Spring Security 101

An Introduction To Securing Spring Applications

Agenda

- What is Spring Security
- How Spring Security Works
- Enabling and Configuring Security
- Working with User Details
- Form Authentication
- Security in the UI Layer
- Debugging tips

Important Questions

- How is your application secured?
- How do you keep up with security concerns?
- How hard is it to extend your security model?
- How do you integrate your security model with all aspects of your application?

Important Concepts

- Authentication
  - Is the User/Device/Application who they claim to be?
- Authorization
  - Is the User/Device/Application allowed to perform the action they are requesting

Important Concepts

- Principle
  - Interface from java.security
  - Represents a logged in User
  - Spring Security Authentication is a Principle

  http://docs.spring.io/autorepo/docs/spring-security/4.0.3.RELEASE/apidocs/org/springframework/security/core/Authentication.html

Important Concepts

- Authority
  - Contains the concept of a ROLE
    - Used for access control decisions

http://docs.spring.io/spring-security/site/docs/current/apidocs/

Important Concept

- UserDetails
  - Contains relevant details about the Principal

https://docs.spring.io/spring-security/site/docs/3.2.6.RELEASE/apidocs/org/springframework/security/core/userdetails/User.html

Important Concept

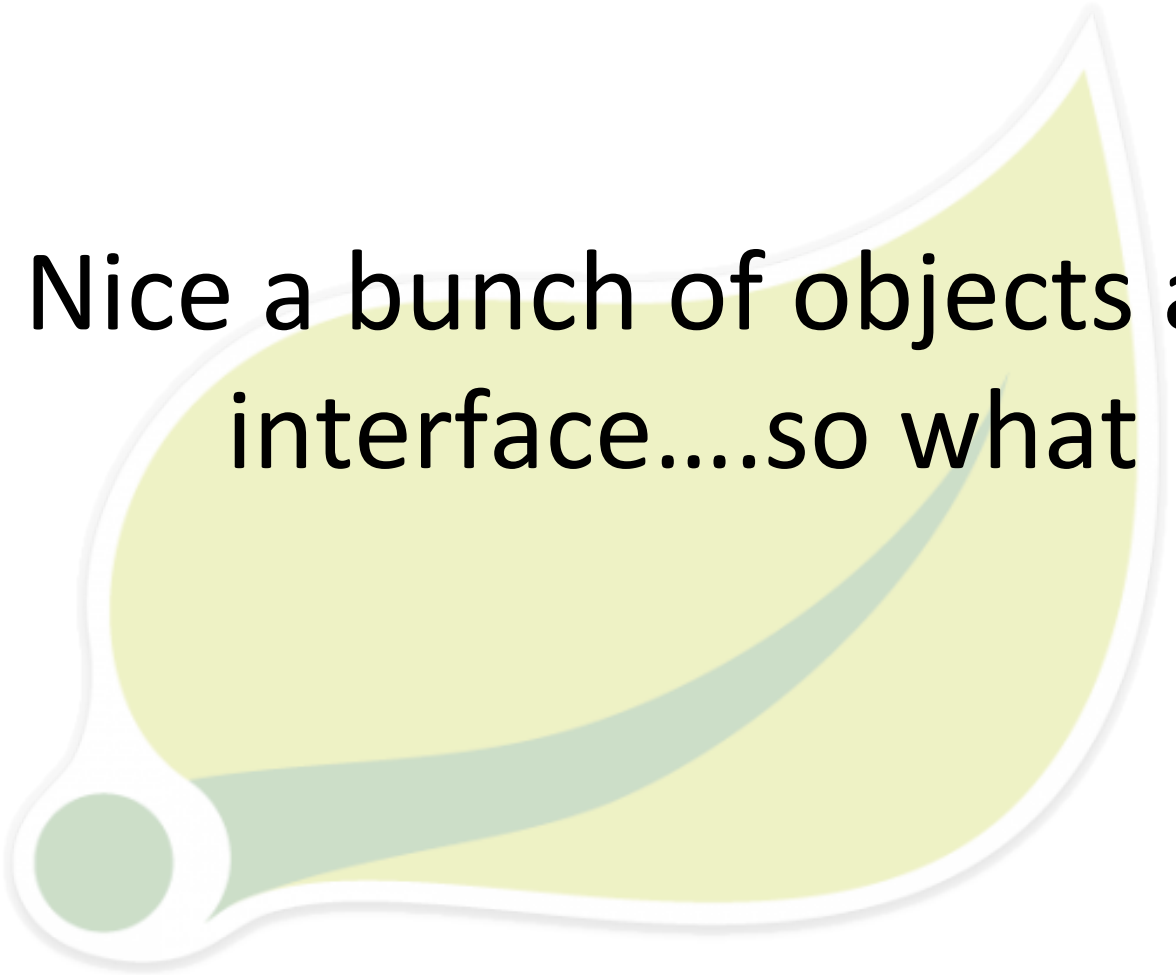
- UserDetailService
  - Implemented to provide a means of getting UserDetail references

http://docs.spring.io/autorepo/docs/spring-security/3.2.2.RELEASE/apidocs/org/springframework/security/core/userdetails/UserDetailsService.html

