



[HOME](#) [POSTS](#) [PORTFOLIO](#) [SPEAKING](#) [CV](#) [CONTACT](#)

Grails Programmer : How to secure your Grails 3 API with Spring Security REST for Grails?

26 / 02

[5 Replies](#)

For this post I will continue reusing the code I created in the [How to use Spring Security Core to Secure your Grails 3 app post](#)

In this post we are going to expose our app product announcements as JSON API and secure it with [Spring Security REST for Grails](#) plugin.

Lets create a service to encapsulate the logic.

```
1 | $ grails create-service ProductAnnouncement
2 |   Created grails-app/services/myapp/ProductAnnouncementService.groovy
3 |   Created src/test/groovy/myapp/ProductAnnouncementServiceSpec.groovy
```

with the content:

```
1 | package myapp
2 |
3 | import grails.transaction.Transactional
4 |
5 | @Transactional
6 | class ProductAnnouncementService {
7 |
8 |     List<ProductAnnouncement> lastAnnouncements() {
9 |
10 |         ProductAnnouncement.createCriteria().list {
11 |             order("dateCreated", "desc")
12 |             maxResults(1)
13 |         }
14 |     }
15 | }
16 | }
```

Lets create a controller for our API endpoints.

```
1 | $ grails create-controller Api
```

```
2 | Created grails-app/controllers/myapp/ApiController.groovy
3 | Created src/test/groovy/myapp/ApiControllerSpec.groovy
```

Lets define a controller action to expose the last announcements as a JSON payload

```
1 package myapp
2
3 import grails.plugin.springsecurity.annotation.Secured
4
5 class ApiController {
6
7     def productAnnouncementService
8
9     @Secured(['ROLE_USER'])
10    def announcements() {
11        render(contentType: "application/json") {
12            announcements {
13                for(a in productAnnouncementService.lastAnnouncements()) {
14                    announcement(message: a.message)
15                }
16            }
17        }
18    }
19 }
```

Install Spring Security REST for Grails

To install it we need to add a dependency to build.gradle

```
1 buildscript {
2     ext {
3         grailsVersion = project.grailsVersion
4     }
5     repositories {
6         mavenLocal()
7         maven { url "https://repo.grails.org/grails/core" }
8     }
9     dependencies {
10        classpath "org.grails:grails-gradle-plugin:$grailsVersion"
11        classpath "com.bertramlabs.plugins:asset-pipeline-gradle:2.5.0"
12        classpath "org.grails.plugins:hibernate4:5.0.0"
13    }
14 }
15
16 version "0.1"
17 group "myapp"
18
19 apply plugin:"eclipse"
20 apply plugin:"idea"
21 apply plugin:"war"
22 apply plugin:"org.grails.grails-web"
23 apply plugin:"org.grails.grails-gsp"
24 apply plugin:"asset-pipeline"
25
26 ext {
27     grailsVersion = project.grailsVersion
28     gradleWrapperVersion = project.gradleWrapperVersion
29 }
30
```

```
31 repositories {
32     mavenLocal()
33     maven { url "https://repo.grails.org/grails/core" }
34 }
35
36 dependencyManagement {
37     imports {
38         mavenBom "org.grails:grails-bom:$grailsVersion"
39     }
40     applyMavenExclusions false
41 }
42
43 dependencies {
44     compile "org.springframework.boot:spring-boot-starter-logging"
45     compile "org.springframework.boot:spring-boot-autoconfigure"
46     compile "org.grails:grails-core"
47     compile "org.springframework.boot:spring-boot-starter-actuator"
48     compile "org.springframework.boot:spring-boot-starter-tomcat"
49     compile "org.grails:grails-dependencies"
50     compile "org.grails:grails-web-boot"
51     compile "org.grails.plugins:cache"
52     compile "org.grails.plugins:scaffolding"
53     compile "org.grails.plugins:hibernate4"
54     compile "org.hibernate:hibernate-ehcache"
55     console "org.grails:grails-console"
56     profile "org.grails.profiles:web:3.1.1"
57     runtime "org.grails.plugins:asset-pipeline"
58     runtime "com.h2database:h2"
59     testCompile "org.grails:grails-plugin-testing"
60     testCompile "org.grails.plugins:geb"
61     testRuntime "org.seleniumhq.selenium:selenium-htmlunit-driver:2.47.1"
62     testRuntime "net.sourceforge.htmlunit:htmlunit:2.18"
63     compile "org.grails.plugins:spring-security-core:3.0.3"
64     compile "org.grails.plugins:spring-security-rest:2.0.0.M2"
65 }
66
67 task wrapper(type: Wrapper) {
68     gradleVersion = gradleWrapperVersion
69 }
70
71 assets {
72     minifyJs = true
73     minifyCss = true
74 }
```

Spring Security REST for Grails exposes an endpoint `/api/login` which we can access with a POST request. We should supply our credentials (username and password) as parameters. If we are successfully authenticated we will get an *access_token* and a *refresh_token*.

