Authentic 2 - Development #47900

corriger le retour d'erreur client oidc

20 octobre 2020 19:41 - Frédéric Péters

Statut:	Fermé	**Début:**	20 octobre 2020
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

```
    client = authenticate_client(request, client=oidc_code.client)
    if client is None:
        return HttpResponse('unauthenticated', status=401)
```

Mais de la spécification https://tools.ietf.org/html/rfc6749#section-5.2 ce code "unauthenticated" n'existe pas.

Révisions associées

Révision a8214192 - 04 décembre 2020 11:21 - Benjamin Dauvergne

idp_oidc: improve error reporting in token endpoint (#47900)

Révision 34e8ca3f - 04 décembre 2020 11:21 - Benjamin Dauvergne

idp_oidc: correctly load session in OIDCCode and OIDCAccessToken (#47900)

- access_token can be valid without a session or with a session linked to the user
- code is only valid with a live session linked to its user
- session was not loaded correctly, it's only loaded after accessing its content, and session_key is only checked if the session is loaded.

Révision 21363956 - 04 décembre 2020 11:21 - Benjamin Dauvergne

idp_oidc: add a simple oidc client fixture (#47900)

Révision 380215ff - 04 décembre 2020 11:21 - Benjamin Dauvergne

idp_oidc: implement correct error reporting in user_info (#47900)

- error and error_description are reported in a status 401 HTTP response, inside the WWW-Authenticate and inside the JSON body of the response.

Révision 4b9be7a3 - 04 décembre 2020 11:21 - Benjamin Dauvergne

idp_oidc: simplify oidc_client fixture (#47900)

- new test test_admin will test the admin view for creating OIDCClient
- default mapping are extracted in an app setting
- OIDC_CLIENT_PARAMS is now only used on the main test SSO, creatint less redundant tests

Révision 847411c2 - 04 décembre 2020 11:21 - Benjamin Dauvergne

idp_oidc: replace secrets.compare_digest() for python<3.6 (#47900)

Historique

#1 - 20 octobre 2020 20:19 - Serghei Mihai

Et aussi il faut retourner 400: The authorization server responds with an HTTP 400 (Bad Request) status code

#2 - 22 octobre 2020 12:17 - Paul Marillonnet

Serghei Mihai a écrit :

> Et aussi il faut retourner 400: The authorization server responds with an HTTP 400 (Bad Request) status code

unless specified otherwise.
(Non sur l'échec d'authn c'est bien 401.)

#3 - 22 octobre 2020 12:23 - Paul Marillonnet

- Fichier 0001-idp_oidc-correct-error-responses-47900.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

Voilà, en corrigeant aussi la réponse sur l'endpoint UserInfo.

#4 - 22 octobre 2020 12:23 - Paul Marillonnet

Paul Marillonnet a écrit :

> Voilà, en corrigeant aussi la réponse sur l'endpoint UserInfo.

Cf. https://openid.net/specs/openid-connect-core-1_0.html#UserInfoError

#5 - 23 octobre 2020 17:53 - Benjamin Dauvergne

- Statut changé de Solution proposée à Nouveau

C'est pas ça du tout, dans le cas token il faut retourner du JSON (éventuellement + WWW-Authenticate: Basic si HTTP-Basic a été utilisé) et super-RFC-pedantic man recommande l'usage de l'entête WWW-Authenticate: Bearer dans le cas de user-info.

#6 - 23 octobre 2020 19:20 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#7 - 24 octobre 2020 09:10 - Paul Marillonnet

Ah bein oui HttpResponse ne fait pas ça, c'est vrai :)
Dis-moi, je refais mon patch sinon, comme tu veux.

#8 - 03 décembre 2020 09:53 - Benjamin Dauvergne

- Fichier 0004-idp_oidc-implement-correct-error-reporting-in-user_i.patch ajouté

- Fichier 0003-idp_oidc-add-a-simple-oidc-client-fixture-47900.patch ajouté

- Fichier 0002-idp_oidc-correctly-load-session-in-OIDCCode-and-OIDC.patch ajouté

- Fichier 0005-idp_oidc-simplify-oidc_client-fixture-47900.patch ajouté

- Fichier 0001-idp_oidc-improve-error-reporting-in-token-endpoint-4.patch ajouté

- Tracker changé de Bug à Development

- Statut changé de Nouveau à Solution proposée

#9 - 04 décembre 2020 09:37 - Paul Marillonnet

Dans 0001 :

- J'ai vu au moins une interpolation positionnelle parmi les chaînes internationalisées :

  ```
  _('OpenIDConnect Error "%s": %s') % (self.error_code, self.error_description)
  ```

  ça va pas marcher avec makemessages.

- pas de possessif sur « client's identifier », « client's secret », je dirais plutôt « client identifier », « client secret », dans les description d'erreur.

- Est-ce qu'on ne pourrait pas plutôt utiliser une property sur le modèle plutôt que de s'encombrer de ce genre de fonctions :

  ```
  +def access_token_duration(client):
  +    return client.access_token_duration or datetime.timedelta(seconds=app_settings.IDTOKEN_DURATION)
  ```

  (même si oui certes c'était déjà là avant.)

