Angular WebApp Security with OAuth2

(Reverse engineering Jhipster Generated Code)

arnaud.nauwynck@gmail.com

this document: https://github.com/Arnaud-Nauwynck/Presentations/Web/Security-OAuth2-Angular-ReverseEngineering-Jhipster

Comparison Only with the JWT Mode

This document focus on comparisons
of the default "**JWT**" mode  "**OAuth2**" Mode

For more detailed screenshots => please see document part 1

Step 1: re-generate ANOTHER Jhipster project with same name

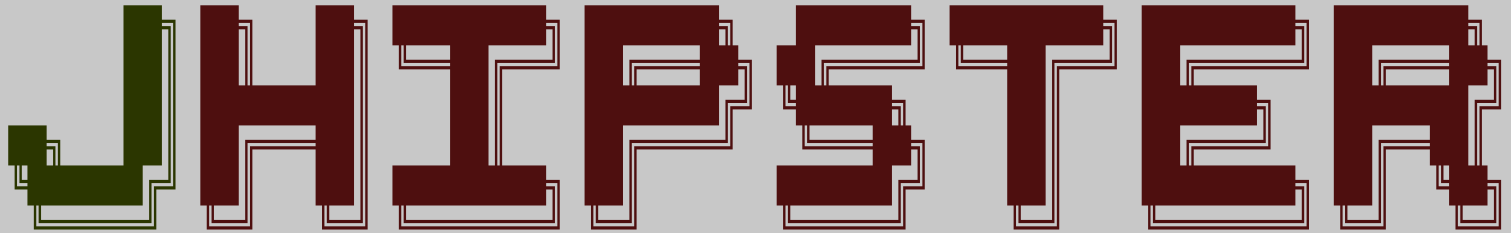
```
# check already install globally
npm install -g generator-jhipster

# create a new empty dir
mkdir demo-oauth2
cd demo-oauth2

# launch jhipster generator
jhipster
```

jhipster

```
$ jhipster
```




```
                    https://www.jhipster.tech
Welcome to JHipster v8.7.3

(node:19104) [DEP0040] DeprecationWarning: The `punycode` module is deprecated. Please use a userland alternative instead.
(Use `node --trace-deprecation ...` to show where the warning was created)
 ──────────────────────────────────────────────────────────────────────────────────────────────────────────────

  Documentation for creating an application is at https://www.jhipster.tech/creating-an-app/

  Application files will be generated in folder: C:\web\demo-jhipster\demo-oauth2
 ──────────────────────────────────────────────────────────────────────────────────────────────────────────────

WARNING! Your Node version is not LTS (Long Term Support), use it at your own risk! JHipster does not support non-LTS relea
f you encounter a bug, please use a LTS version first.
? What is the base name of your application? (demoOauth2)
```

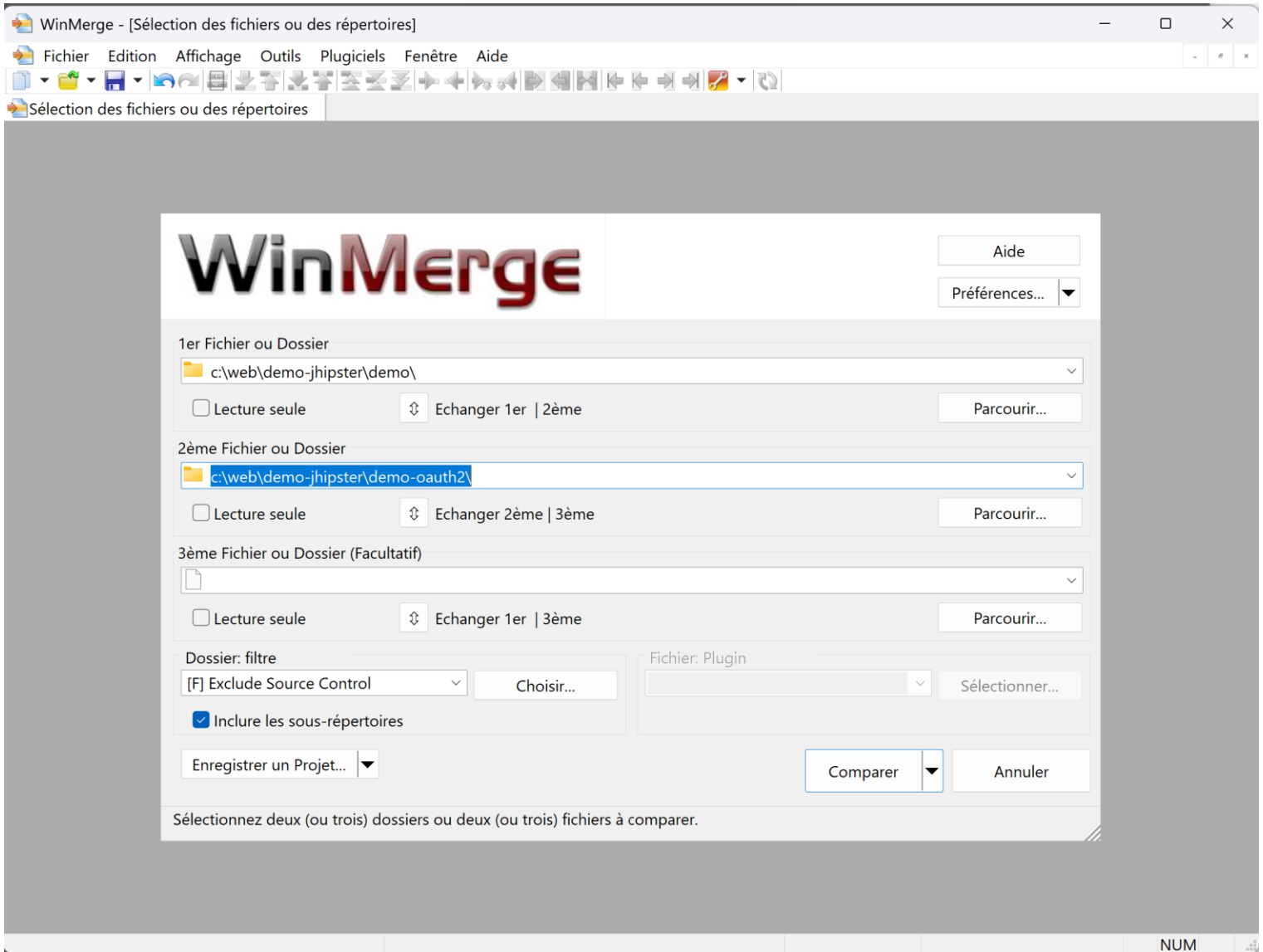
when prompted for project name (inferred for current directory name) => change to be same as "demo" project instead of "demo-oauth2"

```
? What is the base name of your application? demo
```

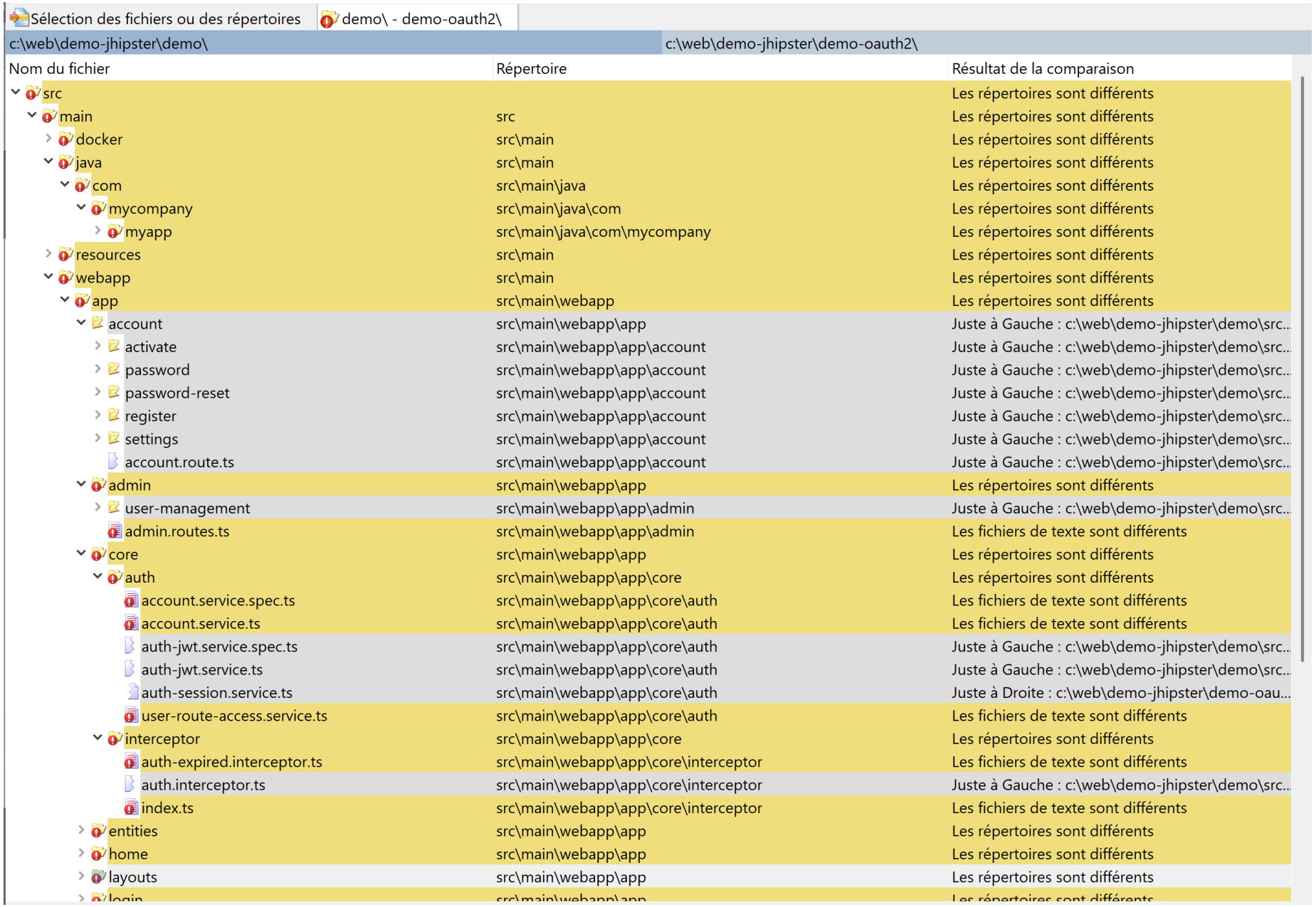
on question "Which type of authentication.. ?" change from default choice #1 to choice #2: OAuth2

```
√ What is the base name of your application? demo
√ Which *type* of application would you like to create? Monolithic application (recommended for simple projects)
√ What is your default Java package name? com.mycompany.myapp
√ Would you like to use Maven or Gradle for building the backend? Maven
√ Do you want to make it reactive with Spring WebFlux? no
? Which *type* of authentication would you like to use?
  JWT authentication (stateless, with a token)
> OAuth 2.0 / OIDC Authentication (stateful, works with Keycloak and Okta)
  HTTP Session Authentication (stateful, default Spring Security mechanism)
```

Comparing (WinMerge) Generated Apps
JWT <-> OAuth2



Differences JWT <-> OAuth2



Sélection des fichiers ou des répertoires | demo\ - demo-oauth2\

c:\web\demo-jhipster\demo\		c:\web\demo-jhipster\demo-oauth2\
Nom du fichier	Répertoire	Résultat de la comparaison
src		Les répertoires sont différents
main	src	Les répertoires sont différents
docker	src\main	Les répertoires sont différents
java	src\main	Les répertoires sont différents
com	src\main\java	Les répertoires sont différents
mycompany	src\main\java\com	Les répertoires sont différents
myapp	src\main\java\com\mycompany	Les répertoires sont différents
resources	src\main	Les répertoires sont différents
webapp	src\main	Les répertoires sont différents
app	src\main\webapp	Les répertoires sont différents
account	src\main\webapp\app	Juste à Gauche : c:\web\demo-jhipster\demo\src...
activate	src\main\webapp\app\account	Juste à Gauche : c:\web\demo-jhipster\demo\src...
password	src\main\webapp\app\account	Juste à Gauche : c:\web\demo-jhipster\demo\src...
password-reset	src\main\webapp\app\account	Juste à Gauche : c:\web\demo-jhipster\demo\src...
register	src\main\webapp\app\account	Juste à Gauche : c:\web\demo-jhipster\demo\src...
settings	src\main\webapp\app\account	Juste à Gauche : c:\web\demo-jhipster\demo\src...
account.route.ts	src\main\webapp\app\account	Juste à Gauche : c:\web\demo-jhipster\demo\src...
admin	src\main\webapp\app	Les répertoires sont différents
user-management	src\main\webapp\app\admin	Juste à Gauche : c:\web\demo-jhipster\demo\src...
admin.routes.ts	src\main\webapp\app\admin	Les fichiers de texte sont différents
core	src\main\webapp\app	Les répertoires sont différents
auth	src\main\webapp\app\core	Les répertoires sont différents
account.service.spec.ts	src\main\webapp\app\core\auth	Les fichiers de texte sont différents
account.service.ts	src\main\webapp\app\core\auth	Les fichiers de texte sont différents
auth-jwt.service.spec.ts	src\main\webapp\app\core\auth	Juste à Gauche : c:\web\demo-jhipster\demo\src...
auth-jwt.service.ts	src\main\webapp\app\core\auth	Juste à Gauche : c:\web\demo-jhipster\demo\src...
auth-session.service.ts	src\main\webapp\app\core\auth	Juste à Droite : c:\web\demo-jhipster\demo-oau...
user-route-access.service.ts	src\main\webapp\app\core\auth	Les fichiers de texte sont différents
interceptor	src\main\webapp\app\core	Les répertoires sont différents
auth-expired.interceptor.ts	src\main\webapp\app\core\interceptor	Les fichiers de texte sont différents
auth.interceptor.ts	src\main\webapp\app\core\interceptor	Juste à Gauche : c:\web\demo-jhipster\demo\src...
index.ts	src\main\webapp\app\core\interceptor	Les fichiers de texte sont différents
entities	src\main\webapp\app	Les répertoires sont différents
home	src\main\webapp\app	Les répertoires sont différents
layouts	src\main\webapp\app	Les répertoires sont différents
login	src\main\webapp\app	Les répertoires sont différents

