w.c.s. - Development #1133

Formdata anonymes

13 décembre 2011 16:32 - Thomas Noël

Statut:	Fermé	**Début:**	13 décembre 2011
Priorité:	Haut	**Echéance:**	21 décembre 2011
Assigné à:	Frédéric Péters	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:		**Planning:**	

Description

CNIL : les réponses aux formulaires ne doivent pas être liées fortement avec les users.

Réponse : la liaison entre formdata et user sera faite via un hash du user. Un user peut donc trouver ses formulaires, mais on ne peut pas (facilement) remonter d'un formulaire vers un user.

A coder :

- une option générale hash_salt qui activera la fonctionnalité si elle existe (chaîne de caractères, qui ne doit jamais être modifiée en cours de route...)
- User.hash()
- enregistrer un formdata.user_hash au lieu du user_id quand le salt existe
- un test : FormData::is_submitter(user) à utiliser un peu partout à la place des fd.user_id == user.id
- lors de l'affichage dans myspace, la cherche les formulaires doit lister ceux qui ont le user_id + ceux qui ont le user_hash
- modif à l'enregistrement de l'historique, pour enregistrer _submitter plutôt que user_id, dans le cas cas où ça se présente (éventuellement ajouter des trucs dans "Evolution" pour gérer un who de type "submitter")

Historique

#1 - 13 décembre 2011 16:32 - Thomas Noël

- Description mis à jour

#2 - 13 décembre 2011 17:10 - Thomas Noël

- Description mis à jour

#3 - 15 décembre 2011 19:40 - Thomas Noël

- Echéance mis à 21 décembre 2011

- Priorité changé de Normal à Haut

RdV avec la CNIL le ~~23~~ 26 décembre, ça serait bien d'avoir ça juste avant (même en PoC) au cas où le technicien demande des détails.

#4 - 18 décembre 2011 16:49 - Frédéric Péters

- Fichier wcs.userhash.diff ajouté

Brièvement testé.

#5 - 18 décembre 2011 17:18 - Thomas Noël

Merci Fred ; première lecture rapide :

- y'a un "user.hash()" qui traine alors que hash est une property
- j'ajouterai bien un hint sur la config du sel, qui dirait « Une fois la valeur du sel choisie, ne la modifiez plus.», quitte à expliquer également à quoi sert ce sel (il rend la liaison entre utilisateur et formulaire unilatérale... mais je ne sais pas trop comment l'expliquer sans faire un roman).

#6 - 18 décembre 2011 17:51 - Frédéric Péters

- Fichier wcs.userhash.diff ajouté

Ack; sans faire un roman c'est pas évident; en attendant j'ai aussi modifié ce formulaire pour que le champ avec le sel soit en lecture seule une fois complété.

#7 - 18 décembre 2011 18:47 - Thomas Noël

- Statut changé de Nouveau à En cours

#8 - 18 décembre 2011 22:30 - Benjamin Dauvergne

Pour moi le sel en question est une configuration inutile, je verrai bien ça comme un truc auto-généré si absent du config.pck au lancement de w.c.s, où à la création du répertoire pour un domaine. Et pour le nommage je propose plutôt que sel comme dans Django la variable de configuration SECRET_KEY. C'est un secret qui sert un peu à tout, signer les cookies, saler les hash des mots de passe, etc..

#9 - 18 décembre 2011 23:58 - Frédéric Péters

On pourrait se contenter d'une case à cocher, cochable une fois, qui derrière générerait ce bout d'aléatoire; par contre je tiens à ce que sa fonction soit et reste limitée à la création d'un hash d'un utilisateur.

#10 - 19 décembre 2011 17:39 - Frédéric Péters

- Fichier wcs.userhash.diff ajouté

Une simple case à cocher et la génération aléatoire du sel.

#11 - 20 décembre 2011 13:43 - Thomas Noël

Pourquoi le "Beware this setting cannot be reverted" ? Selon moi, si on désactive, ça va redonner une bijection formdata<->user, mais la liste des formulaires liés à un utilisateur fonctionnera toujours, y compris pour ceux stockés avec un hash... Non ?