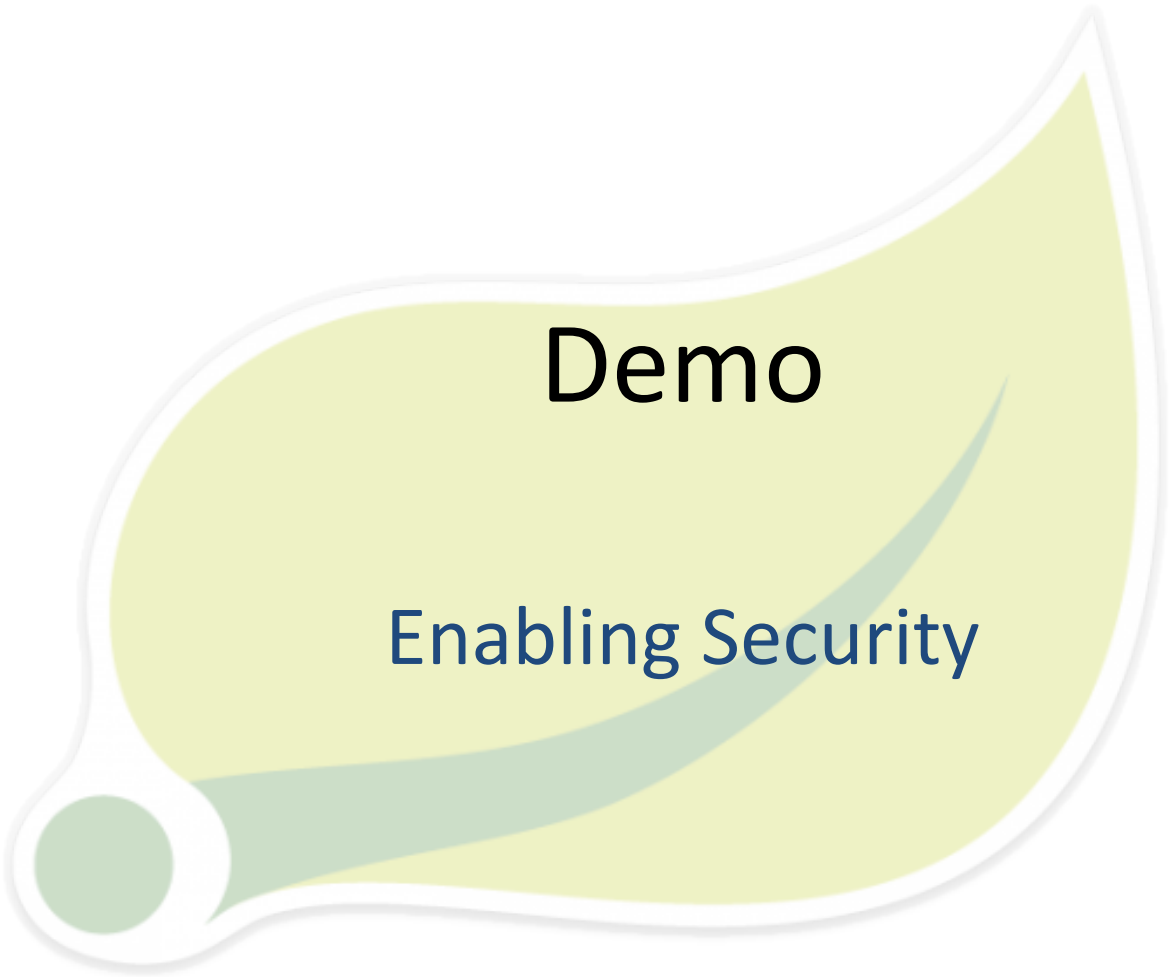
Important Concepts

- SecurityContextHolder
  - Provides a series of method to access the

http://docs.spring.io/spring-security/site/docs/4.0.0.RELEASE/apidocs/org/springframework/security/core/context/SecurityContextHolder.html