Files Only in "JWT" mode

Sélection des fichiers ou des répertoires | demo\ - demo-oauth2\

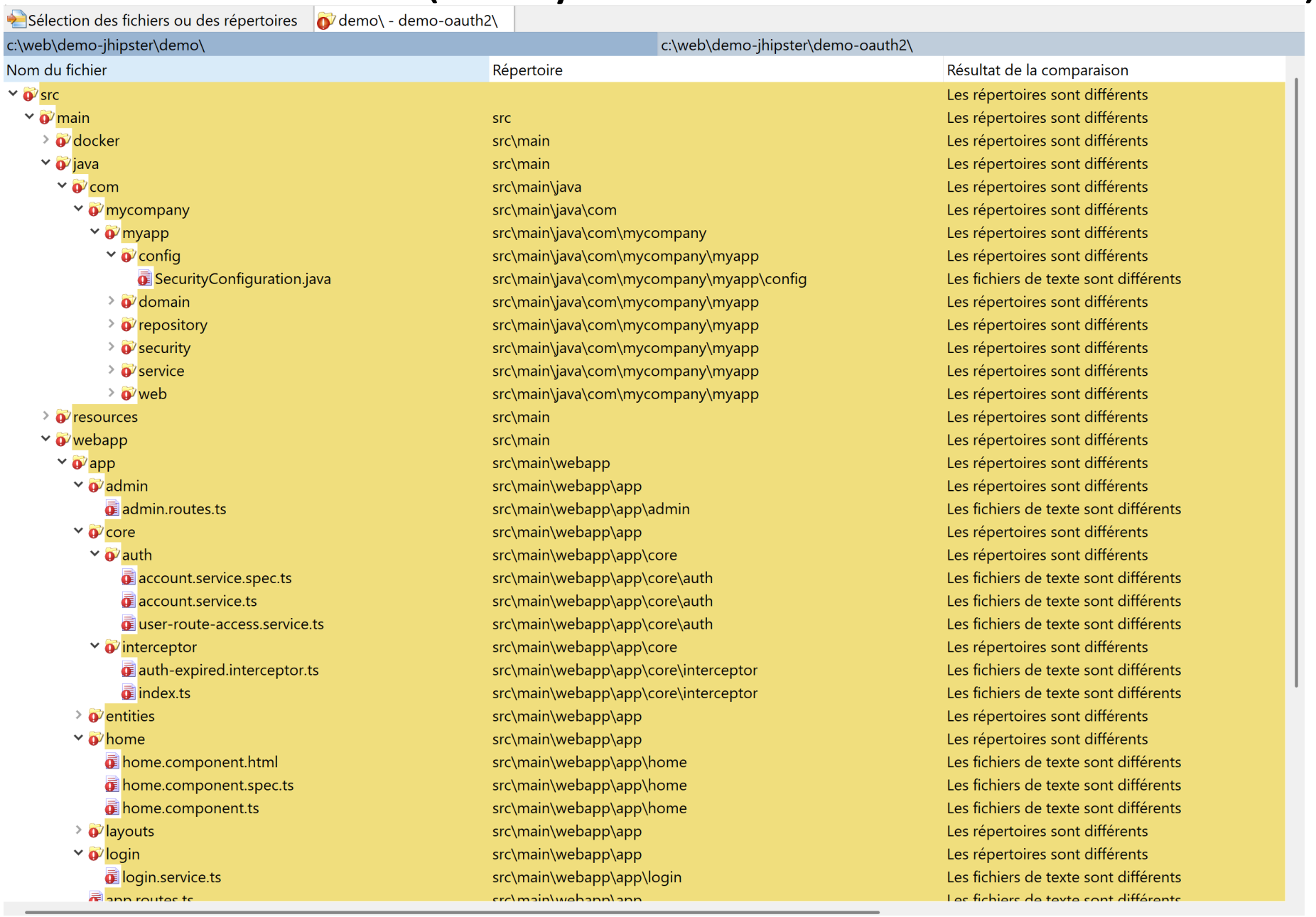
c:\web\demo-jhipster\demo\		c:\web\demo-jhipster\demo-oauth2\	
Nom du fichier	Répertoire	Résultat de la comparaison	D
src		Les répertoires sont différents	
main	src	Les répertoires sont différents	
java	src\main	Les répertoires sont différents	
com	src\main\java	Les répertoires sont différents	
mycompany	src\main\java\com	Les répertoires sont différents	
myapp	src\main\java\com\mycompany	Les répertoires sont différents	
resources	src\main	Les répertoires sont différents	
webapp	src\main	Les répertoires sont différents	
app	src\main\webapp	Les répertoires sont différents	
account	src\main\webapp\app	Juste à Gauche : c:\web\demo-jhipster\demo\src...	*
activate	src\main\webapp\app\account	Juste à Gauche : c:\web\demo-jhipster\demo\src...	*
password	src\main\webapp\app\account	Juste à Gauche : c:\web\demo-jhipster\demo\src...	*
password-reset	src\main\webapp\app\account	Juste à Gauche : c:\web\demo-jhipster\demo\src...	*
register	src\main\webapp\app\account	Juste à Gauche : c:\web\demo-jhipster\demo\src...	*
settings	src\main\webapp\app\account	Juste à Gauche : c:\web\demo-jhipster\demo\src...	*
account.route.ts	src\main\webapp\app\account	Juste à Gauche : c:\web\demo-jhipster\demo\src...	*
admin	src\main\webapp\app	Les répertoires sont différents	
user-management	src\main\webapp\app\admin	Juste à Gauche : c:\web\demo-jhipster\demo\src...	*
core	src\main\webapp\app	Les répertoires sont différents	
auth	src\main\webapp\app\core	Les répertoires sont différents	
auth-jwt.service.spec.ts	src\main\webapp\app\core\auth	Juste à Gauche : c:\web\demo-jhipster\demo\src...	*
auth-jwt.service.ts	src\main\webapp\app\core\auth	Juste à Gauche : c:\web\demo-jhipster\demo\src...	*
interceptor	src\main\webapp\app\core	Les répertoires sont différents	
auth.interceptor.ts	src\main\webapp\app\core\interceptor	Juste à Gauche : c:\web\demo-jhipster\demo\src...	*
login	src\main\webapp\app	Les répertoires sont différents	
login.component.html	src\main\webapp\app\login	Juste à Gauche : c:\web\demo-jhipster\demo\src...	*
login.component.spec.ts	src\main\webapp\app\login	Juste à Gauche : c:\web\demo-jhipster\demo\src...	*
login.component.ts	src\main\webapp\app\login	Juste à Gauche : c:\web\demo-jhipster\demo\src...	*
login.model.ts	src\main\webapp\app\login	Juste à Gauche : c:\web\demo-jhipster\demo\src...	*
i18n	src\main\webapp	Les répertoires sont différents	
test	src	Les répertoires sont différents	
package-lock.json		Juste à Gauche : c:\web\demo-jhipster\demo	*

Files Only in "OAuth2" Mode

Sélection des fichiers ou des répertoires | demo\ - demo-oauth2\

c:\web\demo-jhipster\demo\		c:\web\demo-jhipster\demo-oauth2\
Nom du fichier	Répertoire	Résultat de la comparaison
src		Les répertoires sont différents
main	src	Les répertoires sont différents
docker	src\main	Les répertoires sont différents
java	src\main	Les répertoires sont différents
com	src\main\java	Les répertoires sont différents
mycompany	src\main\java\com	Les répertoires sont différents
myapp	src\main\java\com\mycompany	Les répertoires sont différents
config	src\main\java\com\mycompany\myapp	Les répertoires sont différents
OAuth2Configuration.java	src\main\java\com\mycompany\myapp\config	Juste à Droite : c:\web\demo-jhipster\demo-oau...
security	src\main\java\com\mycompany\myapp	Les répertoires sont différents
oauth2	src\main\java\com\mycompany\myapp\security	Juste à Droite : c:\web\demo-jhipster\demo-oau...
AudienceValidator.java	src\main\java\com\mycompany\myapp\security\oauth2	Juste à Droite : c:\web\demo-jhipster\demo-oau...
CustomClaimConverter.java	src\main\java\com\mycompany\myapp\security\oauth2	Juste à Droite : c:\web\demo-jhipster\demo-oau...
package-info.java	src\main\java\com\mycompany\myapp\security\oauth2	Juste à Droite : c:\web\demo-jhipster\demo-oau...
web	src\main\java\com\mycompany\myapp	Les répertoires sont différents
filter	src\main\java\com\mycompany\myapp\web	Les répertoires sont différents
OAuth2RefreshTokensWebFilter.java	src\main\java\com\mycompany\myapp\web\filter	Juste à Droite : c:\web\demo-jhipster\demo-oau...
rest	src\main\java\com\mycompany\myapp\web	Les répertoires sont différents
AuthInfoResource.java	src\main\java\com\mycompany\myapp\web\rest	Juste à Droite : c:\web\demo-jhipster\demo-oau...
LogoutResource.java	src\main\java\com\mycompany\myapp\web\rest	Juste à Droite : c:\web\demo-jhipster\demo-oau...
webapp	src\main	Les répertoires sont différents
app	src\main\webapp	Les répertoires sont différents
core	src\main\webapp\app	Les répertoires sont différents
auth	src\main\webapp\app\core	Les répertoires sont différents
auth-session.service.ts	src\main\webapp\app\core\auth	Juste à Droite : c:\web\demo-jhipster\demo-oau...
login	src\main\webapp\app	Les répertoires sont différents
logout.model.ts	src\main\webapp\app\login	Juste à Droite : c:\web\demo-jhipster\demo-oau...
test	src	Les répertoires sont différents

Different Files (maybe not for auth mode)

