Authentic 2 - Bug #5617

CSRF token rotation since Django 1.5.2 has broken usability of login and registration page

02 octobre 2014 21:50 - Benjamin Dauvergne

Statut:	Fermé	**Début:**	02 octobre 2014
Priorité:	Haut	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	100%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:	2.1.12		
Patch proposed:	Oui	**Planning:**	

Description

Since the CSRF token is rotated on each login, lot of users see 403 errors when submitting login or registration because they multitask a lot. To fix that we will change three things:

- on login page, we wait after having validated that the user is not already logged to let the the CSRF token check happen, so that we can just redirect to the next_url if it is
- we add a new authentic2.views.csrf_failure_view() which will be used through the setting CSRF_FAILURE_VIEW, this view will just reload the current page using a redirection and display a warning thourgh the messages framework that alerts the user that as he logged in since he loaded this page, the page became out of date.
- we removed CSRF protection on the registration view since it's a public page anyway and nothing can be gained from CSRF on the registration page.

Révisions associées

Révision 40b90493 - 13 janvier 2015 15:02 - Benjamin Dauvergne

Use setting CSRF_FAILURE_VIEW to prevent user seeing 403 on CSRF failure, instead redirect them to the same page and display a warning (refs #5617)

Révision d570b728 - 13 janvier 2015 15:15 - Benjamin Dauvergne

Allow validation of CSRF cookie to be done in view using a CBV mixin or an helper function (refs #5617)

Use the CBV for a do-nothing use or on a function based view you must
apply the decorators @csrf_exempt and @ensure_csrf_cookie on your view
(in this order) and use utils.csrf_token_check(request, form) to check
for the cookie before validating your form.

Révision 9290f3f4 - 13 janvier 2015 15:15 - Benjamin Dauvergne

Use new mixin on registration view to show a form error on CSRF token validation error instead of a redirect (refs #5617)

Révision 14a0e25e - 13 janvier 2015 15:15 - Benjamin Dauvergne

Update french translation (fixes #5617)

Révision 143528d0 - 13 janvier 2015 15:15 - Benjamin Dauvergne

Use new CSRF cookie validation on login view (refs #5617)

Révision 25ef99ff - 10 mars 2015 12:47 - Benjamin Dauvergne

Use setting CSRF_FAILURE_VIEW to prevent user seeing 403 on CSRF failure, instead redirect them to the same page and display a warning (refs #5617)

Révision 31c743d8 - 10 mars 2015 12:47 - Benjamin Dauvergne

Allow validation of CSRF cookie to be done in view using a CBV mixin or an helper function (refs #5617)

Use the CBV for a do-nothing use or on a function based view you must
apply the decorators @csrf_exempt and @ensure_csrf_cookie on your view
(in this order) and use utils.csrf_token_check(request, form) to check
for the cookie before validating your form.

Révision 0baa91cf - 10 mars 2015 12:47 - Benjamin Dauvergne

Use new mixin on registration view to show a form error on CSRF token validation error instead of a redirect (refs #5617)

Révision 8fd5446d - 10 mars 2015 12:47 - Benjamin Dauvergne

Update french translation (fixes #5617)

Révision f2573707 - 10 mars 2015 12:47 - Benjamin Dauvergne

Use new CSRF cookie validation on login view (refs #5617)

Historique

#1 - 02 octobre 2014 21:52 - Benjamin Dauvergne

- Fichier 0001-On-login-view-check-the-CSRF-cookie-only-after-check.patch ajouté

- Fichier 0002-Use-setting-CSRF_FAILURE_VIEW-to-prevent-user-seeing.patch ajouté

- Fichier 0003-If-the-user-is-already-logged-redirect-user-to-next-.patch ajouté

- Fichier 0004-Remove-CSRF-protection-from-registration-view-as-the.patch ajouté

- Fichier 0005-Update-french-translation-fixes-5617.patch ajouté

- Patch proposed changé de Non à Oui

#2 - 08 octobre 2014 17:07 - Benjamin Dauvergne

- Statut changé de Nouveau à En cours

- Assigné à mis à Benjamin Dauvergne

#3 - 09 janvier 2015 14:59 - Serghei Mihai

It works for me

#4 - 13 janvier 2015 15:19 - Benjamin Dauvergne

- Fichier 0001-Use-setting-CSRF_FAILURE_VIEW-to-prevent-user-seeing.patch ajouté

- Fichier 0002-Allow-validation-of-CSRF-cookie-to-be-done-in-view-u.patch ajouté

- Fichier 0003-Use-new-mixin-on-registration-view-to-show-a-form-er.patch ajouté

- Fichier 0004-Update-french-translation-fixes-5617.patch ajouté

- Fichier 0005-Use-new-CSRF-cookie-validation-on-login-view-refs-56.patch ajouté

I reworked my patch, the recipe will serve to other projects:

- I still change the default CSRF cookie validation view
- I added a CBV mixin and an utility function in order to merge CSRF validation inside form validation, CSRF errors are now reported as form errors
- I used the CBV on the registration view and the manual implementation in the default login/password frontend view

Here commes new patches, review is welcome.