Nice a bunch of objects and interface….so what

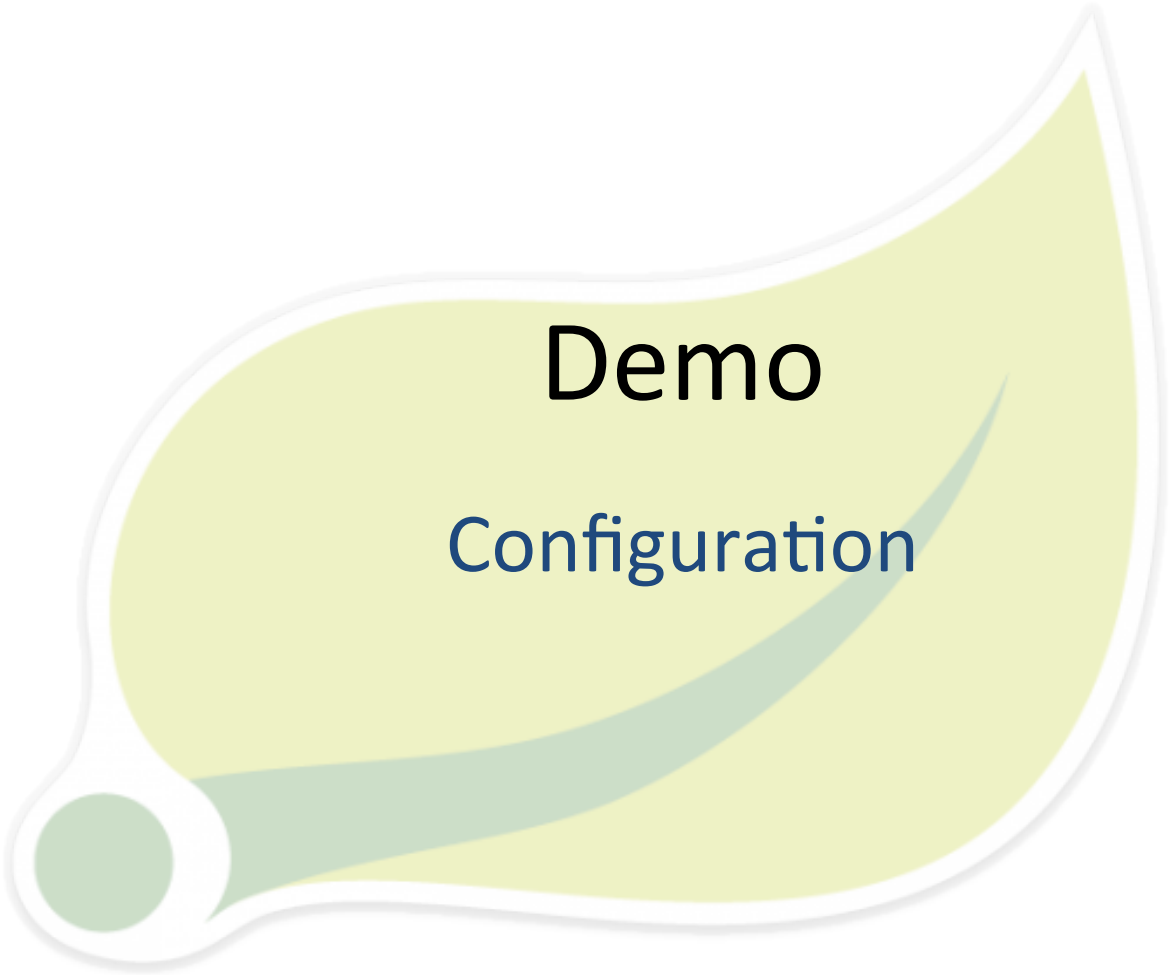


Demo

Enabling Security

Exploring Configuration

- Other things we can enable in the configuration
  - Specify patterns that might not require security
  - Channel Security
  - Cross Site Request Forgery (CSRF)
  - Remember Me Functionality
  - Log Out

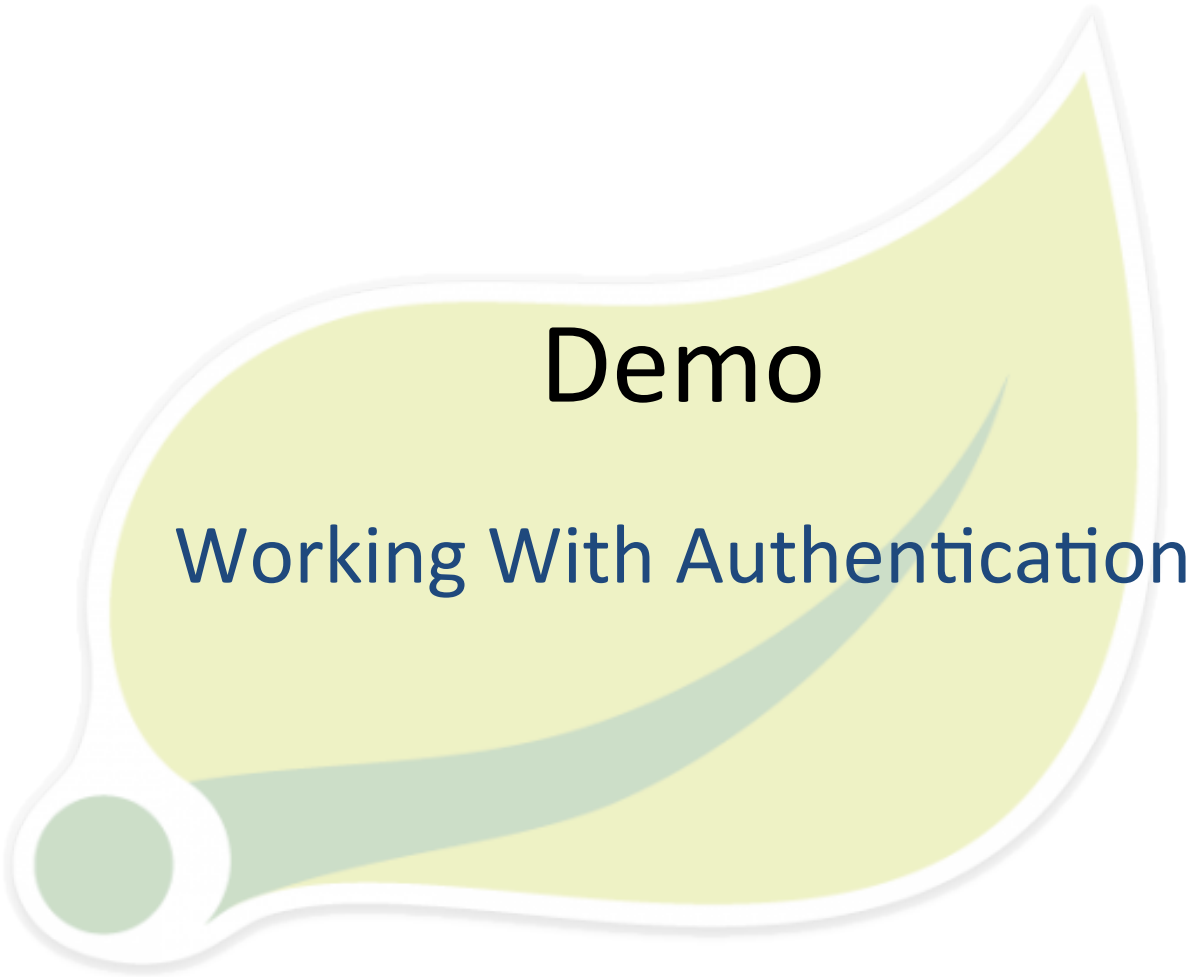


Demo

Configuration

Different Types Of Authentication

- Basic Authentication
  - Generates a Basic Authentication token in the Header of the HTTP Request
- Form Login Authentication
  - Application displays a form to collect information to create the Authentication Object