- des litérales unicodes u'' qui traînent encore ici et là dans le code des vues et qu'on pourrait virer, tant qu'à faire un patch de 2000 lignes :)

- pourquoi est-ce qu'on supprime à certains moments des appels aux hooks, mais pas tous (un grep de 'call_hooks' montre qu'il en reste dans views et utils) ?
- « User consent refused » -> « User denied consent » (? — pas sûr)
- pourquoi zéro log dans la nouvelle fonction parse_http_basic ?
- fonction check_ratelimited -> c'est un nom générique mais en fait restreinte au groupe par cession ro-cred.
  - Je pense qu'il fautajuster en changeant le nom de fonction ou en laissant le groupe passable en paramètre de fonction.
- if check_ratelimited(request, key=lambda group, request: client.client_id): -> pourquoi une fonction lambda ici, pas simplement la chaîne d'id de client puisqu'on la connaît au moment de l'appel et que le paramètre key accepte une chaîne, pas nécessairement un callable ?

Dans 0003 :

- params={} au lieu de params=None dans la signature de make_client t'éviterait de faire un params or {} ensuite, non ?

Dans 0004 :

- 'Token is expired or user is disconnected' -> Je pense que ce serait plus clair avec une forme active, genre 'Token expired or user disconnected'
- Pas de 'Bearer' dans l'entête WWW-Authenticate en cas d'erreur sur l'endpoint UserInfo, cf https://openid.net/specs/openid-connect-core-1_0.html#UserInfoError

#10 - 04 décembre 2020 10:15 - Benjamin Dauvergne

Mes réponses, j'ai intégré toutes les corrections sur la branche.

Paul Marillonnet a écrit :

> Dans 0001 :
>
> - J'ai vu au moins une interpolation positionnelle parmi les chaînes internationalisées :
>   [...]
>   ça va pas marcher avec makemessages.

Corrigé.

> - pas de possessif sur « client's identifier », « client's secret », je dirais plutôt « client identifier », « client secret », dans les description d'erreur.

Corrigé.

> - Est-ce qu'on ne pourrait pas plutôt utiliser une property sur le modèle plutôt que de s'encombrer de ce genre de fonctions :
>   [...]
>   (même si oui certes c'était déjà là avant.)

Ça disparaît dans #48889 donc non je ne m'en occupe pas ici.

> - des litérales unicodes u'' qui traînent encore ici et là dans le code des vues et qu'on pourrait virer, tant qu'à faire un patch de 2000 lignes :)

Ok fait dans models.py et views.py

> - pourquoi est-ce qu'on supprime à certains moments des appels aux hooks, mais pas tous (un grep de 'call_hooks' montre qu'il en reste dans views et utils) ?

Je ne vois pas, dans le patch j'en retire un et j'en rajoute, je l'ai juste déplacé donc (sso-request en début de authorize_for_client).

> - « User consent refused » -> « User denied consent » (? — pas sûr)

J'ai mis "User did not consent".

> - pourquoi zéro log dans la nouvelle fonction parse_http_basic ?

Je ne vois pas, il n'y en avait déjà pas avant, c'est authenticate_client qui lève des exceptions qui seront loggées par OIDCException.redirect_response(), j'ai essayé de rassembler la gestion d'erreur dans ces exceptions.

> - fonction check_ratelimited -> c'est un nom générique mais en fait restreinte au groupe par cession ro-cred.

    - Je pense qu'il fautajuster en changeant le nom de fonction ou en laissant le groupe passable en paramètre de fonction.

Ok renommé en is_ro_cred_grant_ratelimited.

- if check_ratelimited(request, key=lambda group, request: client.client_id): -> pourquoi une fonction lambda ici, pas simplement la chaîne d'id de client puisqu'on la connaît au moment de l'appel et que le paramètre key accepte une chaîne, pas nécessairement un callable ?

Parce que ça ne marche pas comme ça cf. la doc de django-ratelimit si c'est une chaîne ça doit être un truc connu (user, ip, etc..) sinon ça doit être un callable ou un chemin vers un callable[1].

[1] https://django-ratelimit.readthedocs.io/en/stable/keys.html#string-values

Dans 0003 :

- params={} au lieu de params=None dans la signature de make_client t'éviterait de faire un params or {} ensuite, non ?

C'est un code smell en python: c'est malvenu d'utiliser un objet mutable comme valeur par défaut d'un paramètre de fonction (idem pour la valeur par défaut d'un attribut de classe), s'il est modifié ça modifie la valeur pour tous les appelants.

Dans 0004 :

- 'Token is expired or user is disconnected' -> Je pense que ce serait plus clair avec une forme active, genre 'Token expired or user disconnected'

Ok, j'ai corrigé 'Token is unknown' aussi juste avant.

