Audit-code-symfony

1. Concernant les versionning :

   Dans le .gitignore le vendor est en commentaire.
   Cela signifie qu'il peut être versionné et donc que tout le monde peut y avoir accès pour éviter cela il faut le décommenter.

```
#/vendor/
```

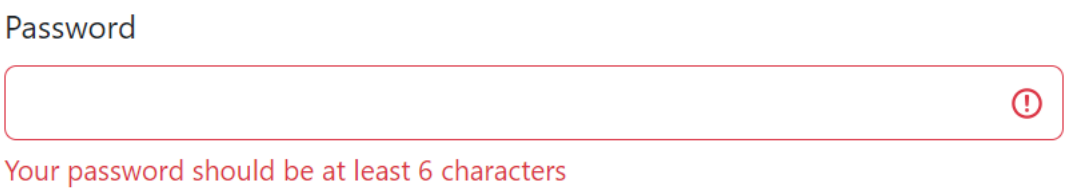
2. Dans le sécurity.yaml problème d'ACL

   Dans le access_control il y a un problème car les lignes sont commentées et donc on donne les accès de tout à tout le monde. Pour éviter ce problème de sécurité il faut attribuer à l'admin ce à quoi il doit avoir accès et au user ce à quoi il doit avoir accès, ainsi que décommenter les lignes.

```
access_control:
    # - { path: ^/admin, roles: ROLE_ADMIN }
    # - { path: ^/profile, roles: ROLE_USER }
```

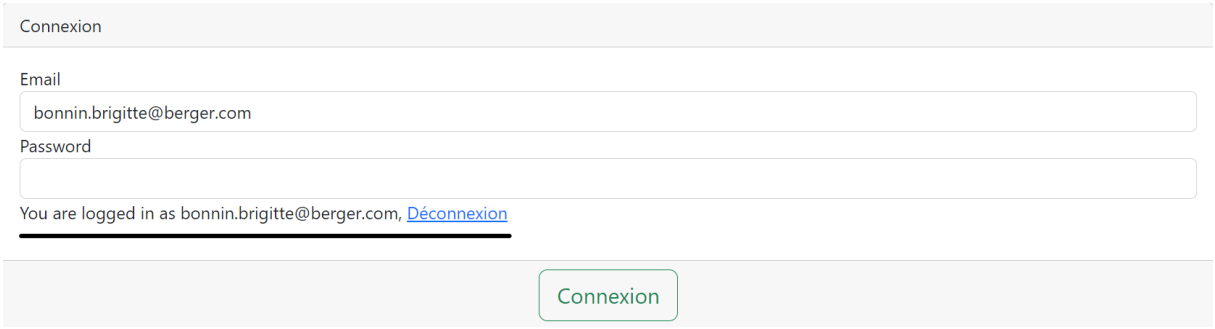
3. Concernant l'inscription depuis cette URL : http://localhost:8000/register

   Le mot de passe ne respecte pas les conditions d'un mot de passe sécurisé car il nécessite uniquement 6 caractères au minimum alors qu'il faudrait suivre les conditions suivantes : au minimum 12 caractères, une majuscule, une minuscule, un caractère spécial et un chiffre. Pour éviter des problèmes de sécurité de ce type il faudrait mettre en place ces conditions de mot de passe.



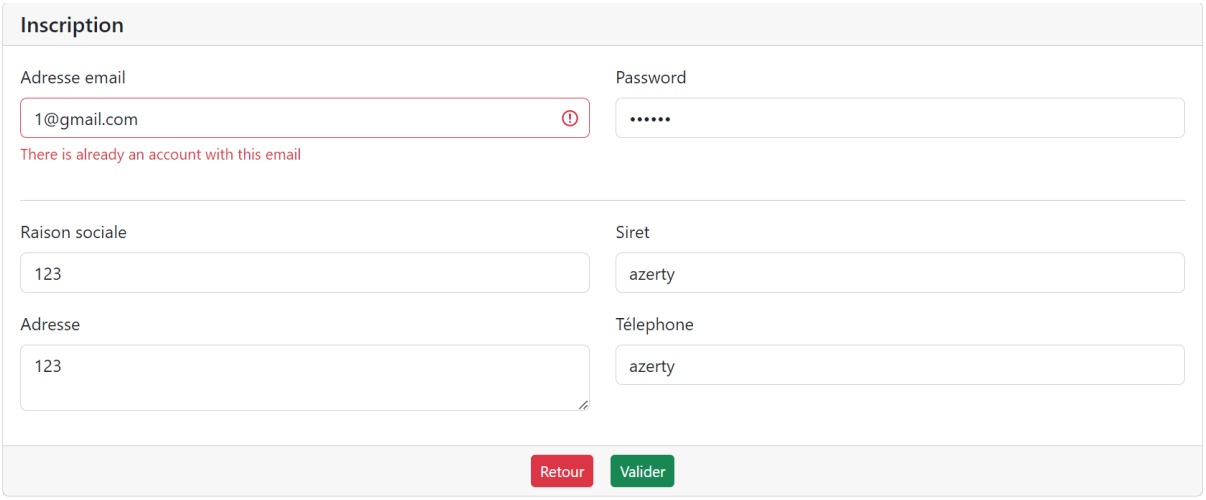
4. Concernant la connexion depuis cette URL : http://localhost:8000/login