#12 - 20 décembre 2011 13:48 - Benjamin Dauvergne

redmine@entrouvert.com écrivait:

> Pourquoi le "Beware this setting cannot be reverted" ? Selon moi, si on désactive, ça va redonner une bijection formdata<->user, mais la liste des formulaires liés à un utilisateur fonctionnera toujours, y compris pour ceux stockés avec un hash... Non ?

Je pense qu'il faut signifier que pour les formulaires soumis durant l'activation de l'option c'est irréversible; mais en même temps ça me parait implicite avec l'existence d'une case à cocher et l'intitulé de l'option. Pour des option one-shot comme la conversion vers utf8 c'est mieux d'utiliser un bouton qui disparait une fois utilisé.

#13 - 22 décembre 2011 19:33 - Thomas Noël

Je ne comprends pas en quoi c'est "irreversible"... On peut très bien la réactiver, et ça va recréer un lien fort user/form le temps de désactivation... et si on réactive, ça refait du hash...

#14 - 22 décembre 2011 19:36 - Thomas Noël

En revanche, un truc important à faire selon moi : si l'option est activée, retirer les variables "form_user*" de la liste affichée (cf les Substitutions.register correspondant à la fin de formdata.py).

Ca permet notamment de "faire comprendre le principe".

#15 - 26 décembre 2011 14:02 - Anonyme

Le "cannot be reverted", c'est parce que le hashage se fait si le sel est mis, donc repasser en mode non hashé signifie enlever la valeur de la clé secrète, et donc les formulaires enregistrés avec un user_hash ne pourront plus être liées.

Alors bien sûr il est possible d'avoir deux paramètres dans les préférences, le fait de hasher ou pas, et la clé secrète.

On fait, on fait pas ?

#16 - 26 décembre 2011 14:24 - Frédéric Péters

- Fichier wcs.userhash.diff ajouté

Nouveau patch avec 1) séparation en deux paramètres (use_user_hash et user_hash_secret_key), 2) en conséquence possibilité d'allers/retours entre l'option activée ou pas, 3) réécriture pour utiliser le module hmac et toujours sha-256 (et donc une dépendance sur Python 2.5+).

#17 - 27 décembre 2011 22:04 - Frédéric Péters

- Statut changé de En cours à Solution déployée

#18 - 27 décembre 2011 22:36 - Frédéric Péters

- Fichier auquo.userhash.diff ajouté

J'avais oublié d'ajouter le patch pour auquo, le voici.

#19 - 28 décembre 2011 18:26 - Frédéric Péters

- Fichier wcs.userhash.diff ajouté

Correction d'un petit bug (user_id utilisé là où ça devrait être user).

#20 - 03 janvier 2012 15:06 - Thomas Noël

Frédéric Péters a écrit :

> Correction d'un petit bug (user_id utilisé là où ça devrait être user).

mmmh... j'ai l'impression qu'au passage, il n'y a plus la séparation use_user_hash/user_hash_secret_key et qu'on a perdu le sha256... non ? (voir note 16 ci-dessus)

#21 - 03 janvier 2012 15:13 - Anonyme

- Fichier wcs.userhash.diff ajouté

Ouaip, je suis reparti du mauvais patch :(Le bon est celui avec hmac, et la correction est que l'appel à is_submitter() doit se faire avec user, et pas user_id, dans workflows.py…

#22 - 10 janvier 2012 14:11 - Frédéric Péters

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

r2218.

#23 - 20 novembre 2013 12:09 - Frédéric Péters

- Statut changé de Résolu (à déployer) à Fermé

#24 - 26 août 2015 16:53 - Thomas Noël

- Version cible Au-quotidien 2012.1 supprimé

Fichiers

wcs.userhash.diff	7,97 ko	18 décembre 2011	Frédéric Péters
wcs.userhash.diff	8,21 ko	18 décembre 2011	Frédéric Péters
wcs.userhash.diff	8,79 ko	19 décembre 2011	Frédéric Péters
wcs.userhash.diff	8,67 ko	26 décembre 2011	Frédéric Péters
auquo.userhash.diff	719 octets	27 décembre 2011	Frédéric Péters
wcs.userhash.diff	8,78 ko	28 décembre 2011	Frédéric Péters
wcs.userhash.diff	8,67 ko	03 janvier 2012	Anonyme