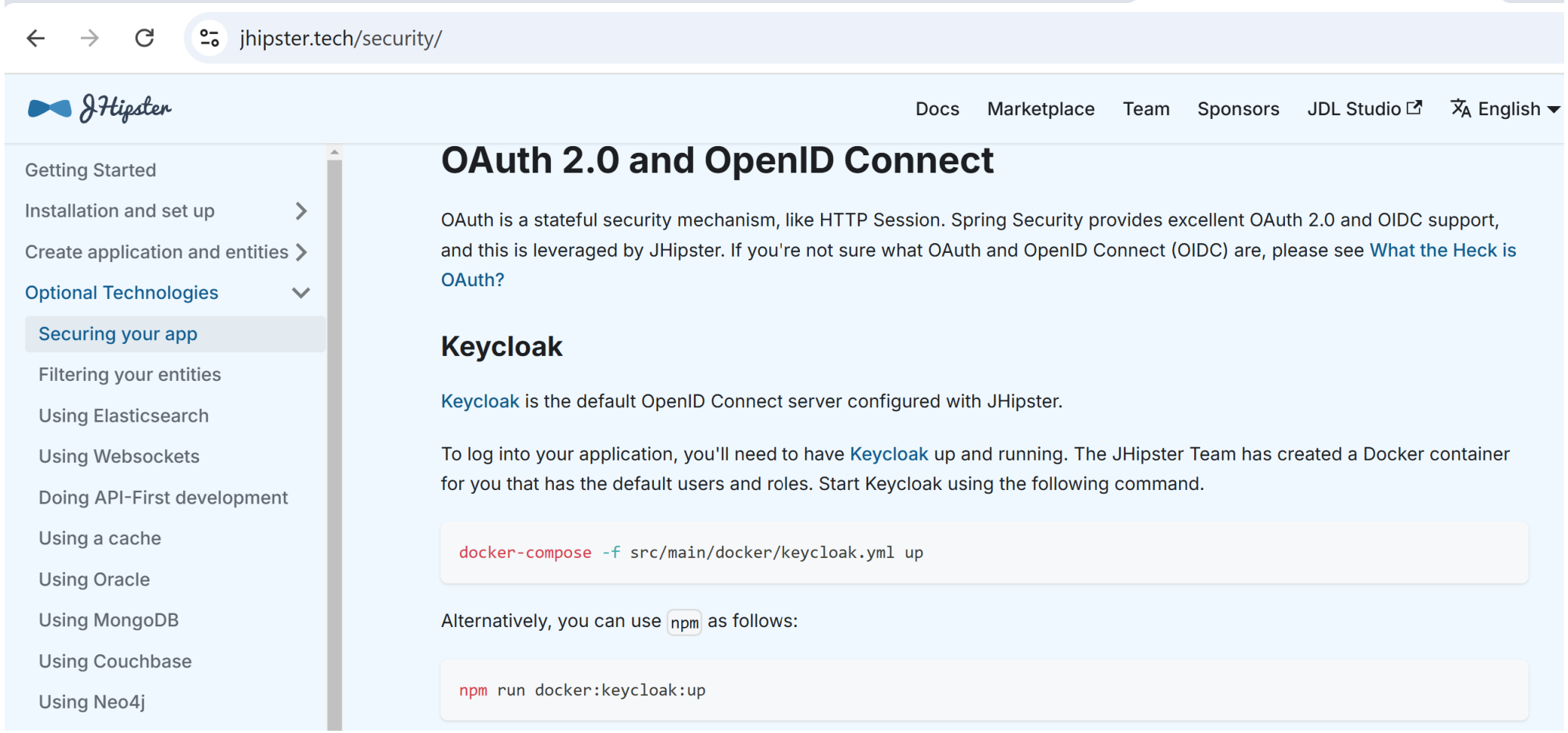


Nom du fichier	Répertoire	Résultat de la comparaison
src		Les répertoires sont différents
main	src	Les répertoires sont différents
docker	src\main	Les répertoires sont différents
java	src\main	Les répertoires sont différents
com	src\main\java	Les répertoires sont différents
mycompany	src\main\java\com	Les répertoires sont différents
myapp	src\main\java\com\mycompany	Les répertoires sont différents
config	src\main\java\com\mycompany\myapp	Les répertoires sont différents
SecurityConfiguration.java	src\main\java\com\mycompany\myapp\config	Les fichiers de texte sont différents
domain	src\main\java\com\mycompany\myapp	Les répertoires sont différents
repository	src\main\java\com\mycompany\myapp	Les répertoires sont différents
security	src\main\java\com\mycompany\myapp	Les répertoires sont différents
service	src\main\java\com\mycompany\myapp	Les répertoires sont différents
web	src\main\java\com\mycompany\myapp	Les répertoires sont différents
resources	src\main	Les répertoires sont différents
webapp	src\main	Les répertoires sont différents
app	src\main\webapp	Les répertoires sont différents
admin	src\main\webapp\app	Les répertoires sont différents
admin.routes.ts	src\main\webapp\app\admin	Les fichiers de texte sont différents
core	src\main\webapp\app	Les répertoires sont différents
auth	src\main\webapp\app\core	Les répertoires sont différents
account.service.spec.ts	src\main\webapp\app\core\auth	Les fichiers de texte sont différents
account.service.ts	src\main\webapp\app\core\auth	Les fichiers de texte sont différents
user-route-access.service.ts	src\main\webapp\app\core\auth	Les fichiers de texte sont différents
interceptor	src\main\webapp\app\core	Les répertoires sont différents
auth-expired.interceptor.ts	src\main\webapp\app\core\interceptor	Les fichiers de texte sont différents
index.ts	src\main\webapp\app\core\interceptor	Les fichiers de texte sont différents
entities	src\main\webapp\app	Les répertoires sont différents
home	src\main\webapp\app	Les répertoires sont différents
home.component.html	src\main\webapp\app\home	Les fichiers de texte sont différents
home.component.spec.ts	src\main\webapp\app\home	Les fichiers de texte sont différents
home.component.ts	src\main\webapp\app\home	Les fichiers de texte sont différents
layouts	src\main\webapp\app	Les répertoires sont différents
login	src\main\webapp\app	Les répertoires sont différents
login.service.ts	src\main\webapp\app\login	Les fichiers de texte sont différents
app.routes.ts	src\main\webapp\app	Les fichiers de texte sont différents

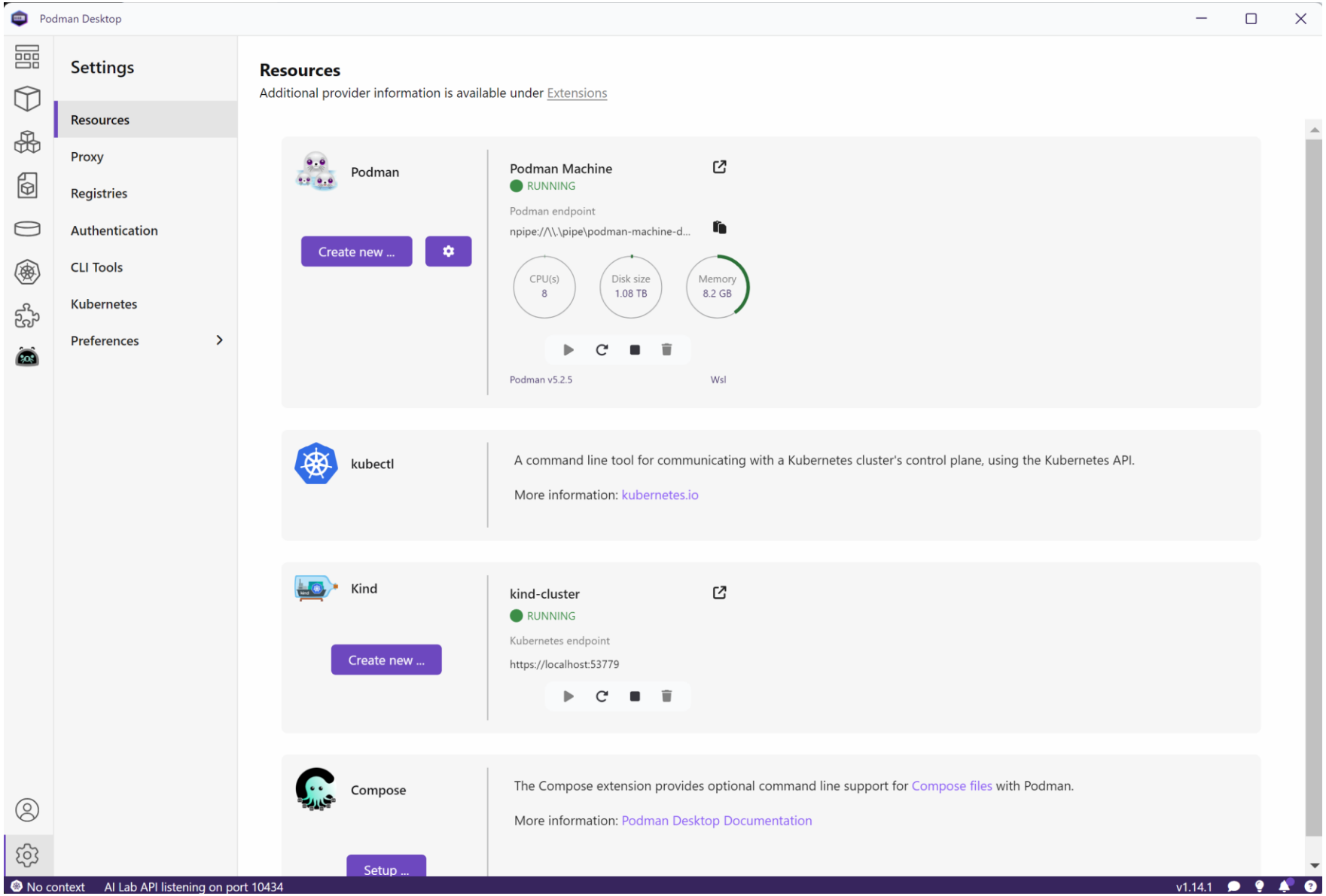
Launching Backend:
mvn -Pdev,tls spring-boot:run
(instead of mvn -Pdev spring-boot:run)
for https:// instead of http://

```
        at org.springframework.security.oauth2.client.registration.ClientRegistrations.getBuilder(ClientRegistrations.java:216)
        ... 74 common frames omitted
Caused by: java.net.ConnectException: Connection refused: getsockopt
        at java.base/sun.nio.ch.Net.pollConnect(Native Method)
        at java.base/sun.nio.ch.Net.pollConnectNow(Net.java:682)
        at java.base/sun.nio.ch.NioSocketImpl.timedFinishConnect(NioSocketImpl.java:542)
        at java.base/sun.nio.ch.NioSocketImpl.connect(NioSocketImpl.java:592)
        at java.base/java.net.Socket.connect(Socket.java:751)
        at java.base/sun.net.NetworkClient.doConnect(NetworkClient.java:178)
        at java.base/sun.net.www.http.HttpClient.openServer(HttpClient.java:531)
        at java.base/sun.net.www.http.HttpClient.openServer(HttpClient.java:636)
        at java.base/sun.net.www.http.HttpClient.<init>(HttpClient.java:280)
```

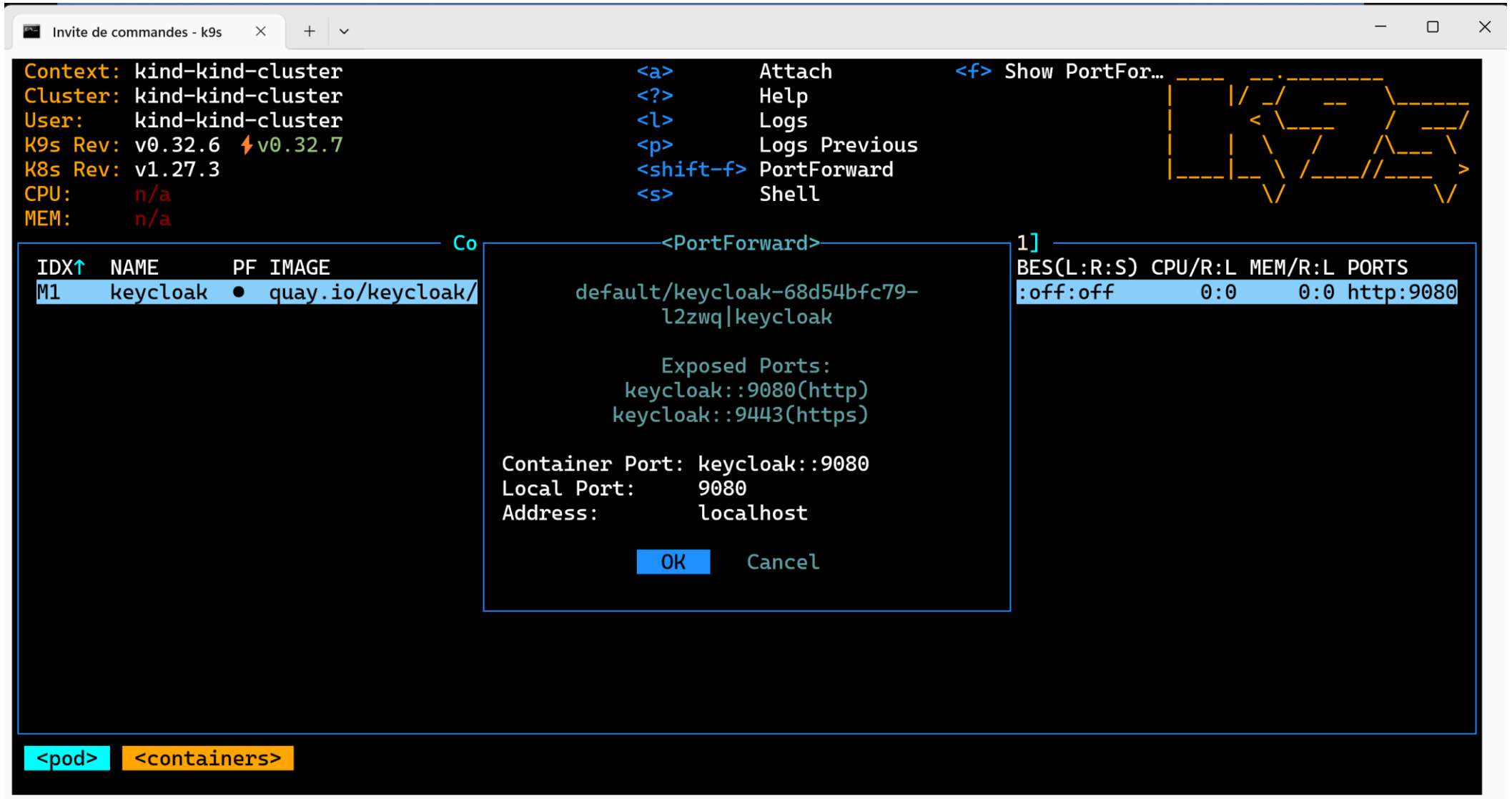
Need to Launch the OAuth2 Server https://jhipster.tech/security



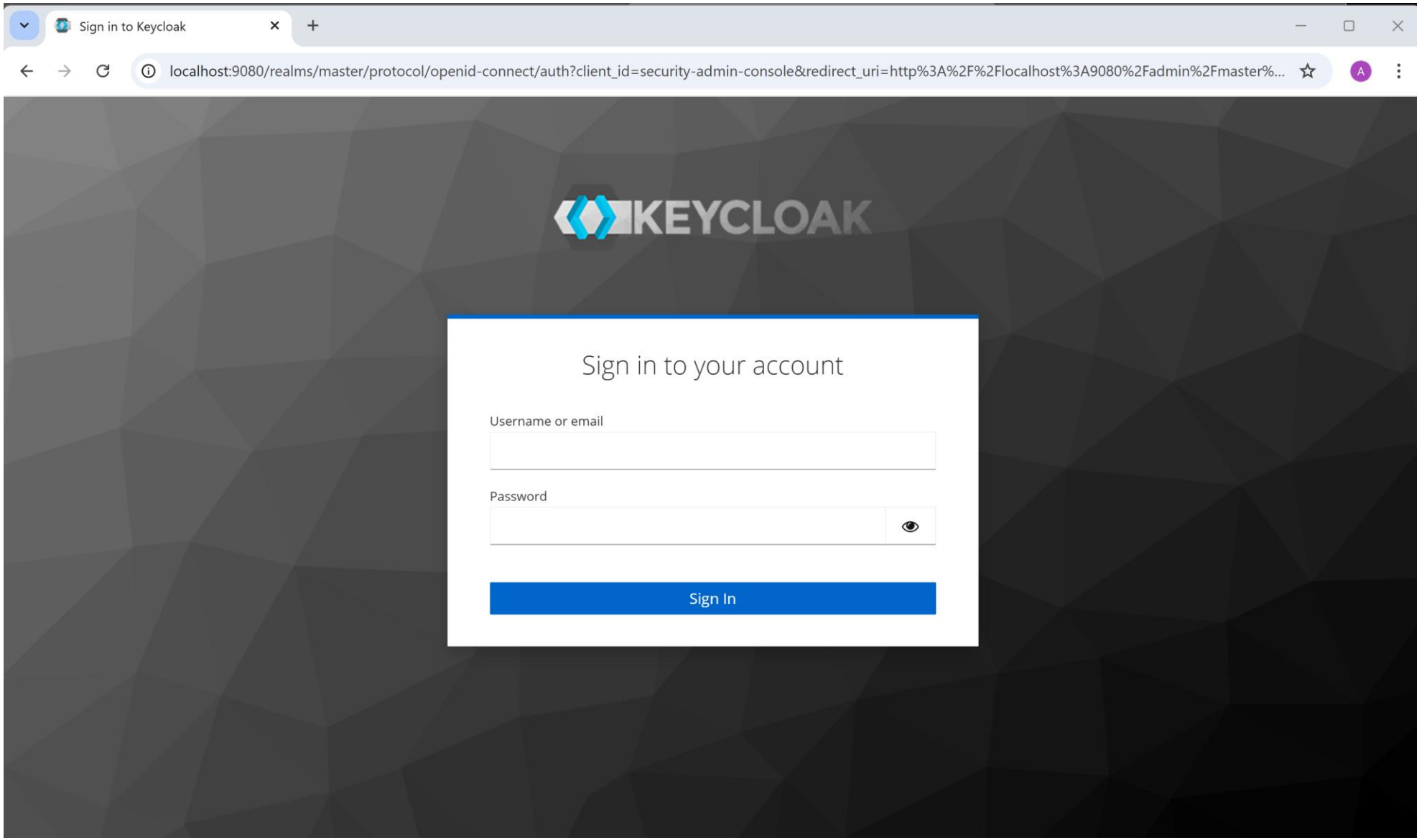
Starting Docker (Podman + Kubernetes)



