Authentic 2 - Development #76835

empêcher le contrôle des redirections sur les mails d'enregistrement et de réinitialisation de mot de passe

20 avril 2023 16:27 - Benjamin Dauvergne

Statut:	Solution proposée	**Début:**	20 avril 2023
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Planning:**	Non

Description

On nous rapporte dans un audit de sécurité qu'il y aurait un souci sur ce point.

Demandes liées:

Lié à Authentic 2 - Development #76858: Ne pas utiliser de signature de next_...	**Solution proposée** 24 avril 2023

Historique

#2 - 20 avril 2023 16:27 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#3 - 20 avril 2023 16:46 - Robot Gitea

Benjamin Dauvergne (bdauvergne) a ouvert une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/authentic/pulls/44
- Titre : tests: check open redirection is impossible for /password/reset/ (#76835)
- Modifications : https://git.entrouvert.org/entrouvert/authentic/pulls/44/files

#4 - 20 avril 2023 17:18 - Robot Gitea

- Statut changé de Nouveau à En cours

Paul Marillonnet (pmarillonnet) a relu et demandé des modifications sur une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/authentic/pulls/44

#5 - 20 avril 2023 22:35 - Benjamin Dauvergne

- Sujet changé de Vérifier la possibilité de redirection arbitraire sur un reset de password à empêcher le contrôle des redirections sur les mails d'enregistrement et de réinitialisation de mot de passe

#6 - 21 avril 2023 09:05 - Benjamin Dauvergne

- Lié à Development #76858: Ne pas utiliser de signature de next_url quand c'est inutile, et limiter leur réutilisation quand c'est utile ajouté

#7 - 03 mai 2023 11:31 - Benjamin Dauvergne

Plein de mouvement sur password-reset pour l'enregistrement par mobile, je reprendrai après.

#8 - 03 mai 2023 12:05 - Paul Marillonnet

Benjamin Dauvergne a écrit :

> Plein de mouvement sur password-reset pour l'enregistrement par mobile, je reprendrai après.

Arf oui désolé :/
Une fois qu'on s'est mis d'accord sur #69890 je pourrai rebaser la partie concernée la branche de ce ticket-ci, si tu veux.

#9 - 03 mai 2023 12:35 - Benjamin Dauvergne

Paul Marillonnet a écrit :

> Une fois qu'on s'est mis d'accord sur #69890 je pourrai rebaser la partie concernée la branche de ce ticket-ci, si tu veux.

Pas la peine, je rebaserai ici.

#12 - 09 novembre 2023 14:24 - Robot Gitea

- Tracker changé de Support à Development

Benjamin Dauvergne (bdauvergne) a ouvert une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/authentic/pulls/171
- Titre : WIP: wip/76835-open-redirection
- Modifications : https://git.entrouvert.org/entrouvert/authentic/pulls/171/files

#13 - 09 novembre 2023 14:25 - Robot Gitea

Benjamin Dauvergne (bdauvergne) a fermé une pull request sur Gitea concernant cette demande.

#14 - 09 novembre 2023 19:31 - Robot Gitea

- Statut changé de En cours à Solution proposée