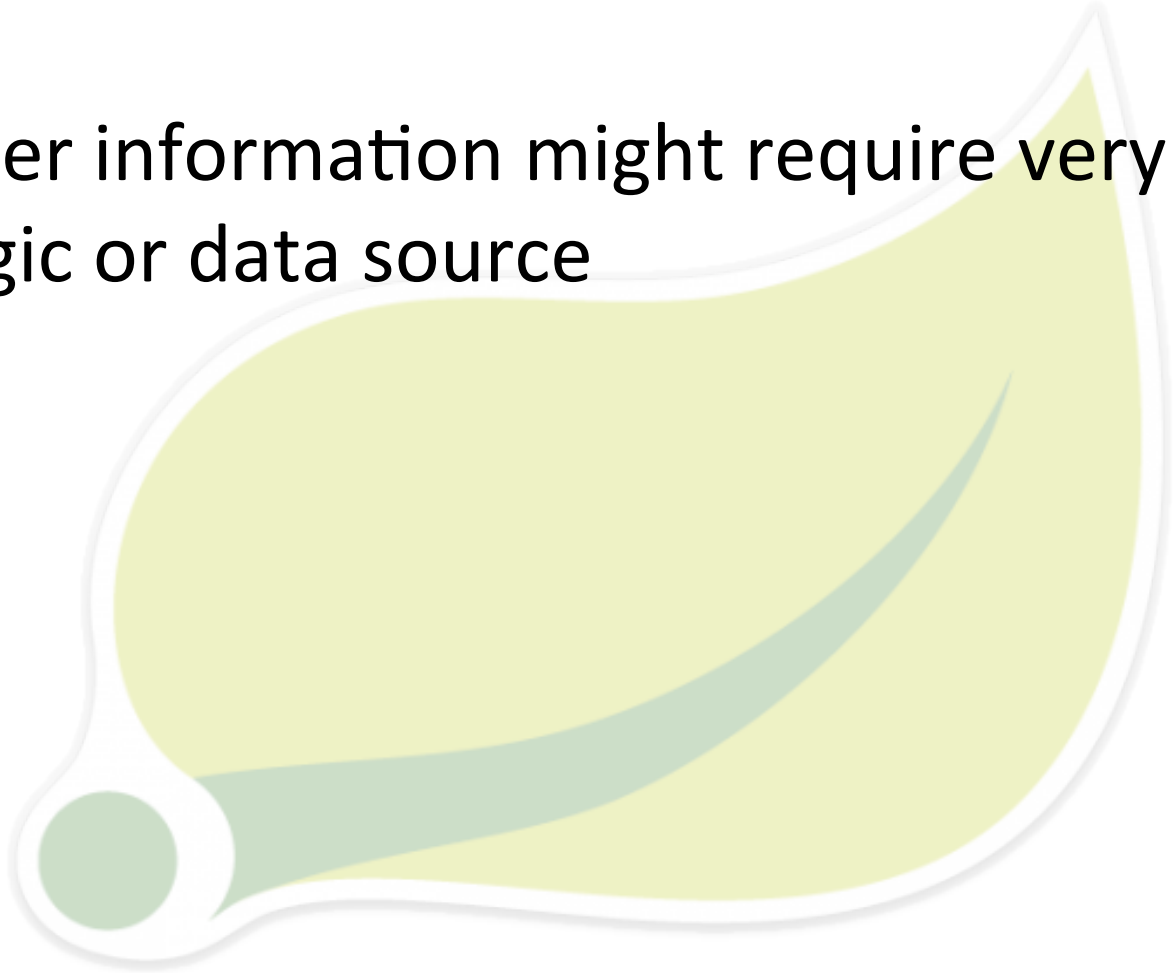


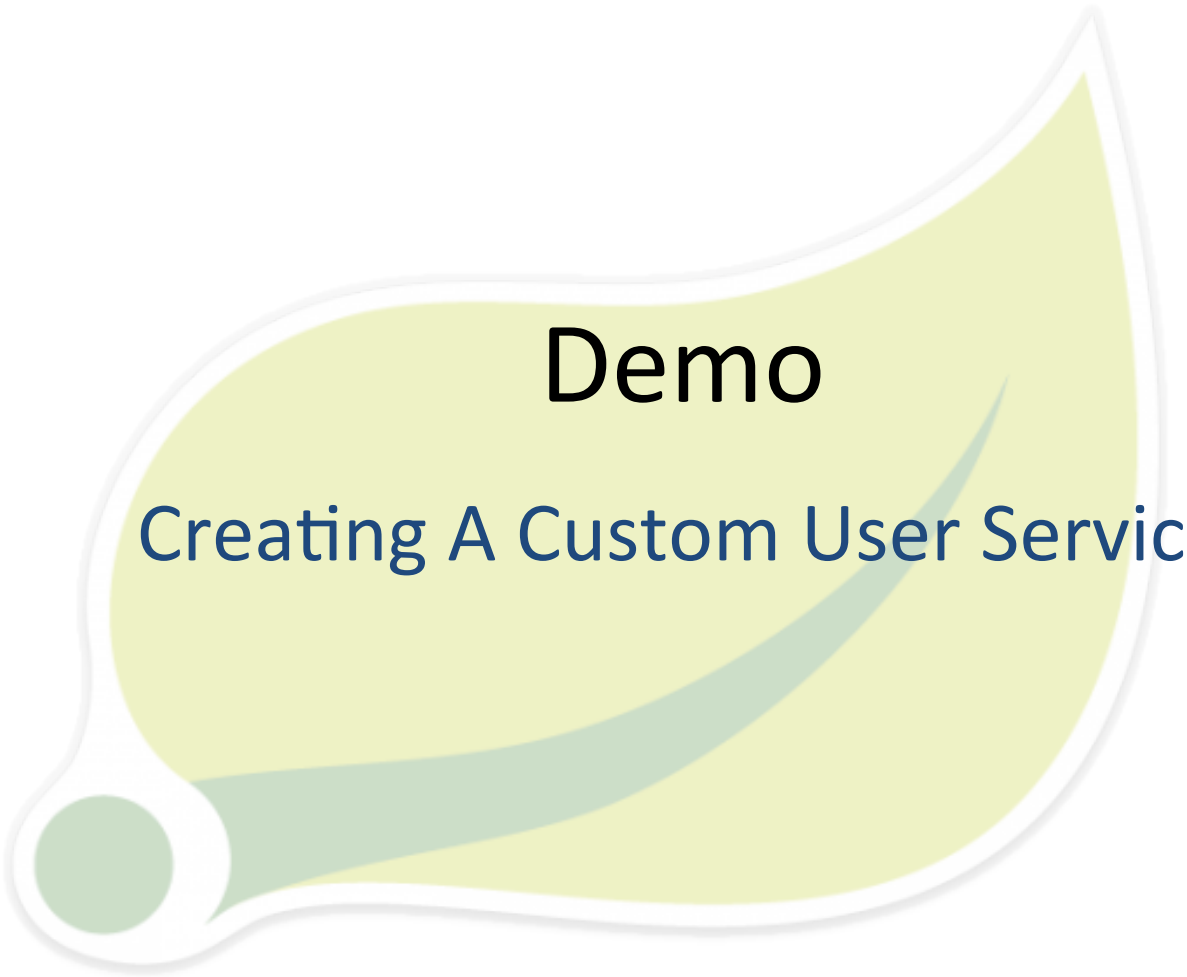
Demo

Working With Authentication

Custom User Services

- User information might require very custom logic or data source



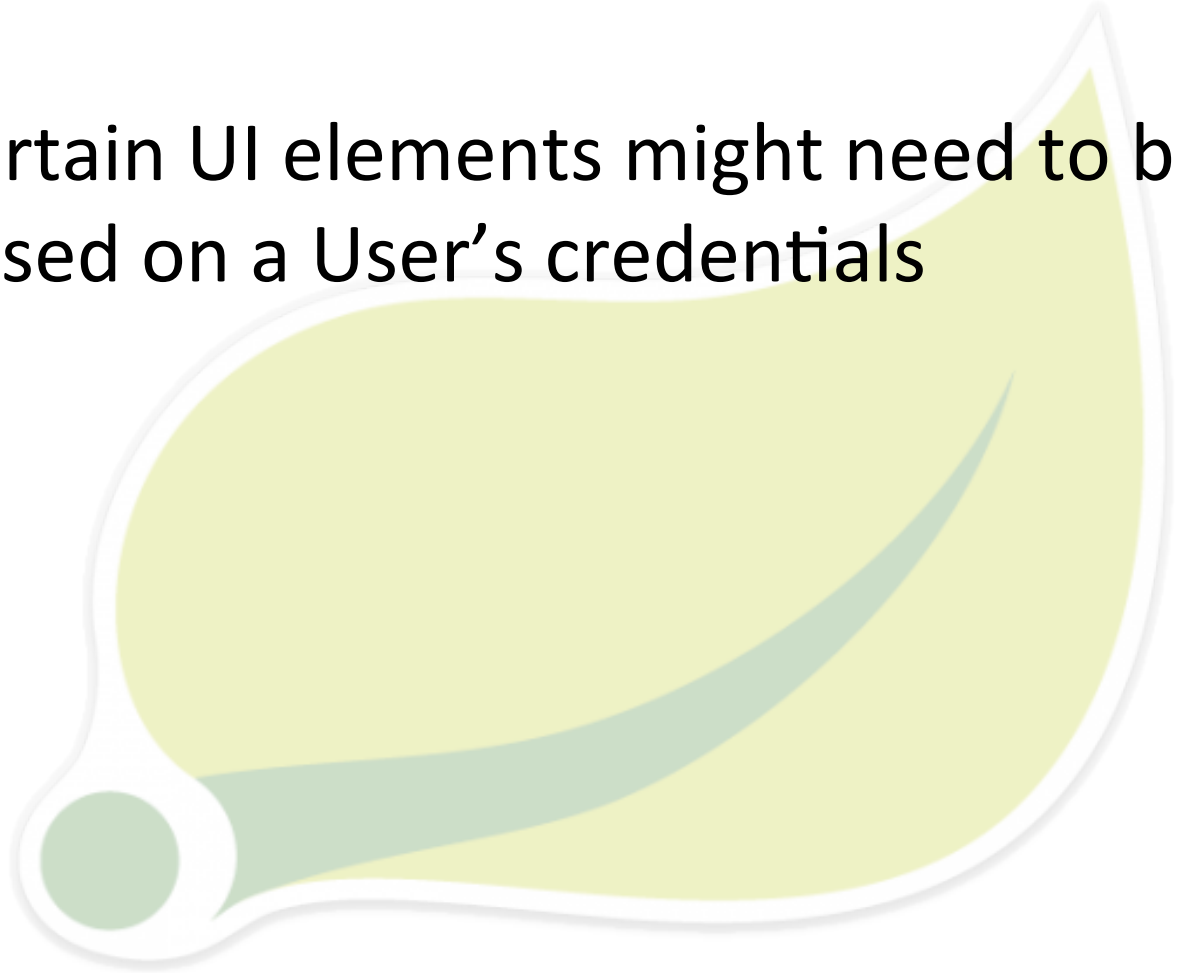


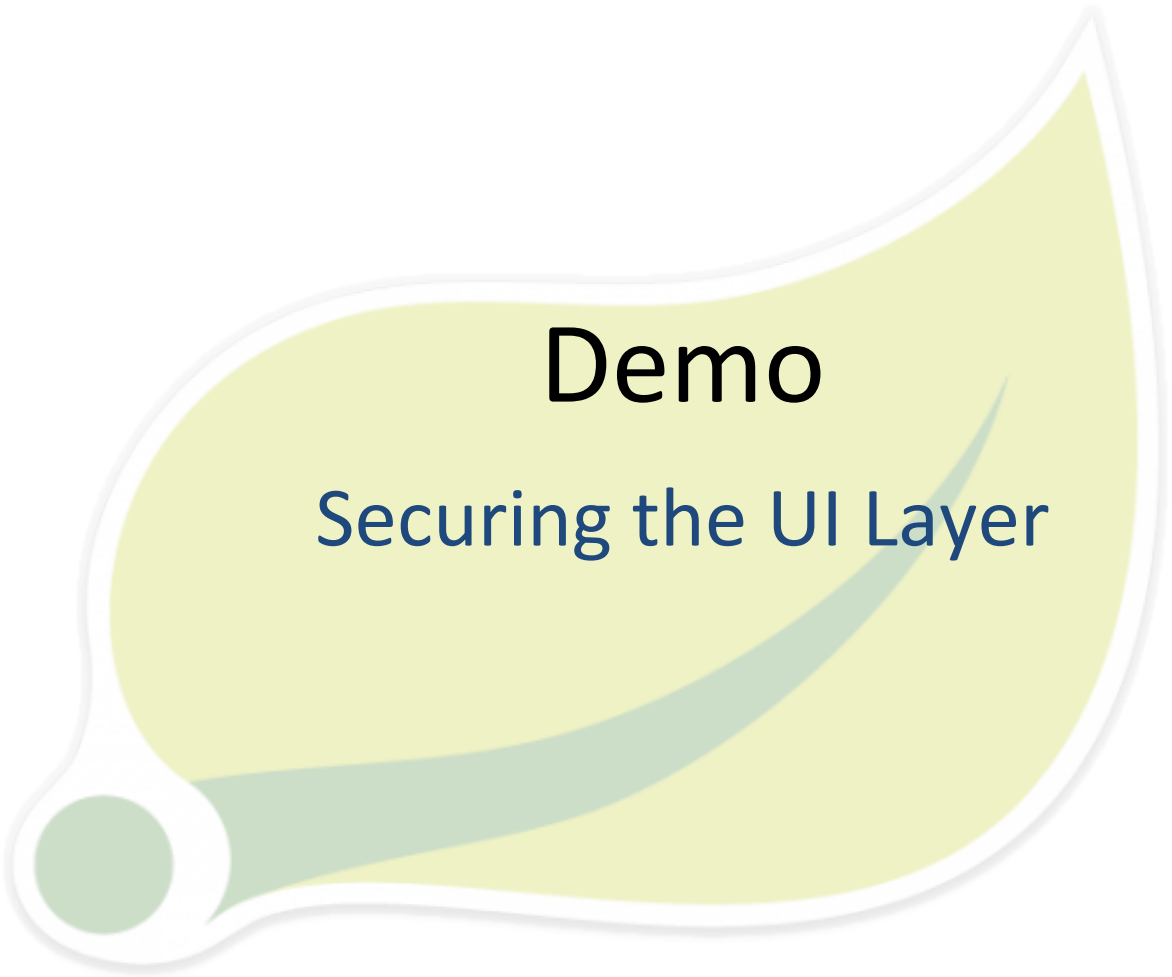
Demo

Creating A Custom User Service

Working With The UI Layer

- Certain UI elements might need to be hidden based on a User's credentials





Demo

Securing the UI Layer

Spring Security Modules

- ACL
  - Provides support for domain object security through access control lists (ACLs).
- Aspects
  - A small module providing support for AspectJ-based aspects instead of stan- dard Spring AOP when using Spring Security annotations.
- CAS Client
  - Support for single sign-on authentication using Jasig's Central Authentication Service (CAS).

Spring Security Modules

- Configuration
  - Contains support for configuring Spring Security with XML and Java. (Java con- figuration support introduced in Spring Security 3.2.)
- Core
  - Provides the essential Spring Security library.
- Cryptography
  - Provides support for encryption and password encoding.

Spring Security Modules

- LDAP
  - Provides support for LDAP-based authentication.
- OpenID
  - Contains support for centralized authentication with OpenID.
- Remoting
  - Provides integration with Spring Remoting.

