

w.c.s. - Bug #10923

Development # 10921 (Rejeté): api/wscall: ne pas transmettre les fichiers sous forme base64 mais via une URL

api: valider les nonces dans les signatures

13 mai 2016 14:26 - Benjamin Dauvergne

Statut:	Fermé	Début:	13 mai 2016
Priorité:	Bas	Echéance:	
Assigné à:	Benjamin Dauvergne	% réalisé:	0%
Catégorie:		Temps estimé:	0:00 heure
Version cible:		Planning:	
Patch proposed:	Oui		
Description			

Révisions associées

Révision c56fada4 - 27 mars 2017 12:57 - Benjamin Dauvergne

api: check signature's nonce (#10923)

It's mandatory to prevent replays. Request is marked as valid after the first check so that multiple call to `is_url_signed()` on the same request do not fail.

Tests had to be modified so they don't use the same signed URL for their web service calls.

Historique

#1 - 13 mai 2016 14:26 - Benjamin Dauvergne

- *Tracker changé de Development à Bug*

#2 - 13 mai 2016 16:50 - Benjamin Dauvergne

- *Fichier 0001-api-check-signature-s-nonce-10923.patch ajouté*

- *Patch proposed changé de Non à Oui*

#3 - 13 mai 2016 16:52 - Benjamin Dauvergne

- *Fichier 0001-api-check-signature-s-nonce-10923.patch supprimé*

#4 - 13 mai 2016 16:52 - Benjamin Dauvergne

- *Fichier 0001-api-check-signature-s-nonce-10923.patch ajouté*

Le cronjob pour nettoyer les nonces s'était perdu dans l'autre patch.

#5 - 15 mai 2016 08:04 - Benjamin Dauvergne

- *Fichier 0001-api-check-signature-s-nonce-10923.patch ajouté*

#6 - 16 septembre 2016 10:01 - Frédéric Péters

Tu aurais une version rebasée sur master ?

#7 - 16 septembre 2016 11:45 - Benjamin Dauvergne

- *Fichier 0001-api-check-signature-s-nonce-10923.patch ajouté*

Voilà, avec des bouts du [#10922](#), suffisamment pour que celui-ci s'applique. J'ai viré le sleep dans les tests qui faisait perdre 6s (à la place j'ai ajouté la possibilité de passer l'heure courante en paramètre à `clean_nonces()`). Je n'ai relancé que `tests/test_api.py` mais tout passe.

#8 - 24 mars 2017 11:40 - Benjamin Dauvergne

- *Fichier 0001-api-check-signature-s-nonce-10923.patch ajouté*

Rebasé et correction d'un bug suite au passage à pytest > 3 (pytest.raises() nettoie sys.exc_*, il faut utiliser la valeur renvoyer par le context manager à la place).

#9 - 27 mars 2017 09:51 - Frédéric Péters

```
def is_url_signed(utcnow=None, duration=DEFAULT_DURATION):
    if getattr(get_request(), 'signed', False):
        return True
```

Plutôt que le getattr(), ajouter l'attribut signed dans l'objet ?

#10 - 27 mars 2017 10:19 - Benjamin Dauvergne

- Fichier 0001-api-check-signature-s-nonce-10923.patch ajouté

```
diff --git a/wcs/api_utils.py b/wcs/api_utils.py
index eaef3fa..d5b61c8 100644
--- a/wcs/api_utils.py
+++ b/wcs/api_utils.py
@@ -33,7 +33,7 @@ DEFAULT_DURATION = 30

 def is_url_signed(utcnow=None, duration=DEFAULT_DURATION):
-     if getattr(get_request(), 'signed', False):
+     if get_request().signed:
         return True
         query_string = get_request().get_query()
         if not query_string:
diff --git a/wcs/qommon/http_request.py b/wcs/qommon/http_request.py
index 2cc4591..9efda02 100644
--- a/wcs/qommon/http_request.py
+++ b/wcs/qommon/http_request.py
@@ -24,6 +24,8 @@ from quixote.errors import RequestError
 from http_response import HTTPResponse

 class HTTPRequest(quixote.http_request.HTTPRequest):
+     signed = False
+
     def __init__(self, *args, **kwargs):
         quixote.http_request.HTTPRequest.__init__(self, *args, **kwargs)
         self.response = HTTPResponse()
```

#11 - 27 mars 2017 10:54 - Frédéric Péters

- Statut changé de Nouveau à En cours

Ack.

#12 - 27 mars 2017 12:58 - Benjamin Dauvergne

- Statut changé de En cours à Résolu (à déployer)

#13 - 23 décembre 2018 14:52 - Frédéric Péters

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

Fichiers

0001-api-check-signature-s-nonce-10923.patch	9,09 ko	13 mai 2016	Benjamin Dauvergne
0001-api-check-signature-s-nonce-10923.patch	9,19 ko	15 mai 2016	Benjamin Dauvergne
0001-api-check-signature-s-nonce-10923.patch	12,5 ko	16 septembre 2016	Benjamin Dauvergne
0001-api-check-signature-s-nonce-10923.patch	12,5 ko	24 mars 2017	Benjamin Dauvergne
0001-api-check-signature-s-nonce-10923.patch	13 ko	27 mars 2017	Benjamin Dauvergne