequisites

The course assumes basic Java programming skills but does not assume an in-depth knowledge of software security. Course demos and solutions to exercises are presented using the Eclipse IDE but students are free to use any IDE for reviewing example code and performing exercises.

Duration

One day