Publik - Support #52633

Documenter d'autres cookies.

01 avril 2021 15:47 - Nicolas Roche

Statut:	Fermé	**Début:**	01 avril 2021
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Club:**	Non
Planning:	Non		

Description

sur https://dev.entrouvert.org/projects/publik/wiki/Cookies,
on ne documente pas les cookies :

- csrftoken-*
- a2_just_logged_out
- cookie-test

Historique

#2 - 01 avril 2021 15:49 - Nicolas Roche

Voici un premier jet de la réponse que je pense apporter dans #52632,
et éventuellement pour mettre à jour notre page de wiki.

nom : csrftoken-*
finalité : cookie de protection contre le « Cross site request forgery » (CSRF)
cf https://docs.djangoproject.com/fr/1.11/ref/csrf/#acquiring-the-token-if-csrf-use-sessions-is-false
durée : 1 an
si refus : la protection CSRF sera désactivée
au profit : du fonctionnement technique du framework Django utilisé par Publik

nom : a2_just_logged_out
finalité : cookie qui signale qu'une déconnexion à eu lieu récemment
cf https://dev.entrouvert.org/issues/6021
durée : 60 secondes
si refus : l'utilisateur risque d'être immédiatement reconnecté avec son précédent compte si celui-ci utilise un mode de connexion automatique (SSL ou Kerberos), c'est très rare. *(correction suite à la remarque ci-dessous)*
au profit : du fonctionnement technique de Publik (ne contient pas de données)

nom : cookie-test
finalite : vérifier l'accéptation des cookies par l'utilisateur
use long duration cookie to check for cookie support in browser
cf https://dev.entrouvert.org/issues/44055
durée : 1 an
si refus : affichage d'un bandeau expliquant que l'on a besoin des cookie pour que le site fonctionne.
au profit : du fonctionnement technique de Publik (ne contient pas de données)

#3 - 01 avril 2021 16:16 - Pierre Cros

écrit comme ça ça laisse penser que csrftoken-* contient des données et nécessite donc une déclaration.

#4 - 01 avril 2021 17:46 - Benjamin Dauvergne

Nicolas Roche a écrit :

> nom : a2_just_logged_out
> finalité : cookie qui signale qu'une déconnexion à eu lieu récemment
> cf https://dev.entrouvert.org/issues/6021
> durée : 60 secondes
> si refu : l'utilisateur peut ne pas être automatiquement délogué via sso

Si refus l'utilisateur risque d'être immédiatement reconnecté avec son précédent compte si celui-ci utilise un mode de connexion automatique (SSL ou Kerberos), c'est très rare.

au profit : du fonctionnement technique de Publik (ne contient pas de données)

#5 - 02 avril 2021 10:56 - Nicolas Roche

écrit comme ça ça laisse penser que csrftoken-* contient des données et nécessite donc une déclaration.

je revois ma copie :

nom : csrftoken-*
finalité : stockage d'un secret permettant la protection contre le « Cross site request forgery » (CSRF)
cf https://docs.djangoproject.com/fr/1.11/ref/csrf/#acquiring-the-token-if-csrf-use-sessions-is-false
durée : 1 an
si refus : les formulaires des sites web utilisant le framework Django ne fonctionneront plus.
au profit : du fonctionnement technique du framework Django utilisé par Publik

#6 - 02 avril 2021 11:24 - Nicolas Roche

Et je propose d'amender la page https://dev.entrouvert.org/projects/publik/wiki/Cookies :

```
Chaque module logiciel de Publik pose un cookie de session, dont le nom commence par "sessionid-" ...
Les modules publique utilisent également des cookies nommés "csrftoken-*" afin d'assurer la protection contre
le « Cross site request forgery » (CSRF).

Le fournisseur d'identité pose aussi
* un cookie nommé "A2_OPENED_SESSION" ...
* un cookie nommé "a2_just_logged_out" qui évite à l'utilisateur risque d'être immédiatement reconnecté avec s
on précédent compte si celui-ci utilise un mode de connexion automatique (SSL ou Kerberos).
* un cookie nommé "cookie-test" pour vérifier l'accéptation des cookies par l'utilisateur.
Ces deux derniers cookies ne contiennent pas de données.

Aucun de ces cookies ne nécessite de déclaration ...
```

#7 - 02 avril 2021 15:07 - Pierre Cros

Vraiment difficile à suivre, je vois pas pourquoi csrftoken-* ne devrait pas apparaître dans le wiki.

Par ailleurs ça ne change rien à ce que j'écrivais et je vais donc être plus explicite : quand on précise pour certains cookies et pas pour d'autres qu'ils ne contiennent pas de données, ça donne à penser que ceux pour lesquels on ne dit rien en contiennent et doivent donc faire l'objet d'une déclaration.

Il faut un peu se mettre à la place de la dame DPO de Villeneuve qui va lire ça, elle le lira comme moi, et va me dire "mais puisqu'ils contiennent des données il faut faire une déclaration contrairement à ce que vous me disiez espèce d'escroc".

Donc :

- S'ils ne contiennent pas de données il faut le dire
- S'ils en contiennent
  - S'il faut une déclaration, il faut le dire
  - S'il n'en faut pas il faut expliquer pourquoi
- Si tu n'en sais rien, il faut que je le sache

#8 - 02 avril 2021 15:37 - Nicolas Roche

Vraiment difficile à suivre,

Oui désolé, j'ai raté mon copier/coller à Villeneuve d'asq. Je corrigerai si tu penses que ça va comme ça :

```
Les modules publique utilisent également des cookies nommés "csrftoken-*" afin d'assurer la protection contre
le « Cross site request forgery » (CSRF). Ce cookie contient uniquement un identifiant permettant de s'assurer
 que le formulaire validé par l'utilisateur est bien celui qui lui a été affiché préalablement.
```

En ajoutant dans le ticket villeneuve d'Asq le paragraphe du dessous :

```
Aucun de ces cookies ne nécessite de déclaration (ils ne servent pas au traçage des activités de l'utilisateur
, mais seulement à des fins techniques d'authentification).
```

#9 - 02 avril 2021 15:40 - Nicolas Roche

> je vois pas pourquoi csrftoken-* ne devrait pas apparaître dans le wiki.

sisi il y est, je propose de l'y mettre juste en dessous du premier paragraphe (mais là dessus j'aimerai quand même avoir l'avis des techs).

#10 - 02 avril 2021 15:49 - Frédéric Péters

Les cookies c'est nécessairement clé=valeur, ils ont tous des données (malgré ce qui a été écrit "Ces deux derniers cookies ne contiennent pas de données).

J'ai complété Cookies pour mentionner les cookies CSRF et cookie-test et a2-just-logged-out; j'ai aussi précisé le contenu, jeton opaque pour session et csrf, "1" pour les autres.

Je ne sais pas si le texte ainsi conviendrait à quelqu'un qui a peur des cookies, je laisse poursuivre les changements.

#12 - 02 avril 2021 16:23 - Pierre Cros

J'ai réagencé la page pour que les différents cookies soient plus visibles.

#13 - 02 avril 2021 16:26 - Frédéric Péters

- Statut changé de Nouveau à Fermé

Ok on peut dire que c'est bon là. (ça reste un wiki si jamais d'autres personnes veulent adapter la page)