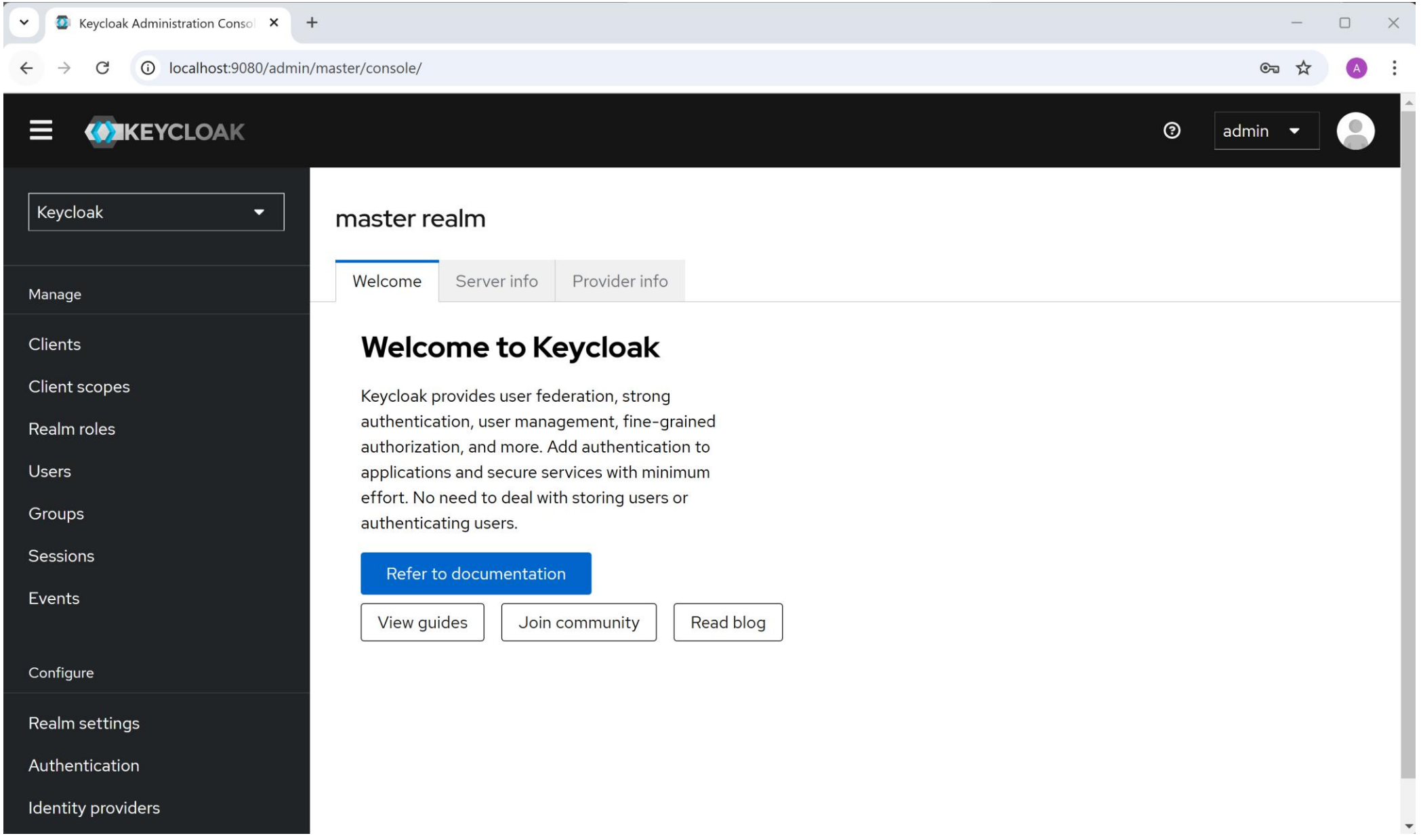
launched using Kubernetes + Port-Forward



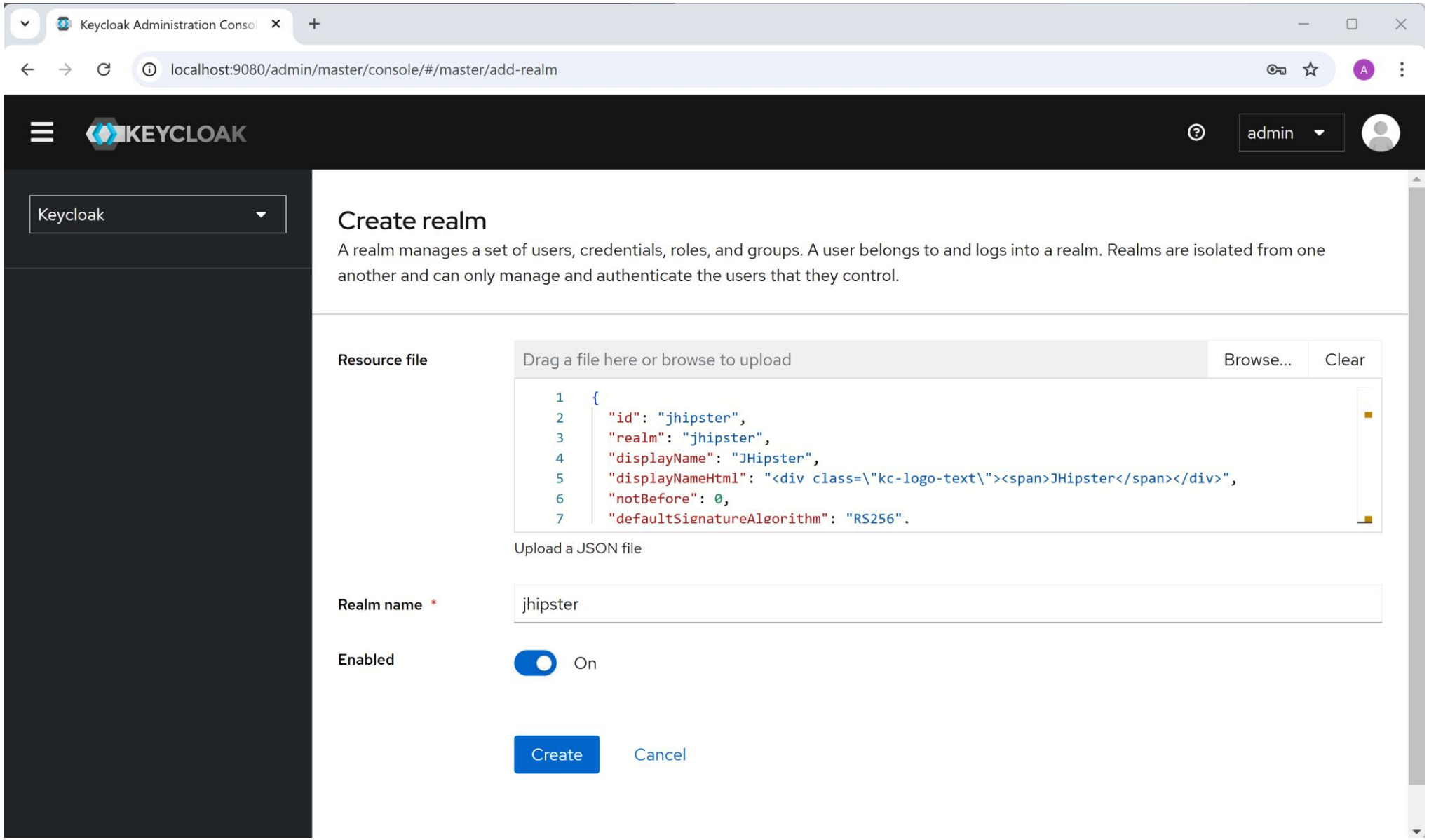
http://localhost:9080



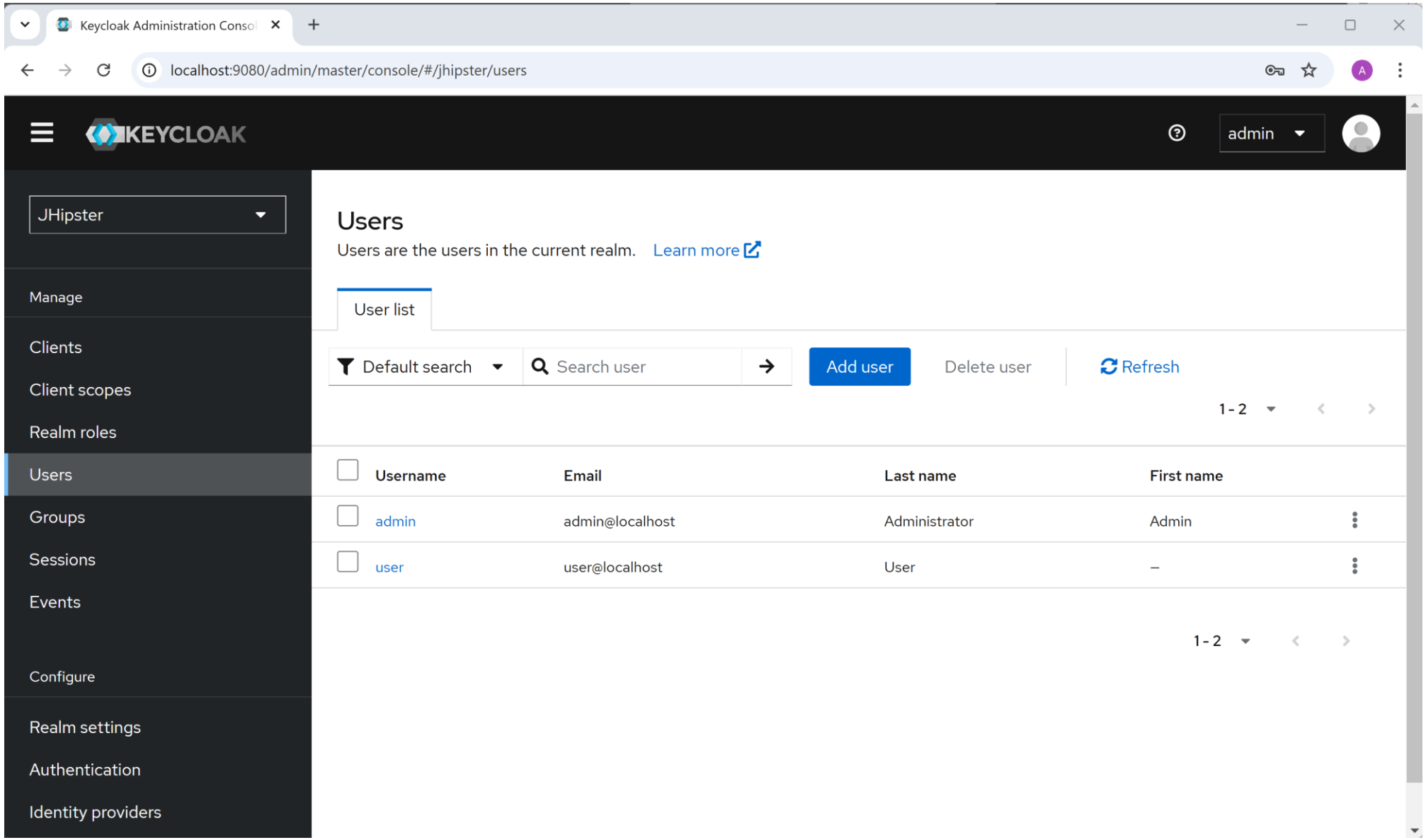
login admin/admin .. check "realm"



Create Realm - import jhipster-realm.json



JHipster Realm : users



Now can restart backend

```
$ mvn -Pdev,tls spring-boot:run
[INFO] Scanning for projects...
[INFO]
[INFO] ----------------------< com.mycompany.myapp:demo >----------------------
[INFO] Building Demo 0.0.1-SNAPSHOT
[INFO]   from pom.xml
[INFO] --------------------------------[ jar ]---------------------------------
[INFO]
[INFO] >>> spring-boot:3.3.5:run (default-cli) > test-compile @ demo >>>
```

```
2024-11-21T22:08:35.141+01:00  INFO 16532 --- [  restartedMain] t.j.s.ssl.UndertowSSLConfiguration       : Setting user cipher suite
 order to true
2024-11-21T22:08:35.236+01:00 DEBUG 16532 --- [  restartedMain] c.m.m.w.f.OAuth2RefreshTokensWebFilter   : Filter 'OAuth2RefreshToke
nsWebFilter' configured for use
2024-11-21T22:08:35.332+01:00  INFO 16532 --- [  restartedMain] org.jboss.threads                        : JBoss Threads version 3.5
.0.Final
2024-11-21T22:08:35.442+01:00  INFO 16532 --- [  restartedMain] com.mycompany.myapp.DemoApp              : Started DemoApp in 11.057
 seconds (process running for 11.636)
2024-11-21T22:08:35.458+01:00  INFO 16532 --- [  restartedMain] com.mycompany.myapp.DemoApp              :
----------------------------------------------------------
        Application 'demo' is running! Access URLs:
        Local:          https://localhost:8080/
        External:       https://172.24.224.1:8080/
        Profile(s):     [dev, api-docs, tls]
----------------------------------------------------------
```

