# Authentic 2 - Bug #44593

## idp_oidc: lors de la validation des URLs de redirection vérifier aussi la querystring et le fragment

29 juin 2020 16:57 - Benjamin Dauvergne

| | | | |
|---|---|---|---|
| **Statut:** | Fermé | **Début:** | 29 juin 2020 |
| **Priorité:** | Normal | **Echéance:** | |
| **Assigné à:** | | **% réalisé:** | 0% |
| **Catégorie:** | | **Temps estimé:** | 0:00 heure |
| **Version cible:** | | | |
| **Patch proposed:** | Oui | **Planning:** | Non |

**Description**

Pour égalité exacte (modulo parsing via parse_qs()).

**Demandes liées:**

| | | |
|---|---|---|
| Lié à Authentic 2 - Development #73903: ignorer un éventuel ancre dans les UR... | **Nouveau** | **26 janvier 2023** |

### Révisions associées

**Révision 1cc56c86 - 16 septembre 2020 13:45 - Paul Marillonnet**

idp_oidc: validate redirect uri query and fragment (#44593)

### Historique

**#1 - 29 juin 2020 16:57 - Benjamin Dauvergne**

*- Sujet changé de oidc: lors de la validation des URLs de redirection vérifier aussi la querystring et le fragment à idp_oidc: lors de la validation des URLs de redirection vérifier aussi la querystring et le fragment*

**#2 - 06 août 2020 16:10 - Paul Marillonnet**

*- Statut changé de Nouveau à Information nécessaire*

J'ai d'abord eu l'impression que c'était de la validation lors de l'enregistrement du client dans l'/admin/ que tu parlais, mais en relisant il me semble que c'est de leur validation de la phase d'autorisation.
Le fragment ou la query string étant utilisés pour passer les paramètres de réponse d'autorisation, je ne comprends pas ce que l'IdP, lui-même à l'origine de cette réponse, devrait vérifier.

**#3 - 06 août 2020 16:26 - Benjamin Dauvergne**

Le client ne doit rien passer de plus ni dans la qs ni dans le fragment, sauf si on le permet (disons avec un wildcard, genre ?*#* ça veut dire qs et fragment libre).

**#4 - 06 août 2020 16:40 - Nicolas Roche**

(pour redonner le contexte)

Je ne retrouve plus le message d'origine, mais à propos de https://dev.entrouvert.org/issues/41785#note-41 / #44589 benjamin écrivait :
"Au niveau de la validation des redirect_uri c'est égalité strict scheme, netloc, path et le reste est libre et conservé."

Parce que l'URI de redirection peut inclure des paramètres comme par exemple sur #44589 :
https://padev5bis.commeunservice.com/account-management/saintdenis-demandeurs/oidc/publik/code?redirectUrl=https%3A%2F%2Fpadev5bis.commeunservice.com%2Faides%2F%23%2Fsaintdenis%2Fconnecte%2Fdashboard%2Faccueil&jwtKey=jwt-saintdenis-portail-depot-demande-aides

**#5 - 10 septembre 2020 11:34 - Paul Marillonnet**

*- Fichier 0001-idp_oidc-validate-redirect-uri-query-and-fragment-44.patch ajouté*

*- Tracker changé de Support à Bug*

*- Statut changé de Information nécessaire à Solution proposée*

*- Patch proposed changé de Non à Oui*

Une première solution toute simple, sans chercher à matcher sur des paramètres de qs. Sans doute ça va casser des trucs, il faudrait faire le tour des clients déclarés en parallèle de ce ticket.

**#6 - 10 septembre 2020 15:21 - Benjamin Dauvergne**

*- Statut changé de Solution proposée à En cours*

Je pense que ça ne coûte rien d'ajouter un parsed_valid_uri.query != parsed_uri.query, à minima on gère une query vide, une query identique ou une query complètement libre (comme pour le fragment).

