

**L'authentification :**

## Partie 1 : les fichiers

Il y a quelques fichiers à connaître :

Tout d'abord il y a le fichier **security.yaml**, qui se trouve dans config/packages.

Dedans on peut retrouver tout ce qui concerne la sécurité, c'est à dire, entre autre le " Provider " (Donc avec quel " Entity " on va se connecter, ici les " User " , et quel propriété on va utiliser en tant que pseudo, ici " username ".

Puis il y a le " firewalls " donc qui utilise le " Provider " et un autre fichier qui permet de vérifier si le bon pseudo et mot de passes sont rentrés. Puis il y a aussi le chemin de déconnexion.

```
security:
  encoders:
    App\Entity\User:
      algorithm: auto

  # https://symfony.com/doc/current/security.html#where-do-users-come-from-user-providers
  providers:
    # used to reload user from session & other features (e.g. switch_user)
    app_user_provider:
      entity:
        class: App\Entity\User
        property: username
  firewalls:
    dev:
      pattern: ^/(_(profiler|wdt)|css|images|js)/
      security: false
    main:
      anonymous: lazy
      provider: app_user_provider
      guard:
        authenticators:
          - App\Security\LoginFormAuthenticator
      logout:
        path: app_logout
        # where to redirect after logout
        # target: app_any_route
```

Puis dans **src/security/** il y a le fichier **LoginFormAuthenticator.php** Qui lui concerne la vérification du pseudo et du mot de passes qui sont rentrés. Le chemin sur lequel on renvoi l'utilisateur une fois qu'il est connecté. Normalement ce fichier n'est quasiment jamais touché, il est juste touché au début pour modifier le chemin vers lequel on renvoi l'utilisateur.

```
public function onAuthenticationSuccess(Request $request, TokenInterface $token, $providerKey)
{
    if ($targetPath = $this->getTargetPath($request->getSession(), $providerKey)) {
        return new RedirectResponse($targetPath);
    }

    // For example : return new RedirectResponse($this->urlGenerator->generate('some_route'));
    // throw new \Exception('TODO: provide a valid redirect inside '.__FILE__);
    return new RedirectResponse($this->urlGenerator->generate('homepage'));
}
```

Dans la même suite il y a le **SecurityController** dans **src/controller**. Il n'y a pas grand chose à en dire, il rend juste le formulaire de connexion avec les erreurs s'il y en a.

Et donc le dernier fichier qui est dans **templates/security/login.html.twig**. C'est le fichier avec le formulaire. Pas grand chose à en dire non plus, c'est de l'HTML et du TWIG.
















Les 2 derniers fichiers mentionnés ne sont pas modifiés, ils sont très bien comme ils sont de base quand ils sont automatiquement créés.

## Partie 2 : l'authentification

Donc c'est très simple, l'utilisateur va se retrouver sur **login.html.twig**, il va recevoir le formulaire devant lui et va donc rentrer ses informations. Une fois qu'il les envoie. C'est le **LoginFormController** qui va prendre la suite. Il va vérifier les informations, le token etc... Si tout est bon, l'utilisateur va se retrouver, pour notre cas, sur la page d'accueil du site, sinon il se retrouve sur la page de login avec les erreurs qu'il a commis (souvent le pseudo/mot de passe qui est erroné)

## Partie 3 : les utilisateurs

Alors les utilisateurs sont stockés tout simplement dans la base de données, ils ont entre autre un rôle qui est rajouté par l'authentification, ce qui permet de mieux les séparer quand on a besoin, par exemple pour une partie Admin.

|                          |   |        | id  | username | roles   | password  | email |        |                |  |
|--------------------------|---|--------|---|----------|---|-----------|-------|--------|----------------|--|
| <input type="checkbox"/> |  | Éditer |  | Copier   |  | Supprimer | 1     | User1  | []             | \$argon2id\$v=19\$m=65536,t=4,p=1\$WjNlbnJKLy5uNjRNUE5... User@user.test1  |
| <input type="checkbox"/> |  | Éditer |  | Copier   |  | Supprimer | 2     | User2  | []             | \$argon2id\$v=19\$m=65536,t=4,p=1\$M2hYXJdD3Yi96b3F... User@user.test      |
| <input type="checkbox"/> |  | Éditer |  | Copier   |  | Supprimer | 3     | User   | []             | \$argon2id\$v=19\$m=65536,t=4,p=1\$V3luOGdQNGhIQ2pKT3Z... User2@user.test  |
| <input type="checkbox"/> |  | Éditer |  | Copier   |  | Supprimer | 4     | Admin  | ["ROLE_ADMIN"] | \$argon2id\$v=19\$m=65536,t=4,p=1\$T3cxRG8vaWJVOTJlQm5... Admin@test.test  |
| <input type="checkbox"/> |  | Éditer |  | Copier   |  | Supprimer | 5     | Admin3 | ["ROLE_ADMIN"] | \$argon2id\$v=19\$m=65536,t=4,p=1\$REtnRjFtQVFuT2JEZWR... Admin3@test.test |