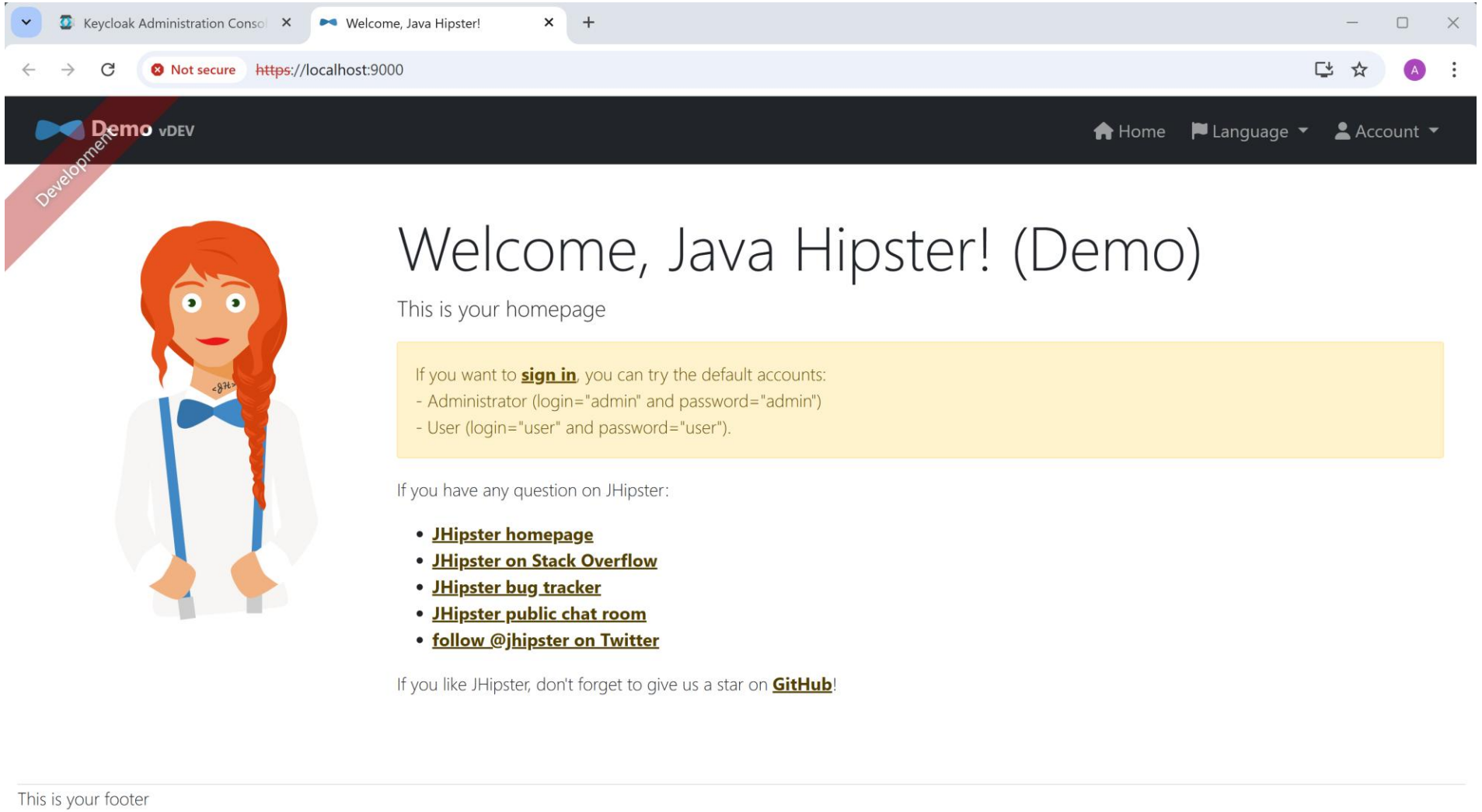
Launching Frontend:
ng serve --ssl (instead of "ng serve")

```
$ ng serve --ssl
Node.js version v23.2.0 detected.
Odd numbered Node.js versions will not enter LTS status and should not be used for production.
s://nodejs.org/en/about/releases/.
√ Browser application bundle generation complete.

Initial chunk files                                                                    | Names
```

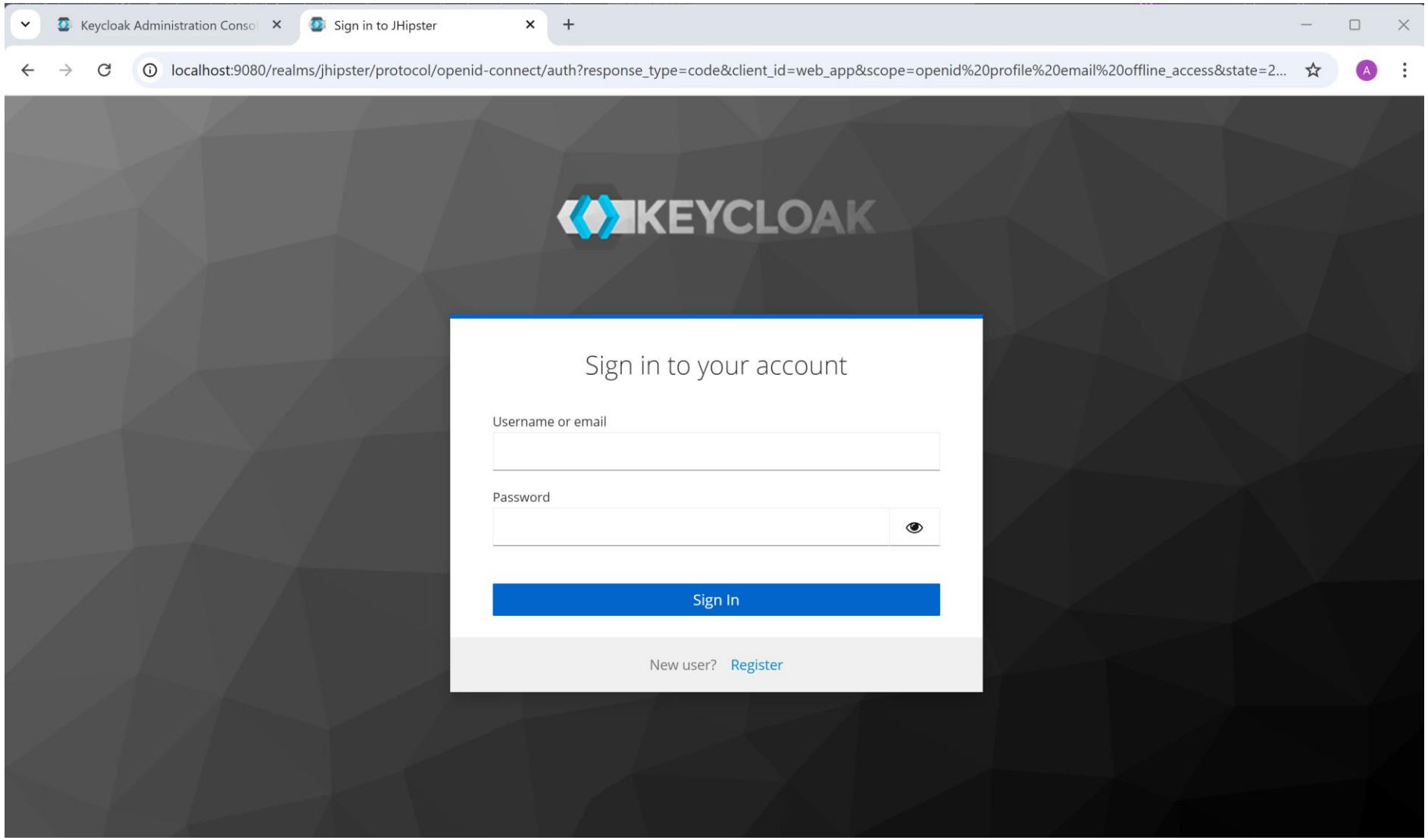
```
[Browsersync] Proxying: https://localhost:4200
[Browsersync] Access URLs:
 ------------------------------------
       Local: https://localhost:9000
    External: https://172.24.224.1:9000
 ------------------------------------
          UI: http://localhost:3001
 UI External: http://172.24.224.1:3001
 ------------------------------------
```

