Authentic 2 - Development #44435

ajouter django.middleware.clickjacking.XFrameOptionsMiddleware

25 juin 2020 10:50 - Benjamin Dauvergne

Statut:	Fermé	**Début:**	25 juin 2020
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Comme ailleurs.

Révisions associées

Révision 8fa965c5 - 26 juin 2020 12:15 - Benjamin Dauvergne

mics: apply xframe_options_deny to views (#44435)

IdP and auth views are exempted.

Historique

#1 - 25 juin 2020 10:50 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#2 - 25 juin 2020 10:54 - Benjamin Dauvergne

- Fichier 0001-settings-add-XFrameOptionsMiddleware-44435.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

#3 - 25 juin 2020 10:55 - Paul Marillonnet

- Statut changé de Solution proposée à Solution validée

Okay.

#6 - 25 juin 2020 11:31 - Frédéric Péters

- Fichier Screenshot_2020-06-25 Montoulouse fr - Auquo - fichier fargo.png ajouté

#10 - 25 juin 2020 11:55 - Paul Marillonnet

- Statut changé de Solution validée à Solution proposée

Et donc décorer (xframe_options_exempt) la vue de login ?

#12 - 25 juin 2020 12:13 - Benjamin Dauvergne

- Fichier 0001-mics-apply-xframe_options_deny-to-views-44435.patch ajouté

Nouvelle idée, /idp/saml2/login sera exempté donc si on est déjà connecté on doit pouvoir ouvrir fargo dans une iframe.

#13 - 25 juin 2020 16:00 - Paul Marillonnet

Benjamin Dauvergne a écrit :

> Nouvelle idée, /idp/saml2/login sera exempté donc si on est déjà connecté on doit pouvoir ouvrir fargo dans une iframe.

N'arrivant pas à reproduire le blocage décrit par Frédéric je ne suis pas en mesure de valider, mais je note tout de même que dans ce nouveau patch on passe de sameorigin à deny pour la valeur de l'entête X-Frame-Options (ce qui est peut-être volontaire, mais si ce n'est pas le cas, c'est le décorateur xframe_options_sameorigin qu'il faut utiliser).

#14 - 25 juin 2020 18:57 - Benjamin Dauvergne

Paul Marillonnet a écrit :

> N'arrivant pas à reproduire le blocage décrit par Frédéric je ne suis pas en mesure de valider,

Je vais tenter de mon coté alors.

> mais je note tout de même que dans ce nouveau patch on passe de sameorigin à deny pour la valeur de l'entête X-Frame-Options (ce qui est peut-être volontaire, mais si ce n'est pas le cas, c'est le décorateur xframe_options_sameorigin qu'il faut utiliser).

C'est volontaire, je n'avais pas réfléchi à deny ou sameorigin dans le premier patch, je faisais juste comme dans combo pour répondre à la demande de l'audit de sécu du CD13. Dans le deuxième patch je me suis dit autant faire le plus, ces vues ne sont pas prévus pour être utilisées dans une iframe, point, mais si c'est jugé trop extrême je peux revenir à sameorigin.

#15 - 26 juin 2020 10:14 - Paul Marillonnet

Benjamin Dauvergne a écrit :

> C'est volontaire, je n'avais pas réfléchi à deny ou sameorigin dans le premier patch, je faisais juste comme dans combo pour répondre à la demande de l'audit de sécu du CD13. Dans le deuxième patch je me suis dit autant faire le plus, ces vues ne sont pas prévus pour être utilisées dans une iframe, point, mais si c'est jugé trop extrême je peux revenir à sameorigin.

Non au contraire, à mon avis l'option le plus restrictif possible qui pour autant ne casse pas nos usages, c'est nickel.

#16 - 26 juin 2020 12:23 - Benjamin Dauvergne

Benjamin Dauvergne a écrit :

> Paul Marillonnet a écrit :
>
> > N'arrivant pas à reproduire le blocage décrit par Frédéric je ne suis pas en mesure de valider,
>
> Je vais tenter de mon coté alors.

Test effectué :

- sur /, /accounts/ et /login/ on a bien le DENY
- j'ai ajouté un champ fichier sur un formulaire avec option pour prendre un fichier dans fargo
- utilisation du formulaire, fargo ouvert dans un autre onglet, je supprime le cookie de session de fargo pour m'assurer qu'on y est pas connecté
- click sur "Utiliser un fichier du porte-document", la liste s'affiche, dans le debugger la requête de SSO donne lieu à une réponse 302 sans entête X-Frame-Options

#17 - 26 juin 2020 12:26 - Paul Marillonnet

- Statut changé de Solution proposée à Solution validée

Benjamin Dauvergne a écrit :

> Test effectué :
> […]

Top, merci, c'est ok pour moi.

#18 - 26 juin 2020 12:29 - Benjamin Dauvergne

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

```
commit 8fa965c522fba3be0b778008d495f11a86c7aa3b
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Thu Jun 25 12:11:39 2020 +0200

    mics: apply xframe_options_deny to views (#44435)

    IdP and auth views are exempted.
```

#19 - 01 juillet 2020 21:16 - Frédéric Péters

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

Fichiers

0001-settings-add-XFrameOptionsMiddleware-44435.patch	801 octets	25 juin 2020	Benjamin Dauvergne
Screenshot_2020-06-25 Montoulouse fr - Auquo - fichier fargo.png	91,9 ko	25 juin 2020	Frédéric Péters
0001-mics-apply-xframe_options_deny-to-views-44435.patch	1,23 ko	25 juin 2020	Benjamin Dauvergne