Authentic 2 - Bug #62868

/manage/ : en se reconnectant avec un utilisateur provenant d'un annuaire, crash lorsque l'annuaire ne reconnaît pas celui-ci

16 mars 2022 16:57 - Benjamin Renard

Statut:	En cours	**Début:**	16 mars 2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Paul Marillonnet	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Sur une nouvelle installation, lorsque je tente de me connecter en tant qu'un autre utilisateur, je tombe sur une erreur 500 :

```
mars 16 16:45:15 srv-idp-test-02 authentic2[1048]: 86.210.112.193 - r:7F4D11FEB7F0 ERROR Internal
Server Error: /su/BMnOcMYHQ3-1gHai3eHHUw/
                                                  Traceback (most recent call last):
                                                    File "/usr/lib/python3/dist-packages/django/c
ore/handlers/exception.py", line 34, in inner
                                                      response = get_response(request)
                                                    File "/usr/lib/python3/dist-packages/django/c
ore/handlers/base.py", line 115, in _get_response
                                                      response = self.process_exception_by_middle
ware(e, request)
                                                    File "/usr/lib/python3/dist-packages/django/c
ore/handlers/base.py", line 113, in _get_response
                                                      response = wrapped_callback(request, *callb
ack_args, **callback_kwargs)
                                                    File "/usr/lib/python3/dist-packages/django/v
iews/decorators/clickjacking.py", line 15, in wrapped_view
                                                      resp = view_func(*args, **kwargs)
                                                    File "/usr/lib/python3/dist-packages/django/v
iews/generic/base.py", line 71, in view
                                                      return self.dispatch(request, *args, **kwar
gs)
                                                    File "/usr/lib/python3/dist-packages/django/v
iews/generic/base.py", line 97, in dispatch
                                                      return handler(request, *args, **kwargs)
                                                    File "/usr/lib/python3/dist-packages/authenti
c2/views.py", line 1519, in get
                                                      return utils_misc.simulate_authentication(r
equest, user, 'su')
                                                    File "/usr/lib/python3/dist-packages/authenti
c2/utils/misc.py", line 1163, in simulate_authentication
                                                      user.backend = backend
                                                  AttributeError: 'NoneType' object has no attrib
ute 'backend'
```

À priori, cela semble venir du fait que, dans la vue *SuView* la méthode *authentic2.utils.misc.authenticate(request, user=user)* retourne *None*. Cette méthode est un wrapper sur *django.contrib.auth.authenticate* à priori et à en croire la doc Django, cette méthode retourne *None* lorsque l'authentification échoue.

Infos sur l'installation :

```
root@srv-idp-test-02:/etc/authentic2 # dpkg -l|grep -E '(authentic2|django)'
ii  authentic2                    3.79-1~eob100+1                  all          Versatile identit
y server Python module
ii  python3-authentic2            3.79-1~eob100+1                  all          Versatile identit
y server
ii  python3-django                2:2.2.24-1~bpo10+1               all          High-level Python
```

```
 web development framework
ii  python3-django-appconf        1.0.2-3                          all          helper class hand
ling configuration defaults of apps - Python 3.x
ii  python3-django-filters        2.1.0-1~bpo10+1                  all          filter Django Que
rySets based on user selections
ii  python3-django-guardian       1.4.9-2                          all          per object permis
sions of django for Python3
ii  python3-django-import-export  1.2.0.post2+gbd7e81a-1~eob100+1  all          Django applicatio
n and library for importing and exporting data
ii  python3-django-mellon         1.32-1~eob100+1                  all          SAML authenticati
on for Django
ii  python3-django-model-utils    3.1.1-1                          all          Django model mixi
ns and utilities — Python 3
ii  python3-django-ratelimit      2.0.0-1~eob100+1                 all          Cache-based rate-
limiting for Django
ii  python3-django-select2        5.10.0-1~eob100+2                all          Select2 option fi
elds for Django (Python 3)
ii  python3-django-tables2        1.21.2-1                         all          Table/data-grid f
ramework for Django (Python 3)
ii  python3-djangorestframework   3.9.0-1                          all          Web APIs for Djan
go, made easy for Python3
```

