Gadjo - Development #40525

POST pour la déconnexion

08 mars 2020 15:19 - Frédéric Péters

Statut:	En cours	**Début:**	08 mars 2020
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Discussion en cours sur django-developers pour aboutir à l'utilisation d'un POST pour le lien de déconnexion,

> there seems to be consensus that logging the client out on GET requests to the logout view is not great. Clients may try to prefetch links (this came up on IRC today). Attackers might annoy users by logging them out with embedded links to the logout URL.

On peut facilement déjà faire ça côté Gadjo. (pour le front il y aurait des questions de style).

Historique

#1 - 08 mars 2020 15:23 - Frédéric Péters

- Fichier 0001-misc-use-POST-for-logout-40525.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

En passant, classe .sr-only pour l'accessibilité (comme dans la proposition #36909) et agrandissement de l'icône lors du survol.

#2 - 09 mars 2020 07:20 - Frédéric Péters

(c'est plutôt pénible pour les tests unitaires qui se basaient sur l'idée d'un seul formulaire sur la page, qu'il faut mettre à jour...)

#3 - 09 mars 2020 10:20 - Benjamin Dauvergne

Ça couvre le prefetch mais pour couvrir les DoS malicieux il faut quand même un support coté serveur (coté authentic il y a un check du Referer sur la vue de logout et aucun check si ça vient d'un site validé où d'une méthode de logout d'une protocole de SSO).

#4 - 11 mars 2020 08:40 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

#5 - 24 avril 2020 09:11 - Frédéric Péters

- Statut changé de Solution validée à En cours

(je retire le côté validé pour éviter de pousser ça qui va péter mille tests ailleurs).

#6 - 24 avril 2020 14:08 - Benjamin Dauvergne

Le faire en JS ?

#7 - 24 avril 2020 15:02 - Frédéric Péters

Ne pas avoir de <form> et un bouton avec un événement qui somehow fasse le POST (en créant à la volée un formulaire bidon ?), peut-être.

#8 - 24 avril 2020 15:59 - Benjamin Dauvergne

Frédéric Péters a écrit :

> Ne pas avoir de <form> et un bouton avec un événement qui somehow fasse le POST (en créant à la volée un formulaire bidon ?), peut-être.

Oui. On pourrait établir une politique de ne plus créer de form sans name ou id mais c'est un peu tard.

Fichiers

0001-misc-use-POST-for-logout-40525.patch	2,47 ko	08 mars 2020	Frédéric Péters