Home page: https://localhost:9000

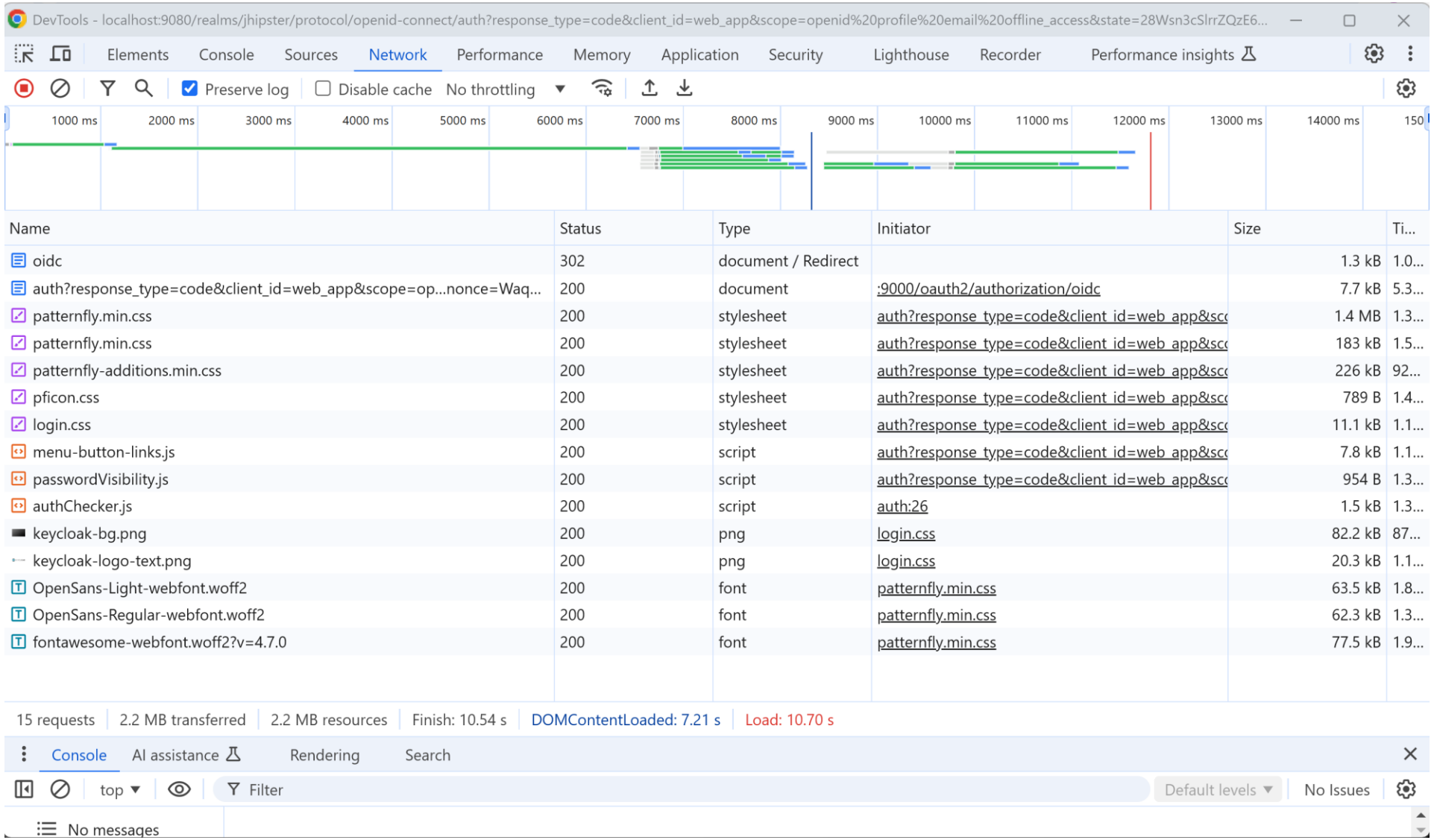


https:// using self-signed certificate => marked as "Not secure" by chrome

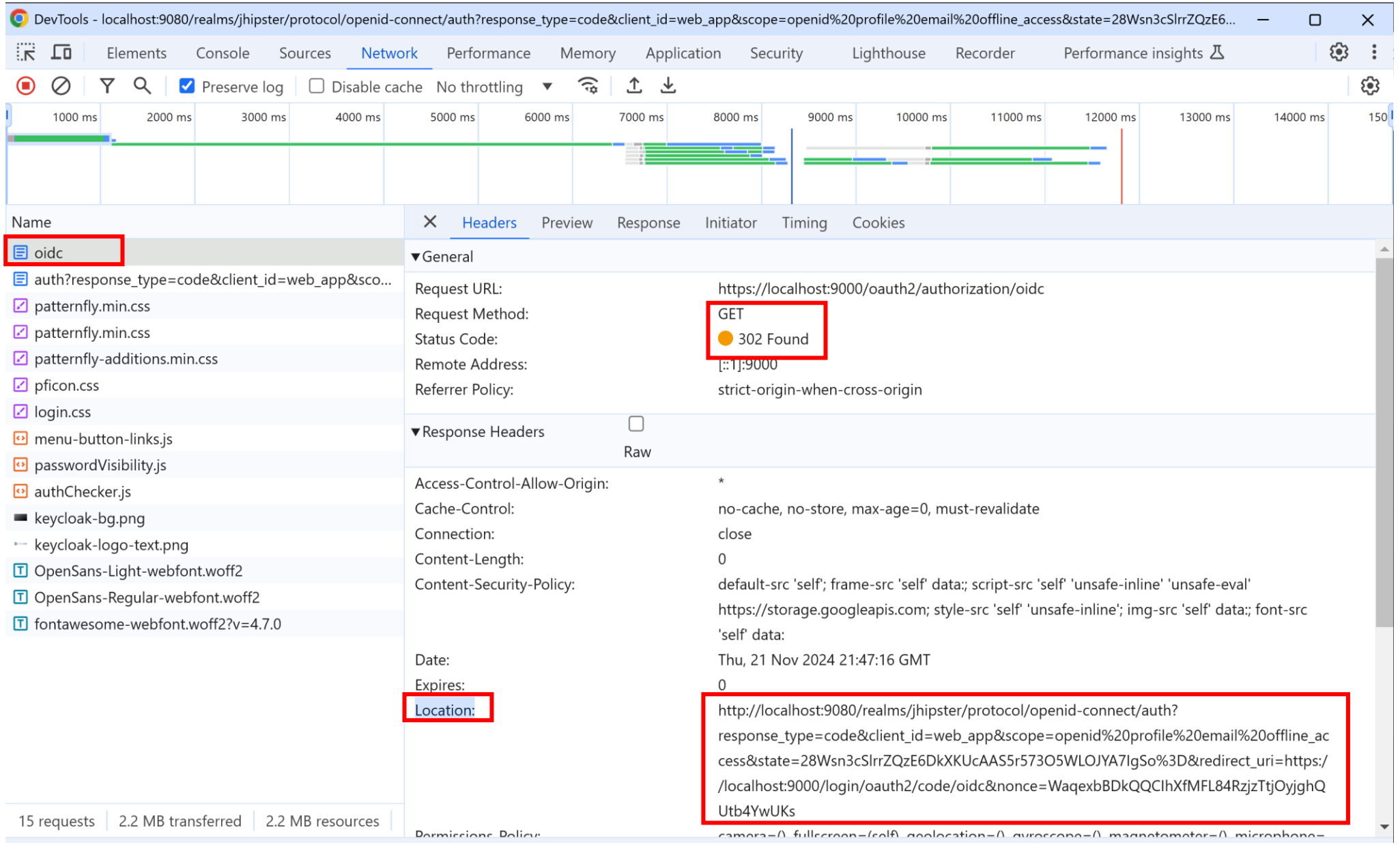
Click sign-in => redirect to login page of OAuth2



Http Request : check Chrome "Preserve Logs"



Request: Https GET "/oauth2/authorization/oidc"



Notice Http Status 303
+ Response Header "location"

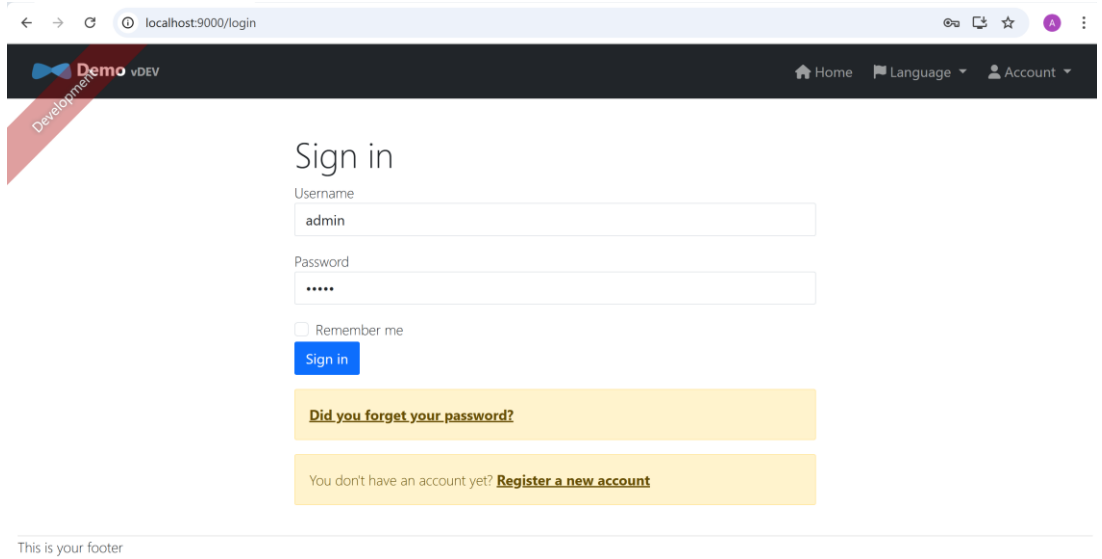
location =

http://localhost:9080/realms/jhipster/protocol/openid-connect/auth?
response_type=code
&**client_id**=web_app
&**scope**=openid%20profile%20email%20offline_access
&**state**=28Wsn3cSlrrZQzE6DkXKUcAAS5r573O5WLOJYA7IgSo%3D
&**redirect_uri**=https://localhost:9000/login/oauth2/code/oidc
&**nonce**=WaqexbBDkQQCIhXfMFL84RzjzTtjOyjghQUtb4YwUKs

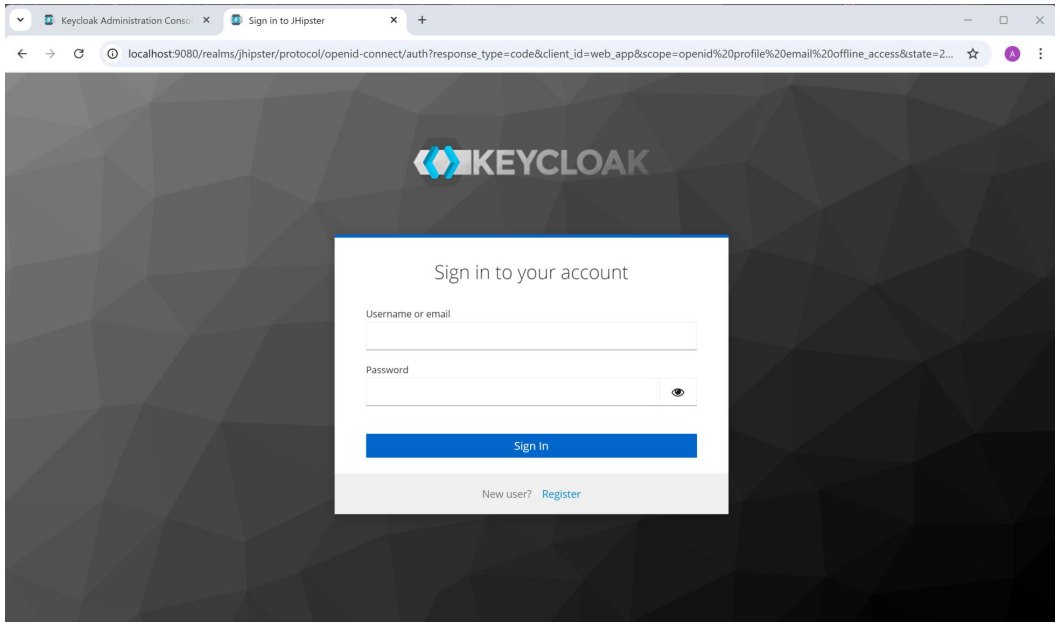
the location URL contains itself a "redirect_url" => back to origin web site after log-in

Comparison with "/login" page in JWT mode

"**JWT**" Mode ⟺ "**OAuth2**" Mode

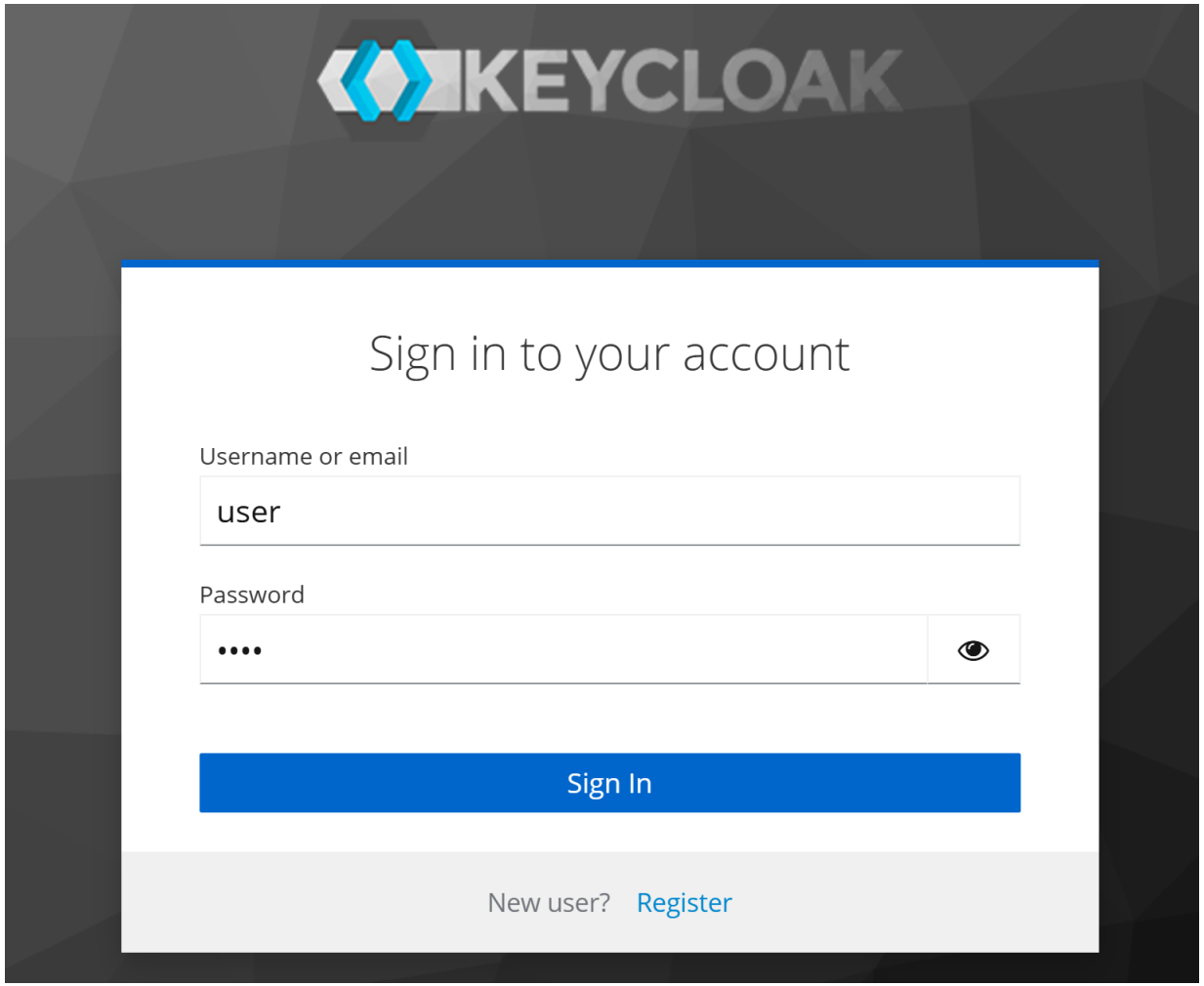


Login Page embedded in Webapp UI
(and user-passwords database in backend application)

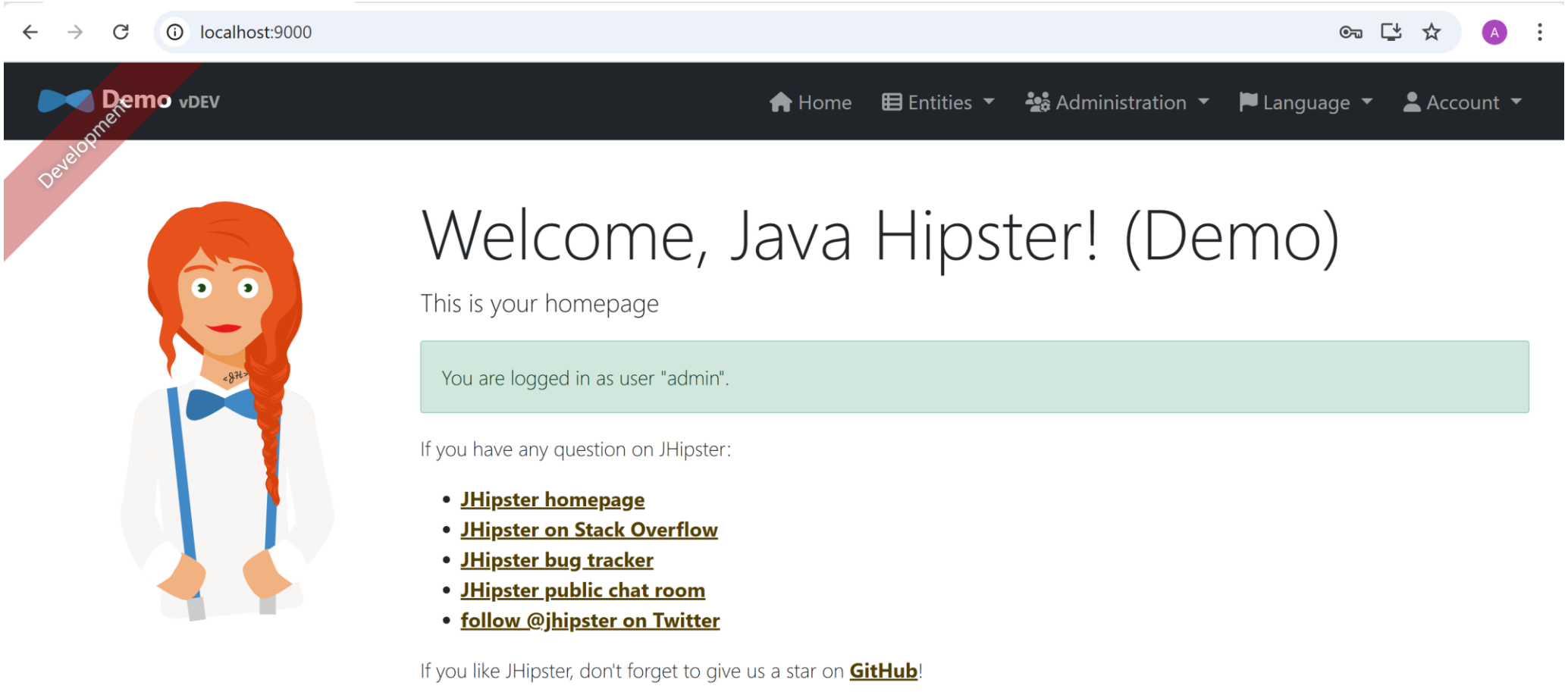


Login Page externalized in OAuth2 webapp UI
(and user-passwords database in OAuth2 application)

