Document Technique rendu Serurité web

Il est important d'évité que n'importe qui ait accès à toutes les routes s'ils ne sont pas connectés.

Dès lors que vous arrivez sur le site vous devrez créer votre compte. Le compte aura un mot de passe crypté :

```
$user→setPassword(
    $userPasswordHasher→hashPassword(
        $user,
        $form→get('plainPassword')→getData()
    )
);
```

De plus les Accès admin sont possible depuis la page des utilisateurs mais en vérifiant le rôle de l'utilisateur donc si tu as le rôle admin.

```
<header><h1>Game Page</h1>

    {% if is_granted('ROLE_ADMIN') %}
        <a href="{{ path('app_game_dashboard') }}">Dashboard</a>
    {% endif %}

</header>
```

Dès lors que tu rentres dans l'espace administrateur tu as accès aux différents routes du Crud que sont la création, la suppression et la modification .

Chaque route vérifie que tu es bien un administrateur. Tout d'abord par le Middleware :

```
access_control:
     - { path: ^/game/dashboard, roles: ROLE_ADMIN }
     - { path: ^/game/edit, roles: ROLE_ADMIN }
     - { path: ^/game/new, roles: ROLE_ADMIN }
     - { path: ^/game/delete, roles: ROLE_ADMIN }
     - { path: ^/game, roles: ROLE_USER }
```

Et ensuite directement dans les routes :

```
$user = $this->getUser();
if ($user === null) {
    return $this->redirectToRoute( route: 'app_login');
}
elseif ($user->getRoles()[0] !== 'ROLE_ADMIN') {
    return $this->redirectToRoute( route: 'app_game');
}
```

Dès le moment ou on cherche à supprimer un article on vérifie son certificat CSRF pour s'assurer qu'il a bien les autorisations nécessaire pour la suppression :

```
if ($this->isCsrfTokenValid( id: 'delete'.$game->getId(), $r->request->get( key: 'csrf'))) {
```

Ethan Delcroix