w.c.s. - Bug #5536

accesdenied lors d'une mauvaise signature (acces api)

18 septembre 2014 11:29 - Thomas Noël

Statut:	Fermé	**Début:**	18 septembre 2014
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	100%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	

Description

Lors d'un accès par signature (api.py), si ça ne marche pas on renvoie un utilisateur None.

Il serait utile quand on détecte une mauvaise signature, de faire un acces denied avec la raison (mauvaise signature, timestamp dépassé, etc).

Révisions associées

Révision 3074204f - 23 septembre 2014 12:23 - Benjamin Dauvergne

Make get_user_from_api_query_string() report detailed errors when signature checking fails (refs #5536)

Révision a9ac6fec - 23 septembre 2014 12:23 - Benjamin Dauvergne

Add tests for get_user_from_api_query_string() (fixes #5536)

Historique

#1 - 18 septembre 2014 11:55 - Benjamin Dauvergne

- Fichier 0001-Make-get_user_from_api_query_string-report-detailed-.patch ajouté

- Assigné à mis à Benjamin Dauvergne

- Patch proposed changé de Non à Oui

J'utilise AccessForbiddenError pour faire remonter le problème précis quand le champ signature est présent (sinon ça retourne None comme avant).

#2 - 18 septembre 2014 12:01 - Frédéric Péters

Pourquoi supprimer le fallback sur l'abance de paramètre algo= ?

```
    MAX_DELTA = 30
    if abs(delta) > datetime.timedelta(seconds=MAX_DELTAT):
```

Modif visiblement pas testée.

#3 - 18 septembre 2014 12:13 - Benjamin Dauvergne

Frédéric Péters a écrit :

> Pourquoi supprimer le fallback sur l'abance de paramètre algo= ?

Ça n'est pas sain: si une personne utilise SHA1 et ne précise pas d'algo cela va systématiquement faire une erreur de signature alors que c'est l'algorithme qui n'est pas le bon et que la signature est bonne en fait (i.e. elle est bien calculée). J'espère juste que rien n'en dépend pour l'instant.

> [...]
>
> Modif visiblement pas testée.

Je tâtais le terrain.

#4 - 18 septembre 2014 12:23 - Frédéric Péters

> Je tâtais le terrain.

Ok, sur une question particulière ? Parce que là Thomas fait le ticket, si c'est sur l'objet même du ticket qu'il y a hésitation, je ne vois pas le sens de faire un patch non testé.

#5 - 23 septembre 2014 11:41 - Benjamin Dauvergne

- Fichier 0001-Make-get_user_from_api_query_string-report-detailed-.patch ajouté

- Fichier 0002-Add-tests-for-get_user_from_api_query_string.patch ajouté

Patchs à jour testés avec des tests.

#6 - 23 septembre 2014 11:41 - Benjamin Dauvergne

```
(wcs)bdauvergne@fenouil:~/Code/wcs$ PYTHONPATH=$(pwd) py.test --run-postgresql tests/test_api.py
============================================================================================== test session s
tarts ==============================================================================================
platform linux2 -- Python 2.7.3 -- py-1.4.24 -- pytest-2.6.2
collected 1 items

tests/test_api.py .

=========================================================================================== 1 passed in 0.59
 seconds ============================================================================================
(wcs)bdauvergne@fenouil:~/Code/wcs$ fg
```

#7 - 23 septembre 2014 11:51 - Frédéric Péters

Il y a un "import sys" volant dans les tests; c'est mieux d'avoir une série de tests qu'un méga long test; par exemple,

```
...

def test_missing_algo():
    output = visit_page('/user?format=json&orig=coucou&signature=xxx')
    content = ''.join(output.generate_body_chunks())
    result = json.loads(content)
    assert result['err_desc'] == 'missing/multiple algo field'

def test_invalid_algo():
    output = visit_page('/user?format=json&orig=coucou&signature=xxx&algo=coin')
    content = ''.join(output.generate_body_chunks())
    result = json.loads(content)
    assert result['err_desc'] == 'invalid algo'

...
```

#8 - 23 septembre 2014 12:01 - Benjamin Dauvergne

- Fichier 0002-Add-tests-for-get_user_from_api_query_string.patch ajouté

Tests séparés, code nettoyé (plus de sus, et création du User et du site-options.cfg dans le setup).

#9 - 23 septembre 2014 12:20 - Frédéric Péters

Cool, ok.

#10 - 23 septembre 2014 12:24 - Benjamin Dauvergne

- Statut changé de Nouveau à Résolu (à déployer)

- % réalisé changé de 0 à 100

Appliqué par commit a9ac6fec89e41bfad4a88407c7bd85285be9bef8.

#11 - 23 septembre 2014 12:24 - Benjamin Dauvergne

- Statut changé de Résolu (à déployer) à Solution déployée

#12 - 23 septembre 2014 14:21 - Thomas Noël

- Statut changé de Solution déployée à Résolu (à déployer)

#13 - 22 décembre 2014 14:07 - Thomas Noël

- Statut changé de Résolu (à déployer) à Fermé

Fichiers

0001-Make-get_user_from_api_query_string-report-detailed-.patch	3,5 ko 18 septembre 2014	Benjamin Dauvergne
0001-Make-get_user_from_api_query_string-report-detailed-.patch	3,5 ko 23 septembre 2014	Benjamin Dauvergne
0002-Add-tests-for-get_user_from_api_query_string.patch	6,13 ko 23 septembre 2014	Benjamin Dauvergne
0002-Add-tests-for-get_user_from_api_query_string.patch	6,89 ko 23 septembre 2014	Benjamin Dauvergne