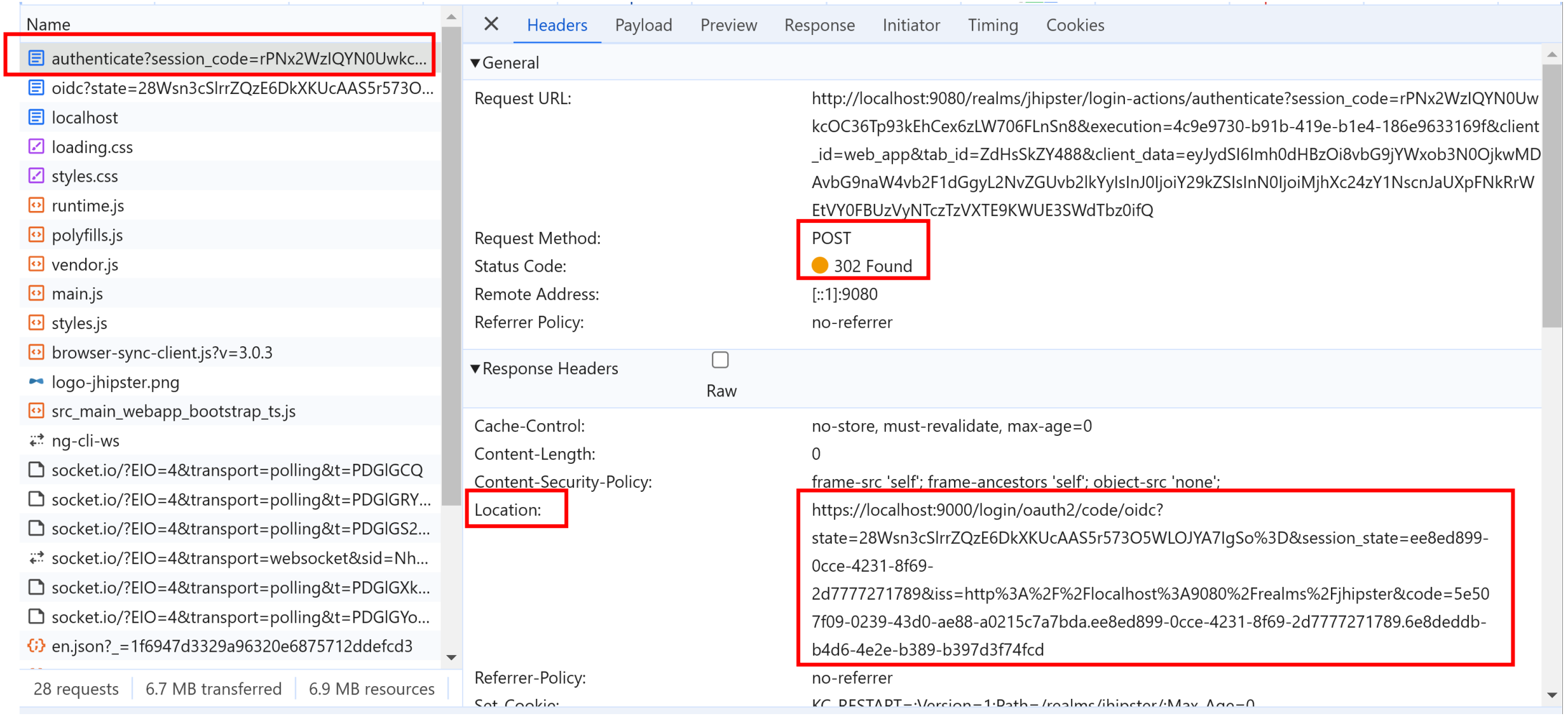
enter user-password (from OAuth2 Realm)



Home Page after logged-in
… redirected back to WebApp



Http POST /realms/jhipster/login-actions-authenticate



entering back to WebApp ... OAuth2 token

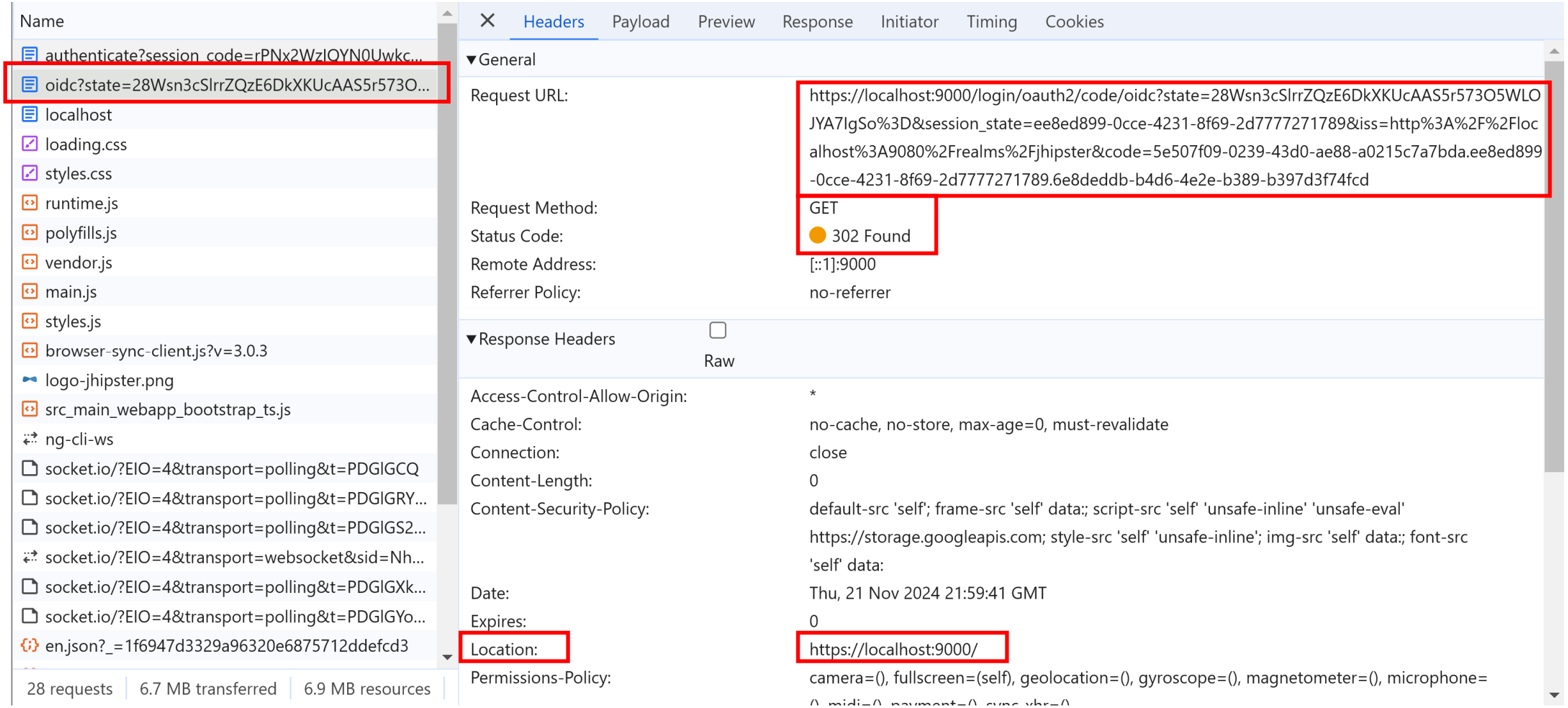
Location

https://localhost:9000/login/oauth2/code/oidc
?**state**=28Wsn3cSlrrZQzE6DkXKUcAAS5r573O5WLOJYA7IgSo%3D
&**session_state**=ee8ed899-0cce-4231-8f69-2d7777271789
&**iss**=http%3A%2F%2Flocalhost%3A9080%2Frealms%2Fjhipster
&**code**=5e507f09-0239-43d0-ae88-a0215c7a7bda.ee8ed899-0cce-4231-8f69-2d7777271789.6e8deddb-b4d6-4e2e-b389-b397d3f74fcd

parameter code ... is a OAuth2 Token (not exactly a JWT format!) : 5e50----bda . ee8e---1789 . 6e8de---74fcd

it does not contains a base64 characters, but also "-", like UUID

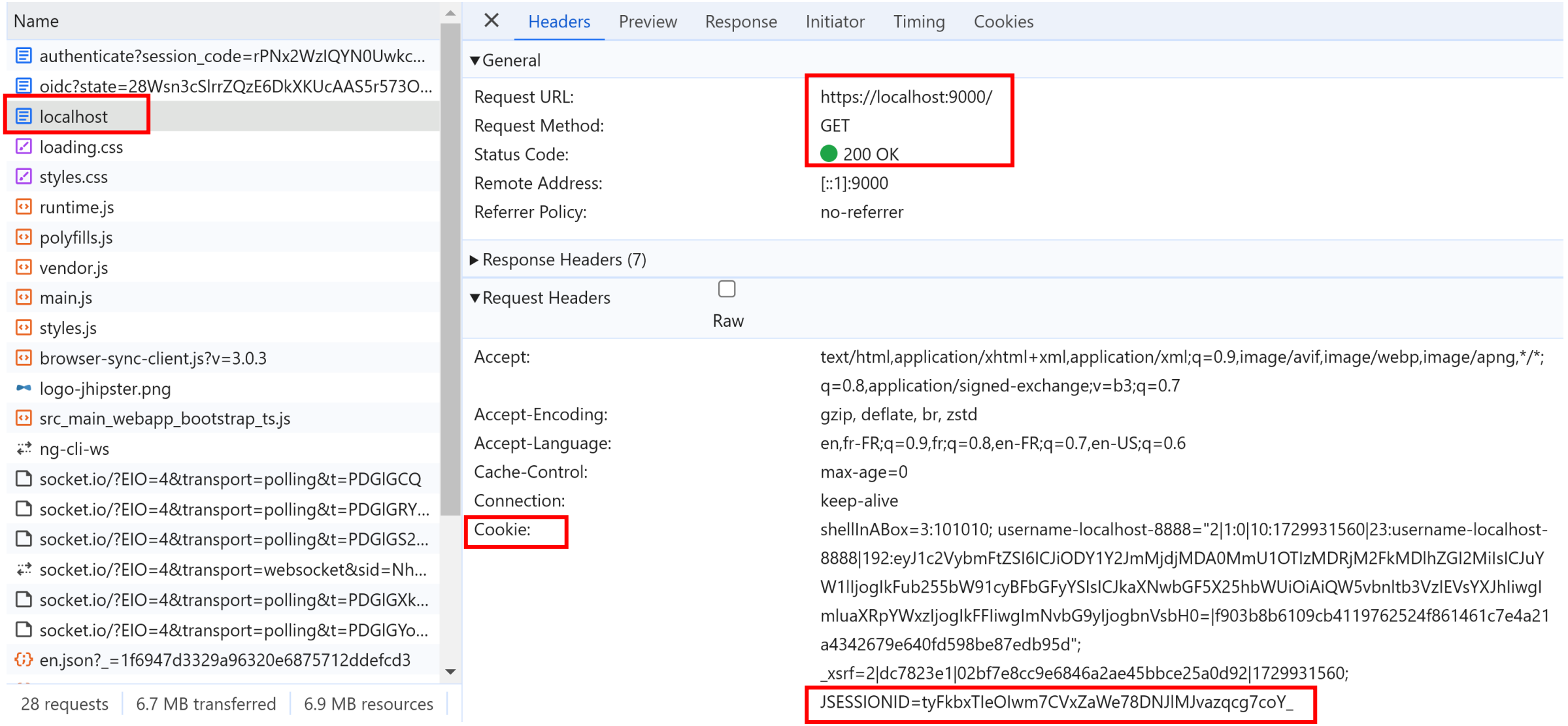
Another Request GET /login/auth2/code/oidc



OAuth2 token previously in Http Header "Location" => now passed as URL param

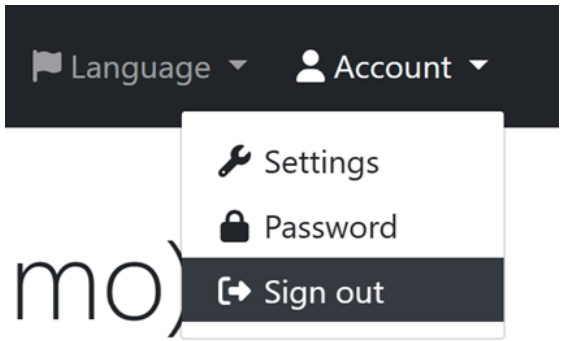
Request URL https://localhost:9000/login/oauth2/code/oidc
?**state**=28Wsn3cSlrrZQzE6DkXKUcAAS5r573O5WLOJYA7IgSo%3D
&**session_state**=ee8ed899-0cce-4231-8f69-2d7777271789
&**iss**=http%3A%2F%2Flocalhost%3A9080%2Frealms%2Fjhipster
&**code**=5e507f09-0239-43d0-ae88-a0215c7a7bda.ee8ed899-0cce-4231-8f69-2d7777271789.6e8deddb-b4d6-4e2e-b389-b397d3f74fcd