Spring Security Modules

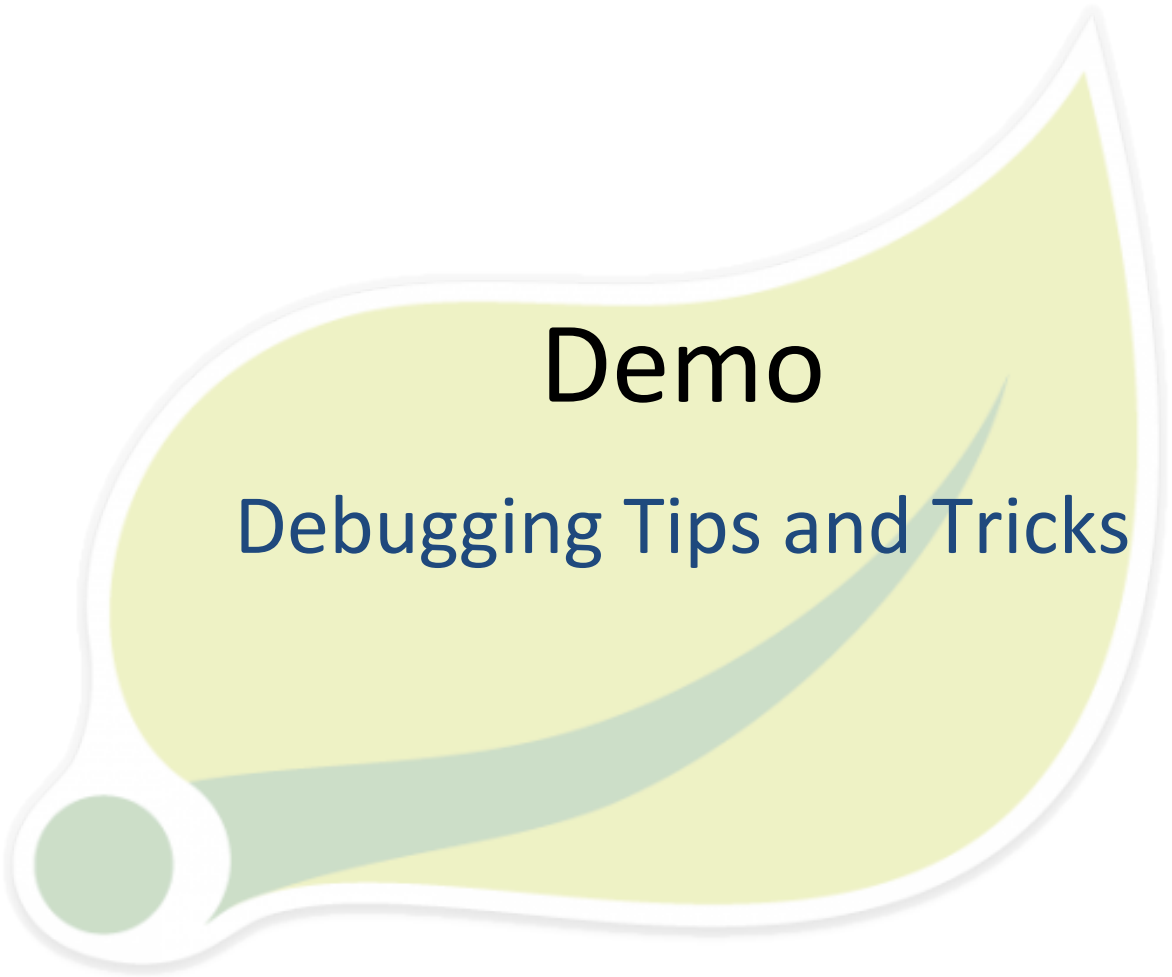
- Tag Library
  - Spring Security's JSP tag library.
- Web
  - Provides Spring Security's filter-based web security support.

Spring Security Related Projects

- Spring Security OAuth
  - support for using Spring Security with OAuth (1a) and OAuth2 using standard Spring and Spring Security programming models and configuration idioms
- Spring LDAP
  - Java library for simplifying LDAP operations, based on the pattern of Spring's JdbcTemplate

Spring Security Related Projects

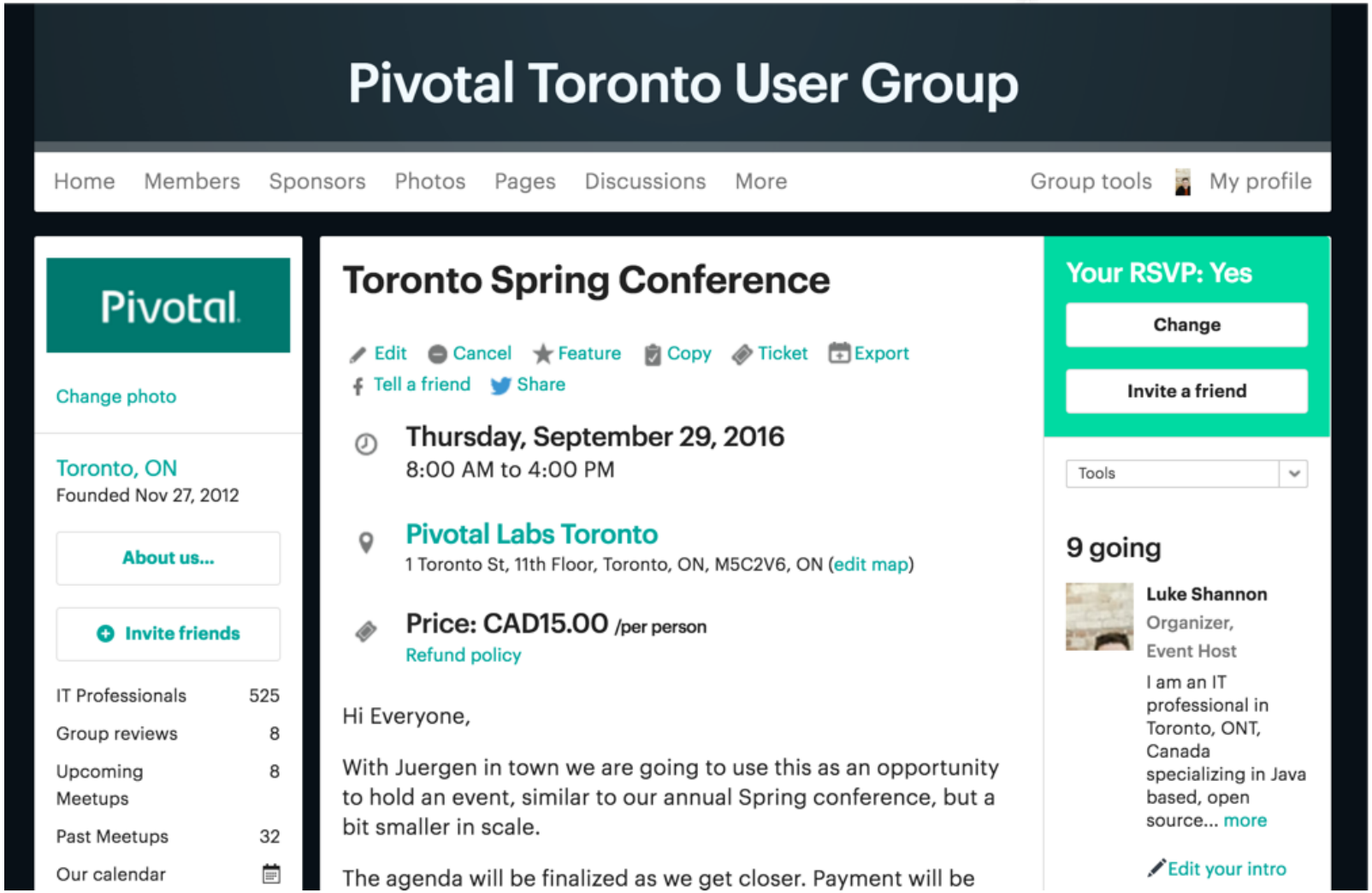
- Spring Security Kerberos
  - With the Spring Security Kerberos Extension, your users are authenticated against your web application just by opening the URL
- Spring Security SAML
  - Seamless combination of SAML 2.0 and authentication and federation mechanisms in a single application. Wide support (ADFS, Okta, Shibboleth, OpenAM, Efecte EIM or Ping Federate)