- Pas de 'Bearer' dans l'entête WWW-Authenticate en cas d'erreur sur l'endpoint UserInfo, cf https://openid.net/specs/openid-connect-core-1_0.html#UserInfoError

C'est la spéc qui se trompe, c'est bien comme ça que c'est décrit dans la RFC sur Bearer authentication (fin de section https://tools.ietf.org/html/rfc6750#section-3). Je pense même qu'il doit y avoir un errata, https://bitbucket.org/openid/connect/issues/990/userinfo-error-response-example-missing

#11 - 04 décembre 2020 10:31 - Paul Marillonnet

- Statut changé de Solution proposée à Solution validée

Benjamin Dauvergne a écrit :

> Je ne vois pas, dans le patch j'en retire un et j'en rajoute, je l'ai juste déplacé donc (sso-request en début de authorize_for_client).

Ok, my bad, mauvaise lecture de ma part.

> Je ne vois pas, il n'y en avait déjà pas avant, c'est authenticate_client qui lève des exceptions qui seront loggées par OIDCException.redirect_response(), j'ai essayé de rassembler la gestion d'erreur dans ces exceptions.

Ok.

> Ok renommé en is_ro_cred_grant_ratelimited.
>
> Parce que ça ne marche pas comme ça cf. la doc de django-ratelimit si c'est une chaîne ça doit être un truc connu (user, ip, etc..) sinon ça doit être un callable ou un chemin vers un callable[1].
>
> [1] https://django-ratelimit.readthedocs.io/en/stable/keys.html#string-values

D'ac, j'avais pas capté.

> C'est un code smell en python: c'est malvenu d'utiliser un objet mutable comme valeur par défaut d'un paramètre de fonction (idem pour la valeur par défaut d'un attribut de classe), s'il est modifié ça modifie la valeur pour tous les appelants.

Ah oui ok en effet c'est nul. J'aurais appris un truc, merci.

> Ok, j'ai corrigé 'Token is unknown' aussi juste avant.

Ok.

> C'est la spéc qui se trompe, c'est bien comme ça que c'est décrit dans la RFC sur Bearer authentication (fin de section https://tools.ietf.org/html/rfc6750#section-3). Je pense même qu'il doit y avoir un errata, https://bitbucket.org/openid/connect/issues/990/userinfo-error-response-example-missing

Bien vu. Bizarre il n'y a jamais eu de màj des spécs sur le site de openid(point)net malgré le correctif.

#12 - 04 décembre 2020 11:21 - Benjamin Dauvergne

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

```
commit 52c939da7e795c3f363596696f6b032366e179e9
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Thu Dec 3 12:29:01 2020 +0100

    idp_oidc: replace secrets.compare_digest() for python<3.6 (#47900)

commit 35cf607528aa8b864b659924e60909a8b4273be2
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Thu Dec 3 07:49:15 2020 +0100

    idp_oidc: simplify oidc_client fixture (#47900)

    * new test test_admin will test the admin view for creating OIDCClient
    * default mapping are extracted in an app setting
    * OIDC_CLIENT_PARAMS is now only used on the main test SSO, creatint
      less redundant tests

commit 74581d61b11ecf5b3c7aa936e715080de8bcf4c1
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Sat Oct 24 18:15:06 2020 +0200

    idp_oidc: implement correct error reporting in user_info (#47900)

    * error and error_description are reported in a status 401 HTTP response,
      inside the WWW-Authenticate and inside the JSON body of the response.

commit d477d21f8a8780b3186715cef4ef0885e43fef79
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Sat Oct 24 18:13:25 2020 +0200

    idp_oidc: add a simple oidc client fixture (#47900)

commit ce1c959a46b438a43731d345b71f1899facfd2a5
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Sat Oct 24 17:56:26 2020 +0200

    idp_oidc: correctly load session in OIDCCode and OIDCAccessToken (#47900)

    * access_token can be valid without a session or with a session linked to the user
    * code is only valid with a live session linked to its user
    * session was not loaded correctly, it's only loaded after accessing its
      content, and session_key is only checked if the session is loaded.

commit e851856c3ce9aa5b891a27d091af3b10ab711fdf
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Fri Oct 23 22:08:45 2020 +0200

    idp_oidc: improve error reporting in token endpoint (#47900)
```

#13 - 15 décembre 2020 17:16 - Frédéric Péters

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

Fichiers

0001-idp_oidc-correct-error-responses-47900.patch	1,45 ko	22 octobre 2020	Paul Marillonnet
0004-idp_oidc-implement-correct-error-reporting-in-user_i.patch	5,92 ko	03 décembre 2020	Benjamin Dauvergne
0003-idp_oidc-add-a-simple-oidc-client-fixture-47900.patch	1,79 ko	03 décembre 2020	Benjamin Dauvergne
0002-idp_oidc-correctly-load-session-in-OIDCCode-and-OIDC.patch	4,1 ko	03 décembre 2020	Benjamin Dauvergne
0005-idp_oidc-simplify-oidc_client-fixture-47900.patch	7,1 ko	03 décembre 2020	Benjamin Dauvergne