   Il y a un problème de sécurité car le dernier compte à être connecter reste connecté et ne se déconnecte pas automatiquement si une personne oublie de le faire, il faudrait faire en sorte qu'après un certain temps la personne est automatiquement déconnecté.



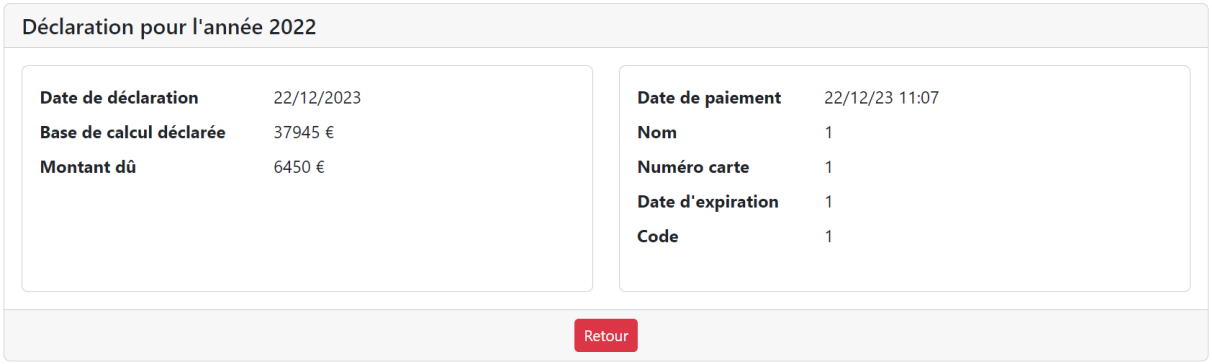
5. Manque d'assert :

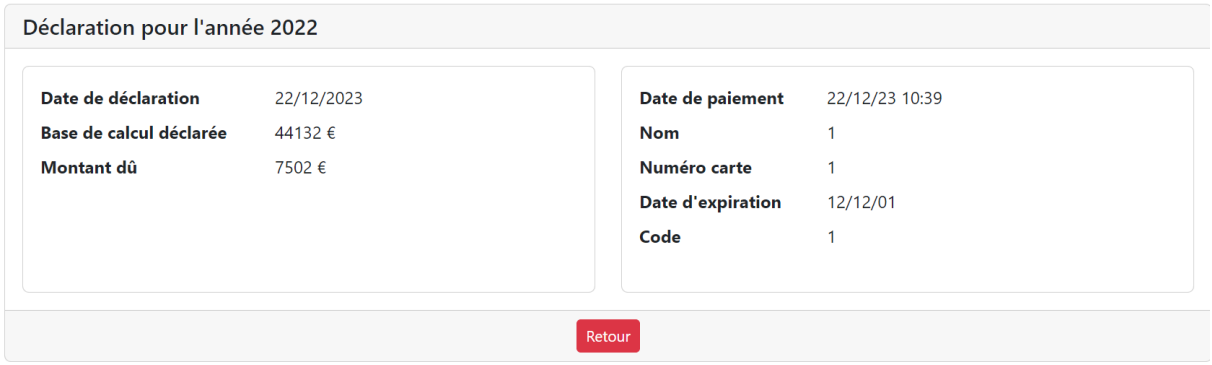
   Il manque des assert dans plusieurs endroits que ce soit dans l'inscription d'un utilisateur, dans le payement… des types String sont acceptées alors que on devrait attendre un type Int par exemple ici : un numéro de Siret est censé être composé de chiffres, avec un certain nombre de chiffres, pareil pour le numéro de téléphone, l'adresse… rien n'est vérifié. Pour solutionner cela il faudrait mettre en place dans les entity des assert.