: POST http://localhost:8080/api/login				200 OK			
Headers URL Params Body Options				Info Request Response Headers JSON Raw			
Text	Key or Index	Type	Value	Key or Index	Type	Value	
JSON	Root	2 items		Root	6 items		
Form URL-Encoded	username	me@sergiodelamo.com		username	me@sergiodelamo.com		
Multipart	password	groovycalamari		roles	1 item		
File				Index 0	ROLE_USER		
				token_type	Bearer		
				access_token	eyJhbGciOiJIUzI1NiJ9.eyJwcmVudG9...		
				expires_in	3600		
				refresh_token	eyJhbGciOiJIUzI1NiJ9.eyJwcmVudG9...		

We can do a GET request to our *http://localhost:8080/api/announcements* endpoint.

We need to add an HTTP header:

Header Name: Authorization

Header Value: Bearer access_token

The access_token is the one we got back from the api/login endpoint.

The above request is illustrated here:

GET http://localhost:8080/api/announcements

Headers
URL Params
Body
Options

Header Name
Header Value

Authorization
Bearer eyJhbGciOiJIUzI1NiJ9.eyJwcmVudG9...

Add Header Name
Add Header Value

Access token returned by api/login

200 OK

Info
Request
Response
Headers
JSON
Raw

Key or Index
Type Value

Root
1 item

announcements
1 item

announcement
1 item

message
Launch day

Note we are using a [JSON Web Token \(JWT\)](#) which we don't need to store on the server side. The token validation is done without a repository (database or similar) call. Thus, better for the scalability of the application.

Access token expire. However in the *api/login* method we got a refresh token which we can use to get a new access token. We can do POST request as shown below:

: POST http://localhost:8080/oauth/access_token/?grant_typ...

200 OK

HeadersURL ParamsBodyOptions

URL Parameter	Value
grant_type	refresh_token
refresh_token	7M0esADRXdmRQvK9BMA40ejSGldRG4w4
Add URL Parameter	Add Value

InfoRequestResponseHeadersJSONRaw

Key or Index	Type	Value
Root	6 items	
username		me@sergiodelamo.com
roles	1 item	
Index 0		ROLE_USER
token_type		Bearer
access_token		eyJhbGciOiJIUzI1NiJ9.eyJwcmliuY2lwYWwiOi...
expires_in		3600
refresh_token		eyJhbGciOiJIUzI1NiJ9.eyJwcmliuY2lwYWwiOi...

Do you like to read about Groovy/Grails development? Yes, then Subscribe to [Groovy Calamari](#) a weekly curated email newsletter about the Groovy ecosystem which I write 🍴

← How to use Spring Security Core to Secure you Grails 3 App?

Grails Programmer : How to change the default port of a Grails 3 App →

5 thoughts on “Grails Programmer : How to secure your Grails 3 API with Spring Security REST for Grails?”



jf li
3 December, 2016 at 5:02

Could you advise what tool you are using while you test the http post form?

Reply ↓



Sergio
3 December, 2016 at 8:06

Sure Jf li. I use PAW (<https://paw.cloud>)

Reply ↓



jf li

3 December, 2016 at 8:17

wonderful! thanks a lot

Reply ↓



Farah

17 May, 2017 at 1:06

What if I want to secure the “def announcements()” for 2 specific users? How can I do that?

I have tried so far....

```
@Secured(["authentication.name == 'admin1'", "authentication.name == 'admin2'"])
```

```
@Secured("authentication.name in ['admin1', 'admin2']")
```

```
@Secured("[ 'admin1', 'admin2'].contains(authentication.name)")
```

None of them are working ☐

Reply ↓



Sergio

27 May, 2017 at 5:47

Farah I believe it is a closure.

That it is to say:

```
@Secured( { ['admin1', 'admin2'].contains(authentication.name) })
```

Note I think your best option would be to add a role to admin1 and admin2 and secured the action based on that role.

Reply ↓

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

☐ Notify me of follow-up comments by email.

☐ Notify me of new posts by email.





**Sergio del Amo**
27,598
62 132 168

Drag to outliner or Upload
Close