

Security

Een webapplicatie kan veel taken uitvoeren, sommige taken zijn voor iedereen toegestaan. Denk aan het aanpassen van de hotel adres of de prijzen van pizza's. Technisch wil je niet alle url's (bv `/admin/pizza/edit/6`) uitvoerbaar maken voor iedereen.

- 1 Je wil eerst weten wie deze url-aanroept (**authentication**)
- 2 En of hij de rechten hiervoor heeft (**authorization**)

We gaan een nieuwe applicatie aanmaken om dit te oefenen. De applicatie heeft vier pagina's.

- homepage
- registratie pagina
- inlog pagina
- homepage klant
- homepage admin

1 Maak een leeg project aan:

```
symfony new login_project --version=5.4 --webapp
```

2 Maak eerst een controller aan

```
php bin/console make:controller DefaultController
```

3 Maak een homepage met twee links naar inloggen en registreren

① 127.0.0.1:8001

Hello DefaultController!

This friendly message is coming from:

- Your login at [inloggen](#)
- Your registration at [registreren](#)

```
class DefaultController extends AbstractController
```

```
{  
  /**  
   * @Route("/", name="app_default")  
   */  
  public function index(): Response  
  {  
    return $this->render('default/index.html.twig', [  
      'controller_name' => 'DefaultController',  
    ]);  
  }  
  
  /**  
   * @Route("/login", name="login")  
   */  
  public function login(): Response  
  {  
    return new Response('login');  
  }  
  
  /**  
   * @Route("/register", name="register")  
   */  
  public function register(): Response  
  {  
    return new Response('register');  
  }  
}
```

```
{% extends 'base.html.twig' %}
```

```
{% block title %}Hello DefaultController!{% endblock %}
```

```
{% block body %}
```


```
<style>
```

```
.example-wrapper { margin: 1em auto; max-width: 800px; width: 95%;  
font: 18px/1.5 sans-serif; }
```

```
.example-wrapper code { background: #F5F5F5; padding: 2px 6px; }
```

```
</style>
```

```
<div class="example-wrapper">
```

```
  <h1>Hello {{ controller_name }}!  </h1>
```

```
  This friendly message is coming from:
```

```
  <ul>
```

```
    <li>Your login at <code><a href="{{ path('login')  
}}">inloggen</a></code></li>
```

```
    <li>Your registration at <code><a href="{{ path('register')  
}}">registreren</a></code></li>
```

```
  </ul>
```

```
</div>
```

```
{% endblock %}
```

4 Om een User entiteit te maken moeten we eerst de database aanmaken

```
DATABASE_URL="mysql://root:@127.0.0.1:3306/login_project?serverVersion=10.4.6-MariaDB&charset=utf8mb4"
```

```
php bin/console doctrine:database:create
```

5 We willen inloggen, daarvoor gaan we een user tabel maken. Hiervoor maken we eerst de entiteit aan met behulp van de makerbundle. (alle default waardes accepteren)

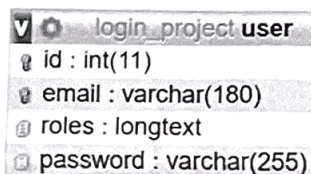
```
php bin/console make:user
```

6 Maak de migratie.

```
php bin/console make:migration
```

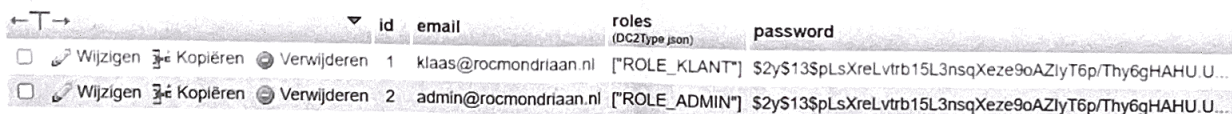
```
php bin/console doctrine:migrations:migrate
```

7 Bekijk de database



id	email	roles	password
int(11)	varchar(180)	longtext	varchar(255)

8 Voeg de volgende twee rijen toe aan de tabel 'user'.



	id	email	roles (DC2Type=json)	password
<input type="checkbox"/> Wijzigen <input type="checkbox"/> Kopiëren <input type="checkbox"/> Verwijderen	1	klaas@rocmondriaan.nl	["ROLE_KLANT"]	\$2y\$13\$SpLsXreLvtrb15L3nsqXeZe9oAZIyT6p/Thy6gHAHU.U...
<input type="checkbox"/> Wijzigen <input type="checkbox"/> Kopiëren <input type="checkbox"/> Verwijderen	2	admin@rocmondriaan.nl	["ROLE_ADMIN"]	\$2y\$13\$SpLsXreLvtrb15L3nsqXeZe9oAZIyT6p/Thy6gHAHU.U...