6. Il y a un problème dans les déclarations

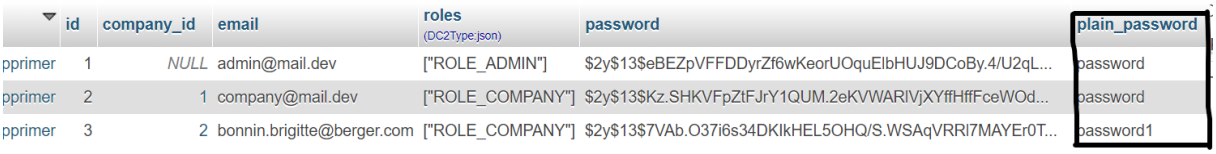
Comme constater ci-dessous on peut payer avec une carte qui a un nom contenant des chiffres, ce qui n'existe pas, on peut rentrer un numéro de carte avec un chiffre, on peut insérer une date qui n'existe même pas. Par conséquent n'importe qui peut payer avec n'importe quelle carte sans que rien ne soit vérifié. Il faudrait donc rajouter des assert mais aussi vérifier la date d'expiration de la date car ils acceptent les dates dépassés (capture 2)





7. Dans la BDD les mots de passe sont en plain_password

Toutes personnes ayant accès à la BDD peut avoir accès aux mots de passes des utilisateurs. C'est un problème de RGPD. Il faudrait donc supprimer la possibilité de visionner cela pour éviter tout problèmes de RGPD.



	id	company_id	email	roles (DC2Type:json)	password	plain_password
pprimer	1	NULL	admin@mail.dev	["ROLE_ADMIN"]	$2y$13$eBEZpVFFDDyrZf6wKeorUOquElbHUJ9DCoBy.4/U2qL...	password
pprimer	2	1	company@mail.dev	["ROLE_COMPANY"]	$2y$13$Kz.SHKVFpZtFJrY1QUM.2eKVWARlVjXYffHffFceWOd...	password
pprimer	3	2	bonnin.brigitte@berger.com	["ROLE_COMPANY"]	$2y$13$7VAb.O37i6s34DKlkHEL5OHQ/S.WSAqVRRI7MAYEr0T...	password1

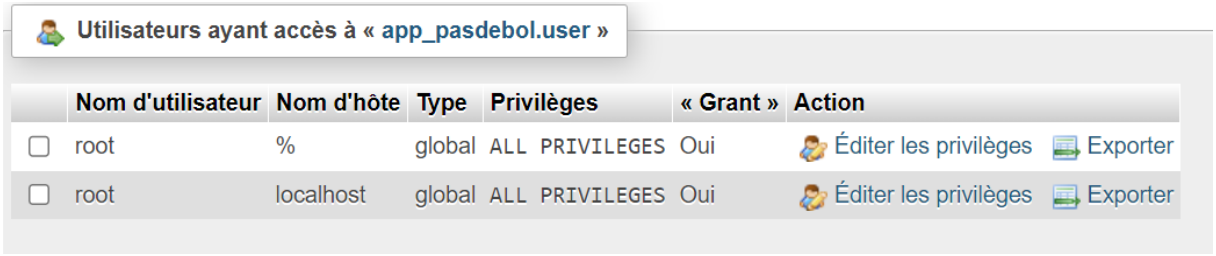
8. Accès à la BDD non sécurisé

   L'accès à la BDD ne nécessite pas de mot de passe donc en mettant root en utilisateur tout le monde peut avoir accès à la bdd. Ce qui est dangereux car tout le monde peut avoir accès aux mots de passes et aux informations des utilisateurs… Pour éviter cela il faut mettre un mot de passe en place respectant les bonnes conditions pour un mot de passe.

```
DATABASE_URL="mysql://root:@127.0.0.1:3306/app_pasdebol?serverVersion=mariadb-10.5.8&charset=utf8mb4"
```

