Spring Security

Beginner to Guru

Cross-site Scripting Attacks

Samy Cross-site Scripting Worm (XSS)

- On October 4th, 2005 the worm "Samy" was released on MySpace by Samy Kamkar
- The worm would add to users profiles "but most of all, Samy is my hero" and add Samy Kamkar as your friend
- The worm would also replicate itself to your profile
- Within 20 hours the worm had spread to over 20 million profiles
  - Still the fastest spreading virus of all time

Samy Cross-site Scripting Worm (XSS)

- The Samy worm shut down MySpace - the largest social media website at the time
- What happened?
  - MySpace profile pages were highly customizable
  - MySpace failed to protect user input from having Javascript
  - Server accepted, stored, and served user supplied Javascript

More about Samy Kamkar

- Samy Kamkar is one of most famous hackers in the U.S.
- He was sentenced to 3 years of Federal Probation for the Samy worm and prohibited from using the internet for that time
- For a fun interview about this and other subject listen to Samy Kamkars' interview on the Tim Ferriss Show, Episode #74, May 2nd, 2015

Anatomy of a XXS Attack

- User enters text in an input field, within text is JavaScript code
- Server accepts text without encoding or sanitizing
- User enter text displayed to user on page, JavaScript code executes

Prevention of a XXS Attack

- Entered text should be scrubbed of JavaScript characters
- Special characters should be HTML encoded
- For complete precautions refer to OWSAP Cross-Site Scripting Prevention
  - Link in lecture resources

Spring Security XXS Prevention

- Header '`X-XSS-Protection`' is set to '`1; mode=block`'
  - Tells browser to to block XSS code when detected
  - Modern Browsers are starting to deprecate this in favor of Content Security Policy (CSP)
- Content Security Policy - Spring Security does not implement a default value
  - Spring Security can easily be configured
  - Refer to OWASP for best practices
    - Link to OWASP recommendations in lesson resources

SPRING FRAMEWORK

GURU