Historique

#1 - 21 septembre 2022 10:20 - Benjamin Renard

Je reproduis aujourd'hui cette erreur sur la version **4.29-1~eob100+1** pour Buster :

```
90.51.84.67 - r:7F069CF42470 ERROR Internal Server Error: /su/Jf7xx2RZQCWLpituD1-g4A/
                                        Traceback (most recent call last):
                                          File "/usr/lib/python3/dist-packages/django/core/handlers/exception
.py", line 34, in inner
                                            response = get_response(request)
                                          File "/usr/lib/python3/dist-packages/django/core/handlers/base.py",
 line 115, in _get_response
                                            response = self.process_exception_by_middleware(e, request)
                                          File "/usr/lib/python3/dist-packages/django/core/handlers/base.py",
 line 113, in _get_response
                                            response = wrapped_callback(request, *callback_args, **callback_k
wargs)
                                          File "/usr/lib/python3/dist-packages/django/views/decorators/clickj
acking.py", line 15, in wrapped_view
                                            resp = view_func(*args, **kwargs)
                                          File "/usr/lib/python3/dist-packages/django/views/generic/base.py",
 line 71, in view
                                            return self.dispatch(request, *args, **kwargs)
                                          File "/usr/lib/python3/dist-packages/django/views/generic/base.py",
 line 97, in dispatch
                                            return handler(request, *args, **kwargs)
                                          File "/usr/lib/python3/dist-packages/authentic2/views.py", line 160
7, in get
                                            return utils_misc.simulate_authentication(request, user, 'su')
                                          File "/usr/lib/python3/dist-packages/authentic2/utils/misc.py", lin
e 1188, in simulate_authentication
                                            user.backend = backend
                                        AttributeError: 'NoneType' object has no attribute 'backend'
```

Infos sur l'installation :

```
# dpkg -l|grep -E '(authentic2|django)'
ii  authentic2                    4.29-1~eob100+1              all          Versatile identity server Pyth
on module
ii  authentic2-supann             1.0-0                        all          adaptations and basic configur
ation for using authentic2 on a SUPANN directory
ii  python3-authentic2            4.29-1~eob100+1              all          Versatile identity server
ii  python3-django                2:2.2.24-1~bpo10+1           all          High-level Python web developm
ent framework
ii  python3-django-appconf        1.0.2-3                      all          helper class handling configur
ation defaults of apps - Python 3.x
ii  python3-django-filters        2.1.0-1~bpo10+1              all          filter Django QuerySets based
on user selections
```

```
ii  python3-django-guardian        1.4.9-2                          all          per object permissions of djan
go for Python3
ii  python3-django-import-export   1.2.0.post2+gbd7e81a-1~eob100+1 all          Django application and library
 for importing and exporting data
ii  python3-django-mellon          1.38-1~eob100+1                  all          SAML authentication for Django
ii  python3-django-model-utils     3.1.1-1                          all          Django model mixins and utilit
ies — Python 3
ii  python3-django-ratelimit       2.0.0-1~eob100+1                 all          Cache-based rate-limiting for
Django
ii  python3-django-select2         5.10.0-1~eob100+2                all          Select2 option fields for Djan
go (Python 3)
ii  python3-django-tables2         1.21.2-1                         all          Table/data-grid framework for
Django (Python 3)
ii  python3-djangorestframework    3.9.0-1+deb10u1                  all          Web APIs for Django, made easy
 for Python3
```

#2 - 21 septembre 2022 10:26 - Benjamin Renard

Je précise que sur une autre machine en Bullseye avec la même version, mais python3-django 2.2.26, ça fonctionne correctement. Ce serait une incompatibilité avec python3-django 2.2.24 ?

#3 - 21 septembre 2022 10:33 - Paul Marillonnet

- Tracker changé de Development à Bug

- Sujet changé de Erreur 500 lors de la connexion en tant qu'une autre personne à /manage/ : en se reconnectant avec un utilisateur provenant d'un annuaire, crash lorsque l'annuaire ne reconnaît pas celui-ci

Dans SuView, on vérifie une première fois que l'usager existe à la résolution du token.
Mais lorsqu'il provient du LDAP on cherche à l'authentifier. On vérifie pas à nouveau qu'il existe, il faudrait.

#4 - 21 septembre 2022 10:34 - Paul Marillonnet

- Statut changé de Nouveau à En cours

- Assigné à mis à Paul Marillonnet

Joli bug, je regarde.