(password coderen met: `php bin/console security:hash-password`)

9 Nu gaan we de login pagina maken. Pas de login actie aan:

← → ↻ ⓘ 127.0.0.1:8001/login

Email: Password:

```

/**
 * @Route("/login", name="login")
 */
public function login(AuthenticationUtils $authenticationUtils): Response
{
    // get the login error if there is one
    $error = $authenticationUtils->getLastAuthenticationError();
    // last username entered by the user
    $lastUsername = $authenticationUtils->getLastUsername();
    return $this->render('default/login.html.twig', [
        'controller_name' => 'LoginController',
        'last_username' => $lastUsername,
        'error' => $error,
    ]);
}

```

```

{% extends 'base.html.twig' %}

{% block body %}
    {% if error %}
        <div>{{ error.messageKey|trans(error.messageData, 'security')}}</div>
    {% endif %}

    <form action="{{ path('login') }}" method="post">
        <label for="username">Email:</label>
        <input type="text" id="username" name="_username" value="{{ last_username }}" />

        <label for="password">Password:</label>
        <input type="password" id="password" name="_password" />

        {# If you want to control the URL the user is redirected to on
        success#}
        <input type="hidden" name="_target_path" value="/" />

        <button type="submit">login</button>
    </form>
{% endblock %}

```

In security.yaml

```

main:
    lazy: true
    provider: app_user_provider

    form_login:
        login_path: login
        check_path: login

```

10 Na succesvol inloggen wordt je doorverwezen naar de homepage. Onderaan staat dat je ingelogd bent.

Hello DefaultController! ✓

This friendly message is coming from:

- Your login at [inloggen](#)
- Your registration at [registreren](#)

Logged in as klaas@rocmondriaan.nl
Authenticated Yes
Roles ROLE_KLANT + 1 more
Token class UsernamePasswordToken
Firewall name main

127.0.0.1:8001/_profiler/928424?panel=security 3 4 klaas@roc 25 ms 1 Server 5.4.9

11 Na inloggen wil je ook kunnen uitloggen

Hello DefaultController! ✓

This friendly message is coming from:

- Your login at [inloggen](#)
- Your registration at [registreren](#)
- Your logout at [uitloggen](#)

200 @ app... 597 ms 2.0 MIB 3 4 n/a 23 ms

```

/**
 * @Route("/logout", name="logout")
 */
public function logout(): Response
{
    // controller can be blank: it will never be called!
    throw new \Exception('Don\'t forget to activate logout in
security.yaml');
}

```

In security.yaml

```

main:
    lazy: true
    provider: app_user_provider

    form_login:
        login_path: login
        check_path: login

    logout:
        path: logout

```

```

<ul>
    <li>Your login at <code><a href="{{ path('login')
}}>inloggen</a></code></li>
    <li>Your registration at <code><a href="{{ path('register')
}}>registreren</a></code></li>
    <li>Your logout at <code><a href="{{ path('logout')
}}>uitloggen</a></code></li>
</ul>

```

12 We willen nu acties gaan maken voor twee soorten gebruikers, de klant en de admin. Eerst maken we voor hun een controller aan.

```
php bin/console make:controller AdminController
```

```
php bin/console make:controller KlantController
```

