Mandaye - Bug #13263

ne pas utiliser la SECRET_KEY de django pour le chiffrement des mots de passe

21 septembre 2016 18:08 - Serghei Mihai

Statut:	Fermé	**Début:**	21 septembre 2016
Priorité:	Normal	**Echéance:**	
Assigné à:	Serghei Mihai	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	

Description

Car la valeur de la clé pour le cryptage doit avoir une longueur particulière:

```
  File "/usr/lib/python2.7/dist-packages/Crypto/Cipher/AES.py", line 59, in __init__
    blockalgo.BlockAlgo.__init__(self, _AES, key, *args, **kwargs)
  File "/usr/lib/python2.7/dist-packages/Crypto/Cipher/blockalgo.py", line 141, in __init__
    self._cipher = factory.new(key, *args, **kwargs)
ValueError: AES key must be either 16, 24, or 32 bytes long
```

et ce n'est pas le cas de la clé générée par Django.

Révisions associées

Révision f56e7786 - 22 septembre 2016 16:34 - Serghei Mihai

use secret key's hash to encrypt user passwords (#13263)

Historique

#1 - 21 septembre 2016 18:30 - Benjamin Dauvergne

Faire un sha256 et garder 16 octets.

#2 - 21 septembre 2016 18:47 - Serghei Mihai

- Fichier 0001-use-secret-key-s-hash-to-encrypt-user-passwords-1326.patch ajouté

- Statut changé de Nouveau à En cours

- Assigné à mis à Serghei Mihai

- Patch proposed changé de Non à Oui

Ok

#4 - 22 septembre 2016 10:25 - Benjamin Dauvergne

- Utiliser directement sha256().digest() qui renvoit une chaîne de 32 octets adaptée pour AES (16, 24 ou 32 octets).
- Ne pas utiliser un vecteur d'initialisation à '0000000' (IV) mais une chaîne générée par SystemRandom de 16 octets, encodé ensuite en base64 et préfixé au chiffré avec un caractère '$' entre les deux.

Tu peux aussi copier directement le code d'authentic sur ce sujet: http://git.entrouvert.org/authentic.git/tree/src/authentic2/crypto.py

#5 - 22 septembre 2016 10:39 - Serghei Mihai

- Fichier 0001-use-secret-key-s-hash-to-encrypt-user-passwords-1326.patch ajouté

Ok

#6 - 22 septembre 2016 11:37 - Serghei Mihai

- Fichier 0001-use-secret-key-s-hash-to-encrypt-user-passwords-1326.patch supprimé

#7 - 22 septembre 2016 11:37 - Serghei Mihai

- Fichier 0001-use-secret-key-s-hash-to-encrypt-user-passwords-1326.patch ajouté

#8 - 22 septembre 2016 16:45 - Josué Kouka

Ack, le test passe

#9 - 22 septembre 2016 16:51 - Serghei Mihai

- Statut changé de En cours à Résolu (à déployer)

```
commit f56e7786012f1152ea69d5a54a06a2e5c83d175d
Author: Serghei Mihai <smihai@entrouvert.com>
Date:   Wed Sep 21 18:46:20 2016 +0200

    use secret key's hash to encrypt user passwords (#13263)
```

#10 - 30 novembre 2016 11:22 - Benjamin Dauvergne

- Statut changé de Résolu (à déployer) à Fermé

Fichiers

0001-use-secret-key-s-hash-to-encrypt-user-passwords-1326.patch	1,89 ko 21 septembre 2016	Serghei Mihai
0001-use-secret-key-s-hash-to-encrypt-user-passwords-1326.patch	3,16 ko 22 septembre 2016	Serghei Mihai