#5 - 21 septembre 2022 11:18 - Paul Marillonnet

- Fichier 0001-manage-do-not-crash-while-trying-to-impersonate-stal.patch ajouté

- Statut changé de En cours à Solution proposée

- Patch proposed changé de Non à Oui

#6 - 21 septembre 2022 11:21 - Paul Marillonnet

Ça devrait éviter le crash. Je ne sais pas si ça a un lien avec la différence de version debian buster/bullseye, mais lors d'un des essais consistant à se reconnecter avec l'usager provenant du LDAP, ce dernier ne reconnaissait pas l'usager (peut-être l'annuaire indisponible à ce moment là ?). Il faut échouer proprement au lieu de crasher, c'est l'objet de ce patche.

#7 - 21 septembre 2022 12:23 - Benjamin Dauvergne

- Statut changé de Solution proposée à En cours

Tu ferais un test aussi au niveau de la vue qui initialise le lien pour ne pas arriver jusqu'à la 404 ? (authentic2.manager.user_views.UserSuView), je pense que vérifier que utils_misc.authenticate(request, user=user) != None suffit à s'assurer que ça marchera plus tard.

#8 - 23 septembre 2022 11:24 - Paul Marillonnet

- Fichier 0001-manage-do-not-crash-while-trying-to-impersonate-stal.patch ajouté

- Statut changé de En cours à Solution proposée

Benjamin Dauvergne a écrit :

> Tu ferais un test aussi au niveau de la vue qui initialise le lien pour ne pas arriver jusqu'à la 404 ? (authentic2.manager.user_views.UserSuView)

C'est déjà fait dans les deux tests au dessus (test_su_superuser_post et test_su_permission_ldap_user_authn_failed), je loupe un truc ?

> , je pense que vérifier que utils_misc.authenticate(request, user=user) != None suffit à s'assurer que ça marchera plus tard.

Ok, patch corrigé ici.

#9 - 23 septembre 2022 11:48 - Paul Marillonnet

Et donc j'avais loupé que le user = utils_misc.authenticate(request, user=user) est bien là pour quelque chose, sans quoi :

```
    def test_switch_user_ldap_user(slapd, settings, app, db, caplog):
        caplog.set_level(logging.DEBUG)  # force pytest to reset log level after test

        settings.LDAP_AUTH_SETTINGS = [
            {
                'url': [slapd.ldap_url],
                'binddn': force_text(slapd.root_bind_dn),
                'bindpw': force_text(slapd.root_bind_password),
                'basedn': 'o=ôrga',
                'use_tls': False,
                'attributes': ['carLicense'],
            }
        ]
        # get all users
        management.call_command('sync-ldap-users', verbosity=2)

        user = User.objects.get(username=USERNAME + '@ldap')
        url = switch_user.build_url(user)
        response = app.get(url).follow()
>       assert app.session['_auth_user_backend'] == 'authentic2.backends.ldap_backend.LDAPBackendPasswordLost'
E       AssertionError: assert 'authentic2.b....ModelBackend' == 'authentic2.b...dPasswordLost'
E         - authentic2.backends.ldap_backend.LDAPBackendPasswordLost
E         + authentic2.backends.models_backend.ModelBackend
```

C'est la première version du patch (#62868-5) qui revient donc pour relecture.

#10 - 20 octobre 2022 09:38 - Benjamin Dauvergne

- Statut changé de Solution proposée à En cours

Paul Marillonnet a écrit :

> Benjamin Dauvergne a écrit :
>
> > Tu ferais un test aussi au niveau de la vue qui initialise le lien pour ne pas arriver jusqu'à la 404 ?
> > (authentic2.manager.user_views.UserSuView)
>
> C'est déjà fait dans les deux tests au dessus (test_su_superuser_post et test_su_permission_ldap_user_authn_failed), je loupe un truc ?

Ok je t'ai perdu avec le mot "test", je veux dire ajouter une condition dans la vue "UserSuView" pour ne pas créer "su_url" si utils_misc.authenticate(request, user=user) == None et afficher directement que ce ne sera pas possible; ça ne sert à rien de filer un lien qui ne marche pas aux gens, on ne doit pas arriver jusqu'à la 404 dans le test authn_failed.

Fichiers

0001-manage-do-not-crash-while-trying-to-impersonate-stal.patch	3,13 ko 21 septembre 2022	Paul Marillonnet
0001-manage-do-not-crash-while-trying-to-impersonate-stal.patch	3,25 ko 23 septembre 2022	Paul Marillonnet