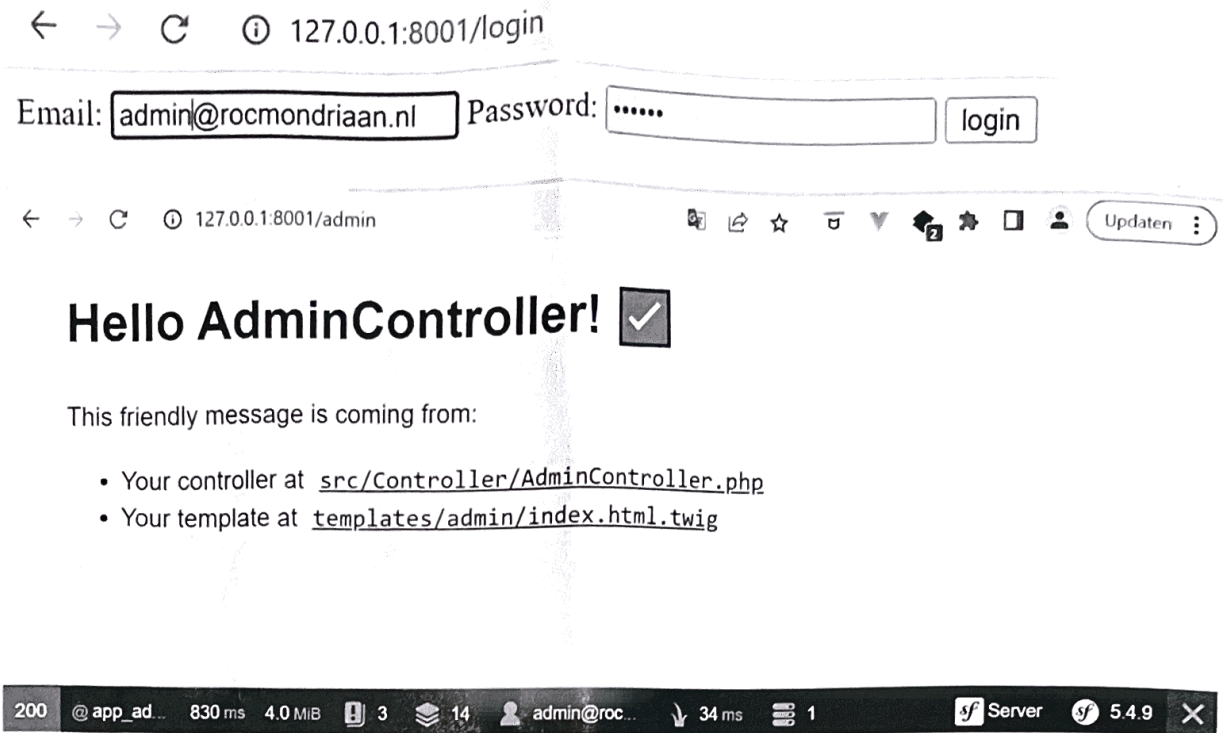
13 Nu gaan de pagina's van de admin en klant beveiligen

```

access_control:
    - { path: ^/admin, roles: ROLE_ADMIN }
    - { path: ^/klant, roles: ROLE_KLANT }

```

14 Nu zijn de pagina's beveiligd. Probeer maar /admin. De login pagina wordt getoond. Na inloggen en het verkrijgen van de ROLE_ADMIN kan je wel naar /admin.



15 Mooi dat je naar /admin (homepage) kan gaan, maar graag ga ik vanzelf na inloggen naar de homepage van admin of van klant

Verander in het loginformulier de route na succesvol inloggen

```
<input type="hidden" name="_target_path" value="/redirect"/>
```

Nu gaan we de route /redirect maken in de DefaultController

```
/**
 * @Route("/redirect", name="redirect")
 */
public function redirectAction(Security $security)
{
    if ($security->isGranted('ROLE_ADMIN')) {
        return $this->redirectToRoute('app_admin');
    }
    if ($security->isGranted('ROLE_KLANT')) {
        return $this->redirectToRoute('app_klant');
    }
    return $this->redirectToRoute('app_default');
}
```

Probeer nu in te loggen als klaas@rocmondriaan.nl (klant) en daarna als admin@rocmondriaan.nl en zie wat er gebeurt.

16 Toegang vanuit de twig

In de twig toegang tot bepaalde onderdelen:

```
{% if is_granted('IS_AUTHENTICATED_FULLY') %}  
    <a class="link" href="{{ path('logout') }}">Logout</a>  
  
{% else %}  
    <a class="link" href="{{ path('login_form') }}">Login</a>  
  
{% endif %}
```

Rol:

```
{% if is_granted('ROLE_USER') %}  
  
{% else %}  
  
{% endif %}
```