Demo

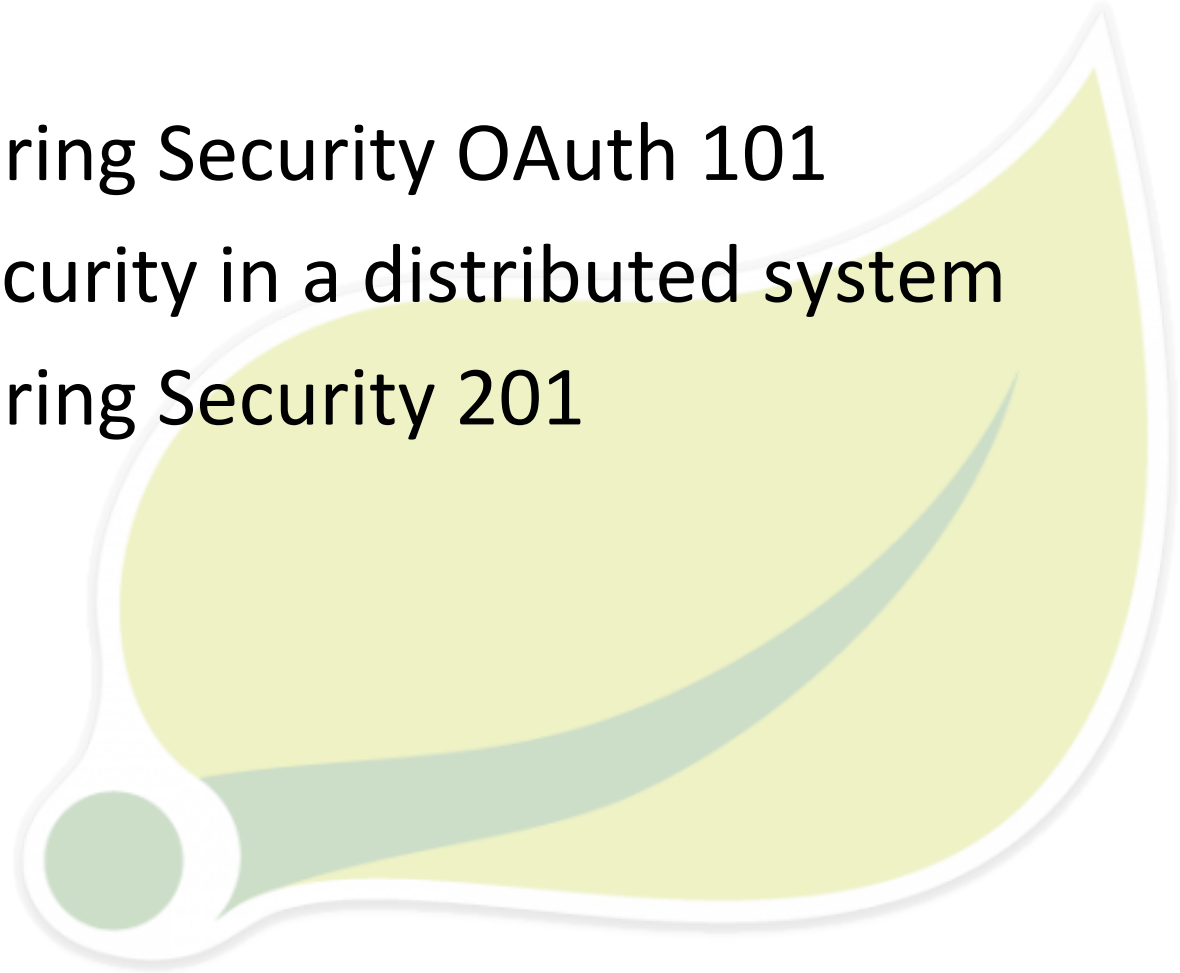
Debugging Tips and Tricks

Get Your Spring On!



Future Talks

- Spring Security OAuth 101
- Security in a distributed system
- Spring Security 201



Questions?