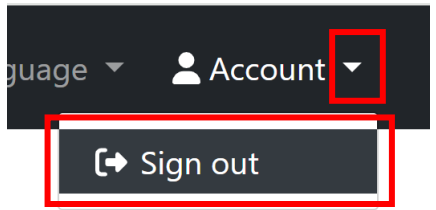
redirected to "/", with COOKIE JSESSIONID



Different Menu for Account Sub Menu Item "Sessions"

"**JWT**" Mode ⟺ "**OAuth2**" Mode





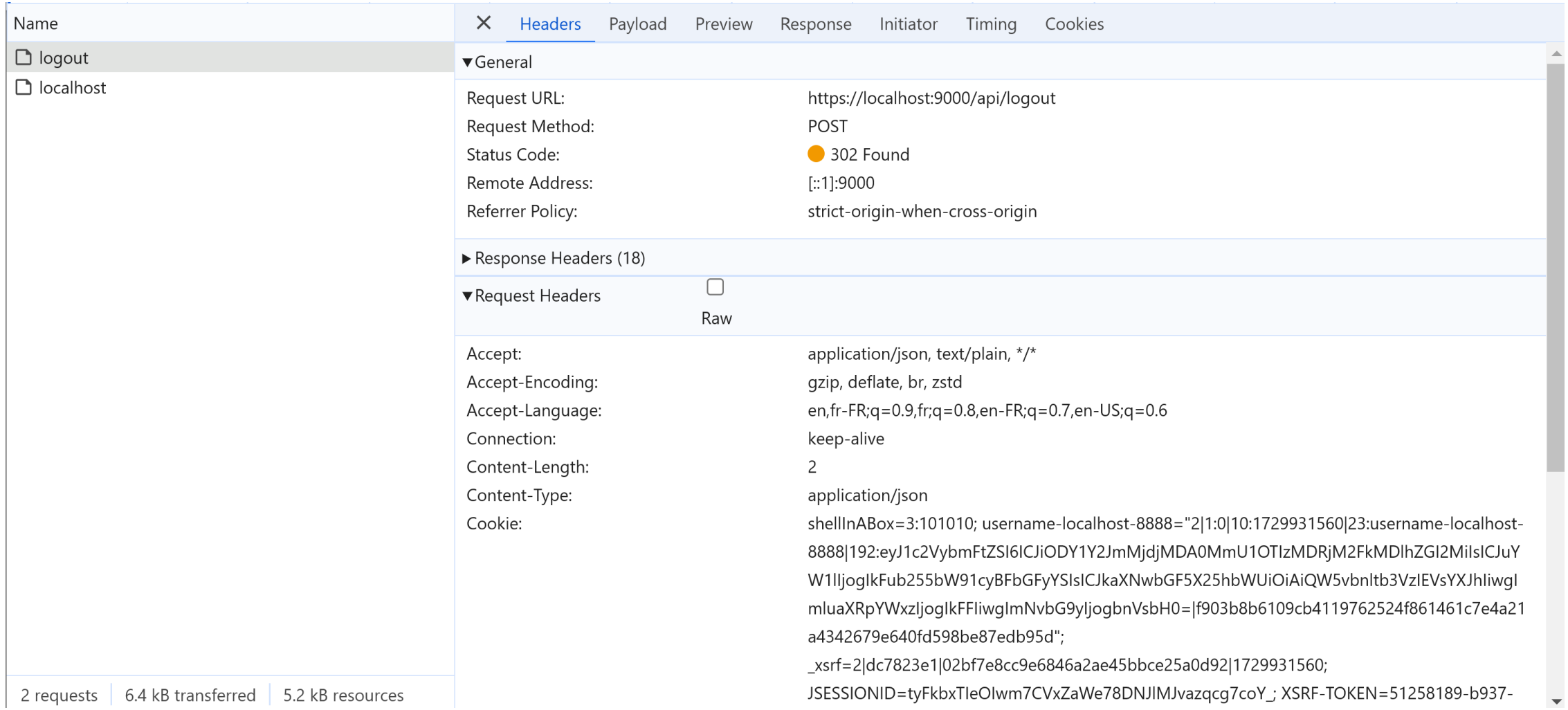
user and password is NO MORE stored on webapp
=> no more menu to save

cf OAuth2 app instead

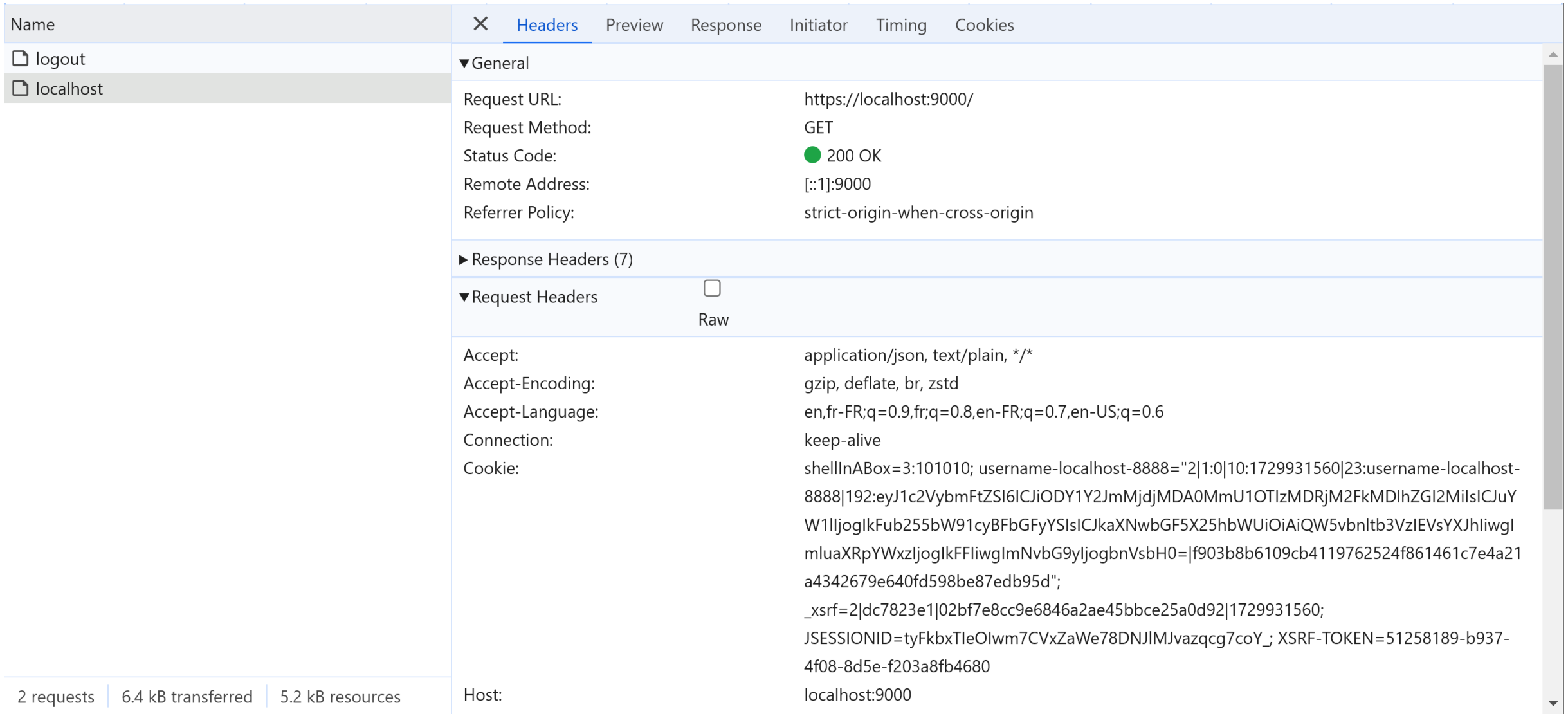
Click Sign-Out => 2 Requests

Name	Status	Type	Initiator
logout	302	xhr / Redirect	login.service.ts:19
localhost	200	xhr	logout

Http POST /logout



Redirected "/"


Name
logout
localhost
2 requests
6.4 kB transferred
5.2 kB resources
Headers
Preview
Response
Initiator
Timing
Cookies
General
Request URL:
https://localhost:9000/
Request Method:
GET
Status Code:
200 OK
Remote Address:
[::1]:9000
Referrer Policy:
strict-origin-when-cross-origin
Response Headers (7)
Request Headers
Raw
Accept:
application/json, text/plain, */*
Accept-Encoding:
gzip, deflate, br, zstd
Accept-Language:
en,fr-FR;q=0.9,fr;q=0.8,en-FR;q=0.7,en-US;q=0.6
Connection:
keep-alive
Cookie:
shellInABox=3:101010; username-localhost-8888="2|1:0|10:1729931560|23:username-localhost-8888|192:eyJ1c2VybmFtZSI6ICJiODY1Y2JmMjdjMDA0MmU1OTIzMDRjM2FkMDlhZGI2MiIsICJuYW1lIjogIkFub255bW91cyBFbGFyYSIsICJkaXNwbGF5X25hbWUiOiAiQW5vbnltb3VzIEVsYXJhIiwgImluaXRpYWxzIjogIkFFIiwgImNvbG9yIjogbnVsbH0=|f903b8b6109cb4119762524f861461c7e4a21a4342679e640fd598be87edb95d";
_xsrf=2|dc7823e1|02bf7e8cc9e6846a2ae45bbce25a0d92|1729931560;
JSESSIONID=tyFkbxTIeOIwm7CVxZaWe78DNJlMJvazqcg7coY_; XSRF-TOKEN=51258189-b937-4f08-8d5e-f203a8fb4680
Host:
localhost:9000

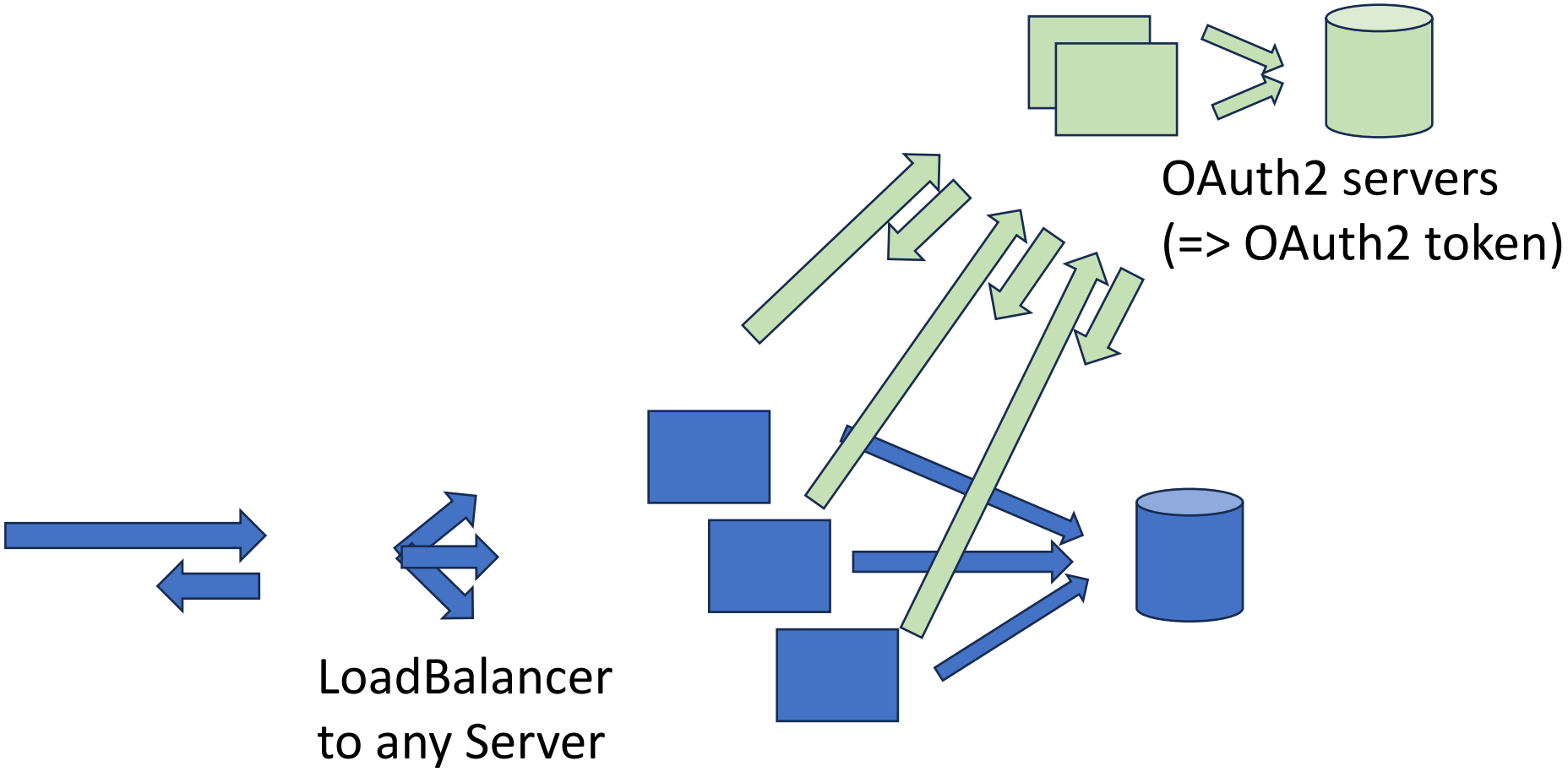
Authorisations

For Authorization (ROLE_*)
there is NO difference with the others mode JWT or Http SEssion.

Please see previous detailed document on JWT

Network & Infrastructure Deployments Options

Servers + OAuth2 Servers
(Statefull for JESSIONID- Need Database)



Take Away

[1/4]: Debugging "JWT" security mode
[2/4]: Debugging old-style COOKIE "jsessionId" security mode
[3/4]: Debugging "Basic Auth"
[4/4] Debugging the OAuth2 security mode

Security is difficult & sensitive - Leave it to experts.

Read code to learn in JHipster

Questions

arnaud.nauwynck@gmail.com