#### #7 - 10 septembre 2020 15:42 - Paul Marillonnet

*- Fichier 0001-idp_oidc-validate-redirect-uri-query-and-fragment-44.patch ajouté*

*- Statut changé de En cours à Solution proposée*

Benjamin Dauvergne a écrit :

> Je pense que ça ne coûte rien d'ajouter un parsed_valid_uri.query != parsed_uri.query, à minima on gère une query vide, une query identique ou une query complètement libre (comme pour le fragment).

Ok.

#### #8 - 10 septembre 2020 15:44 - Benjamin Dauvergne

*- Statut changé de Solution proposée à Solution validée*

#### #9 - 15 septembre 2020 12:32 - Paul Marillonnet

Discuté par courriel sur la liste :

> Et, sur le point de taper dans un pad la liste des A2 pour faire le changement, je me dis qu'on va mettre ce ?*#* partout dans les config déjà en place et celles à venir. Et que donc cette restriction va être systématiquement court-circuitée…
>
> Peut-être cette restriction ferait-elle davantage sens si on rendait possible de valider sur des motifs d'ancre et de paramètres de chaîne de requête ?
> Genre ?foo-*=*#part3-*

Et donc ?*#* pourrait être le comportement par défaut lorsque rien n'est précisé, et dans le cas contraire on déclarerait des motifs plus précis que ce double wildcard.

#### #10 - 15 septembre 2020 13:17 - Benjamin Dauvergne

Paul Marillonnet a écrit :

> Et donc ?*#* pourrait être le comportement par défaut lorsque rien n'est précisé, et dans le cas contraire on déclarerait des motifs plus précis que ce double wildcard.

Mais comment dire que ça doit être strictement vide ? "?$#", je trouve ça dommage alors que c'est le comportement par défaut préconisé par la spécification.

Le laisser libre par défaut, c'est prendre un risque par défaut; je suis incapable de donner un cas, la spéc dit que le metch doit être strict, lors d'un audit si les auditeurs s'y intéressent on aura une remarque et on devra repasser à chaque fois pour ajouter "?#". On a quand même très peu de service OIDC déployés en dehors de GLC, ajouter "?*#*" en one shot ne me dérange pas (et sur GLC on peut s'en passer, on est sensé être strict, on l'a mis dans la documentation de GLC).

#### #11 - 15 septembre 2020 13:49 - Paul Marillonnet

Benjamin Dauvergne a écrit :

> ajouter "?*#*" en one shot ne me dérange pas (et sur GLC on peut s'en passer, on est sensé être strict, on l'a mis dans la documentation de GLC).

Ok faisons comme ça.

#### #17 - 16 septembre 2020 11:12 - Paul Marillonnet

*- Statut changé de Solution validée à Information nécessaire*

#### #22 - 16 septembre 2020 13:44 - Paul Marillonnet

*- Statut changé de Information nécessaire à En cours*

#### #24 - 16 septembre 2020 13:46 - Paul Marillonnet

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

```
commit 1cc56c86521bd663254ecc80da976a1da503cf99
Author: Paul Marillonnet <pmarillonnet@entrouvert.com>
Date:   Thu Sep 10 10:48:31 2020 +0200

    idp_oidc: validate redirect uri query and fragment (#44593)
```

#### #25 - 18 septembre 2020 08:16 - Frédéric Péters

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

#### #29 - 24 septembre 2020 17:53 - Benjamin Dauvergne

Script appliqué en production à 16:07.

#### #30 - 26 janvier 2023 16:59 - Paul Marillonnet

*- Lié à Development #73903: ignorer un éventuel ancre dans les URL de la configuration OIDC (?) ajouté*

### Fichiers

| | | |
|---|---|---|
| 0001-idp_oidc-validate-redirect-uri-query-and-fragment-44.patch | 2,58 ko 10 septembre 2020 | Paul Marillonnet |
| 0001-idp_oidc-validate-redirect-uri-query-and-fragment-44.patch | 2,67 ko 10 septembre 2020 | Paul Marillonnet |