#5 - 13 janvier 2015 15:21 - Benjamin Dauvergne

To test them, open a form (registration or login) in a tab, then open a new tab, login then logout in this tab, them come back to the first tab and try to use the form. The form must validate on first try. If it does not validate then it does not report CSRF validation errors, as the CSRF cookie will be updated after re-display of the form, and so you will not really test this patch.

#6 - 13 janvier 2015 18:25 - Benjamin Dauvergne

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

- % réalisé changé de 0 à 100

Appliqué par commit 14a0e25eed69f80c3c2a5bc9ce5a1d271e2ab38e.

#7 - 06 mars 2015 16:05 - Benjamin Dauvergne

- Version cible mis à 2.1.12

#8 - 06 mars 2015 16:24 - Benjamin Dauvergne

- Fichier 0001-On-login-view-check-the-CSRF-cookie-only-after-check.patch supprimé

#9 - 06 mars 2015 16:24 - Benjamin Dauvergne

- Fichier 0002-Use-setting-CSRF_FAILURE_VIEW-to-prevent-user-seeing.patch supprimé

#10 - 06 mars 2015 16:24 - Benjamin Dauvergne

- Fichier 0003-If-the-user-is-already-logged-redirect-user-to-next-.patch supprimé

#11 - 06 mars 2015 16:24 - Benjamin Dauvergne

- Fichier 0004-Remove-CSRF-protection-from-registration-view-as-the.patch supprimé

#12 - 06 mars 2015 16:24 - Benjamin Dauvergne

- Fichier 0005-Update-french-translation-fixes-5617.patch supprimé

#13 - 06 mars 2015 16:24 - Benjamin Dauvergne

- Fichier 0001-Use-setting-CSRF_FAILURE_VIEW-to-prevent-user-seeing.patch supprimé

#14 - 06 mars 2015 16:24 - Benjamin Dauvergne

- Fichier 0002-Allow-validation-of-CSRF-cookie-to-be-done-in-view-u.patch supprimé

#15 - 06 mars 2015 16:25 - Benjamin Dauvergne

- Fichier 0003-Use-new-mixin-on-registration-view-to-show-a-form-er.patch supprimé

#16 - 06 mars 2015 16:25 - Benjamin Dauvergne

- Fichier 0004-Update-french-translation-fixes-5617.patch supprimé

#17 - 06 mars 2015 16:25 - Benjamin Dauvergne

- Fichier 0005-Use-new-CSRF-cookie-validation-on-login-view-refs-56.patch supprimé

#18 - 06 mars 2015 16:25 - Benjamin Dauvergne

- Fichier 0001-Use-setting-CSRF_FAILURE_VIEW-to-prevent-user-seeing.patch ajouté

- Fichier 0002-Allow-validation-of-CSRF-cookie-to-be-done-in-view-u.patch ajouté

- Fichier 0003-Use-new-mixin-on-registration-view-to-show-a-form-er.patch ajouté

- Fichier 0004-Update-french-translation-fixes-5617.patch ajouté

- Fichier 0005-Use-new-CSRF-cookie-validation-on-login-view-refs-56.patch ajouté

- Statut changé de Résolu (à déployer) à Nouveau

- Priorité changé de Normal à Haut

Update to last master state.

#19 - 10 mars 2015 09:55 - Serghei Mihai

- Fichier 0002-Allow-validation-of-CSRF-cookie-to-be-done-in-view-u.patch ajouté

- Fichier 0004-Update-french-translation-fixes-5617.patch ajouté

- Fichier 0003-Use-new-mixin-on-registration-view-to-show-a-form-er.patch ajouté

Here are modified the patches 2, 3, 4 fixing some errors and adaptations to last master state

#20 - 10 mars 2015 12:49 - Benjamin Dauvergne

Thanks for updating patch to master.

#21 - 10 mars 2015 12:50 - Benjamin Dauvergne

- Statut changé de Nouveau à Résolu (à déployer)

Appliqué par commit 8fd5446dc0da2eccf48c02617527d8848be55501.

#22 - 13 mars 2015 17:10 - Benjamin Dauvergne

- Statut changé de Résolu (à déployer) à Fermé

Fichiers

0001-Use-setting-CSRF_FAILURE_VIEW-to-prevent-user-seeing.patch	1,97 ko	06 mars 2015	Benjamin Dauvergne

0002-Allow-validation-of-CSRF-cookie-to-be-done-in-view-u.patch	2,73 ko	06 mars 2015	Benjamin Dauvergne
0003-Use-new-mixin-on-registration-view-to-show-a-form-er.patch	1,96 ko	06 mars 2015	Benjamin Dauvergne
0004-Update-french-translation-fixes-5617.patch	1,91 ko	06 mars 2015	Benjamin Dauvergne
0005-Use-new-CSRF-cookie-validation-on-login-view-refs-56.patch	3,01 ko	06 mars 2015	Benjamin Dauvergne
0002-Allow-validation-of-CSRF-cookie-to-be-done-in-view-u.patch	2,93 ko	10 mars 2015	Serghei Mihai
0004-Update-french-translation-fixes-5617.patch	1,14 ko	10 mars 2015	Serghei Mihai
0003-Use-new-mixin-on-registration-view-to-show-a-form-er.patch	1,31 ko	10 mars 2015	Serghei Mihai