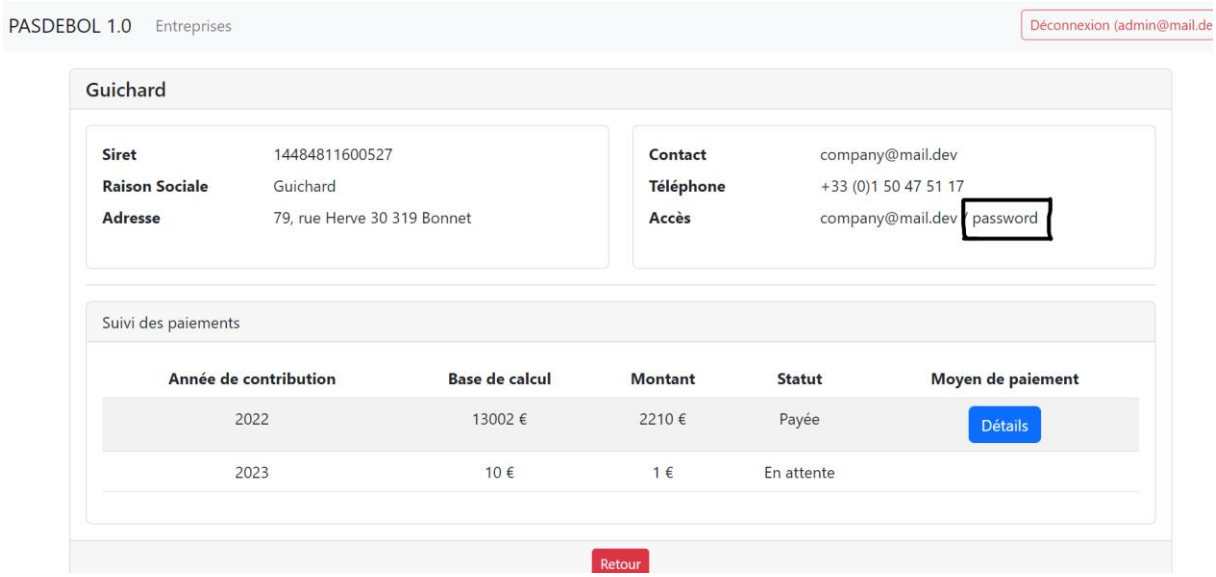
9. Dans les privilèges de la BDD

   On peut voir que root a tous les accès ce qui n'est pas du tout sécuriser. Il faut donner les bons accès aux bonnes personnes éviter des problèmes de sécurité.



10. Dans les fiches détaillées auxquels les admins ont accès :

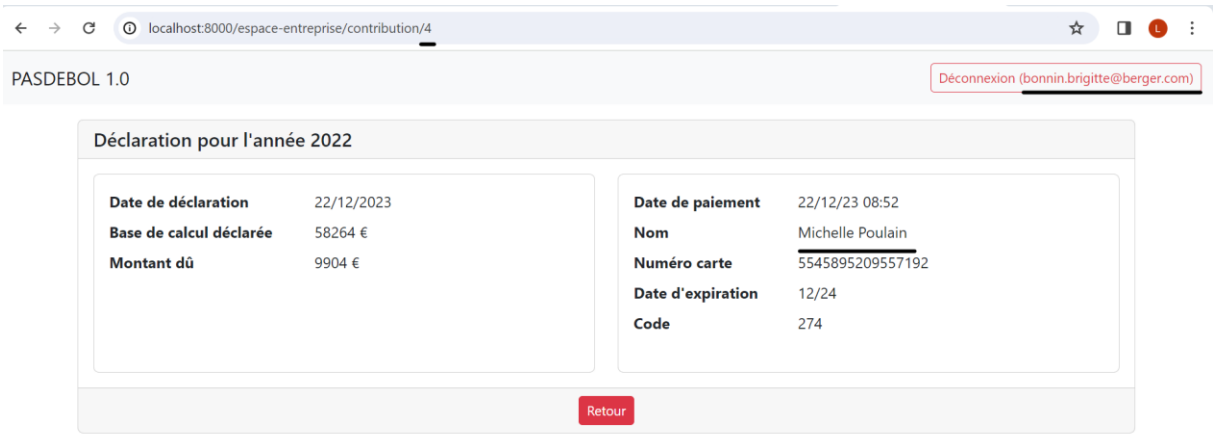
    Ils ont accès depuis le détail du client à son mot de passe, ce qui est un problème de RGPD. Il suffit qu'une personne mal attentionnée accède à cet endroit elle aura toutes les informations pour se connecter au compte du client. Il faudrait donc que le mot de passe ne soit pas affiché.



11. Problème de cloisonnement des espaces :

Non cloisonnement des espaces users et admin. Lorsqu'un user est connecté et regarde ses déclarations avec l'URL suivante : http://localhost:8000/espace-entreprise/contribution/2
le user peut accéder à ses déclarations comme on le voit si dessous :

Mais peut aussi changer l'Url en changeant l'id et accéder aux déclarations d'autres utilisateurs comme vu ci-dessous :



Ceci est un problème de sécurité, de RGPD. Pour remédier à cela il faut mettre l'id en paramètre dans le controller comme ca si l'utilisateur est connecté, on lui affiche les infos et si il n'est pas connecter au bon compte ca renvoi rien.

12. Dans le détail d’un moyen de paiement

Toutes personnes ayant accès à cela peut visionner le numéro de carte et le code de carte du client. Partons du principe que c’est un vrai numéro de carte pas comme celui en dessous et un vrai code. Le compte bancaire est très rapidement piraté… La RGPD n’est pas du tout respectée. Pour éviter cela il faudrait cacher la fin du numéro de carte bancaire et le code.