Authentic 2 - Development #62866

Erreur 500 peu explicite lors d'une tentative de reset de password

16 mars 2022 16:43 - Benjamin Renard

Statut:	Fermé	**Début:**	16 mars 2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Lorsqu'un utilisateur tente de réinitialiser son mot de passe, mais qu'il n'a pas d'adresse email connue, il se retrouve sur une page d'erreur peu explicite **Server Error (500)**. Il serait bien de mettre un message d'erreur un peu plus explicite sur le problème.

Révisions associées

Révision 01482579 - 29 avril 2022 12:16 - Benjamin Dauvergne

forms: show error if all accounts for reset have no email (#62866)

Révision 0cfd6ba7 - 29 avril 2022 12:16 - Benjamin Dauvergne

forms: fail cleanly if LDAP user cannot be retrieved (#62866)

Historique

#1 - 16 mars 2022 21:06 - Benjamin Dauvergne

Si c'est une 500 c'est un bug, tu n'aurais pas une trace dans un mail d'erreur ?

#2 - 17 mars 2022 09:32 - Benjamin Renard

Benjamin Dauvergne a écrit :

> Si c'est une 500 c'est un bug, tu n'aurais pas une trace dans un mail d'erreur ?

```
mars 17 09:32:01 srv-idp-test-02 authentic2[13169]: 86.210.112.193 - r:7FB5E80574E0 ERROR Internal Server Erro
r: /accounts/password/reset/
                                                  Traceback (most recent call last):
                                                    File "/usr/lib/python3/dist-packages/django/core/handler
s/exception.py", line 34, in inner
                                                      response = get_response(request)
                                                    File "/usr/lib/python3/dist-packages/django/core/handler
s/base.py", line 115, in _get_response
                                                      response = self.process_exception_by_middleware(e, req
uest)
                                                    File "/usr/lib/python3/dist-packages/django/core/handler
s/base.py", line 113, in _get_response
                                                      response = wrapped_callback(request, *callback_args, *
*callback_kwargs)
                                                    File "/usr/lib/python3/dist-packages/django/views/decora
tors/clickjacking.py", line 15, in wrapped_view
                                                      resp = view_func(*args, **kwargs)
                                                    File "/usr/lib/python3/dist-packages/django/views/generi
c/base.py", line 71, in view
                                                      return self.dispatch(request, *args, **kwargs)
                                                    File "/usr/lib/python3/dist-packages/django/views/generi
c/base.py", line 97, in dispatch
                                                      return handler(request, *args, **kwargs)
                                                    File "/usr/lib/python3/dist-packages/django/views/generi
c/edit.py", line 142, in post
                                                      return self.form_valid(form)
                                                    File "/usr/lib/python3/dist-packages/authentic2/views.py
", line 800, in form_valid
                                                      form.save()
                                                    File "/usr/lib/python3/dist-packages/authentic2/forms/pa
sswords.py", line 83, in save
```

```
                                                  user=user, name='can_reset_password', default=user.has
_usable_password()
                                              AttributeError: 'NoneType' object has no attribute 'has_us
able_password'
```

#3 - 23 mars 2022 06:51 - Benjamin Dauvergne

Donc le bug ici c'est qu'on ne contrôle pas que la recherche de l'utilisateur dans le LDAP de l'utilisateur ait réussie ou pas :

```
            if user.userexternalid_set.exists():
                user = utils_misc.authenticate(user=user)  # get LDAPUser
                can_reset_password = utils_misc.get_user_flag(
                    user=user, name='can_reset_password', default=user.has_usable_password()
                )
```

on doit pouvoir envoyer un mail d'erreur dans ce cas.

#4 - 23 mars 2022 06:58 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#5 - 23 mars 2022 07:45 - Benjamin Dauvergne

- Fichier 0001-forms-fail-cleanly-if-LDAP-user-cannot-be-retrieved-.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

#6 - 14 avril 2022 16:06 - Paul Marillonnet

- Statut changé de Solution proposée à Solution validée

Top.

#7 - 14 avril 2022 19:36 - Benjamin Renard

En fait, le patch proposé ne fonctionne pas dans le cas où l'utilisateur n'est pas trouvé dans l'annuaire LDAP. On se retrouve alors avec l'exception suivante :

```
ERROR Internal Server Error: /accounts/password/reset/
                                                Traceback (most recent call last):
                                                  File "/usr/lib/python3/dist-packages/django/core/handle
rs/exception.py", line 34, in inner
                                                    response = get_response(request)
                                                  File "/usr/lib/python3/dist-packages/django/core/handle
rs/base.py", line 115, in _get_response
                                                    response = self.process_exception_by_middleware(e, re
quest)
                                                  File "/usr/lib/python3/dist-packages/django/core/handle
rs/base.py", line 113, in _get_response
                                                    response = wrapped_callback(request, *callback_args,
**callback_kwargs)
                                                  File "/usr/lib/python3/dist-packages/django/views/decor
ators/clickjacking.py", line 15, in wrapped_view
                                                    resp = view_func(*args, **kwargs)
                                                  File "/usr/lib/python3/dist-packages/django/views/gener
ic/base.py", line 71, in view
                                                    return self.dispatch(request, *args, **kwargs)
                                                  File "/usr/lib/python3/dist-packages/django/views/gener
ic/base.py", line 97, in dispatch
                                                    return handler(request, *args, **kwargs)
                                                  File "/usr/lib/python3/dist-packages/django/views/gener
ic/edit.py", line 142, in post
                                                    return self.form_valid(form)
                                                  File "/usr/lib/python3/dist-packages/authentic2/views.p
y", line 800, in form_valid
                                                    form.save()
                                                  File "/usr/lib/python3/dist-packages/authentic2/forms/p
asswords.py", line 92, in save
                                                    login_url = utils_misc.get_token_login_url(user)
                                                  File "/usr/lib/python3/dist-packages/authentic2/utils/m
isc.py", line 747, in get_token_login_url
                                                    token = Token.create('login', {'user': user.pk})
                                                AttributeError: 'NoneType' object has no attribute 'pk'
```

Par ailleurs, ici, je comprends pas trop pourquoi cette erreur se produit, car l'utilisateur existe bien et a bien un email. Sauriez-vous me dire ce que tente de faire *utils_misc.authenticate(user=user)* pour que j'essaye de comprendre pourquoi ça coince dans mon cas ? Il s'agit d'un AD et pour le coup, je n'ai pas accès aux logs pour voir la recherche qu'Authentic tente d'y faire (enfin, je suppose).

#8 - 22 avril 2022 10:15 - Benjamin Dauvergne

Si la recherche a échoué il devrait y avoir un log d'erreur de la part du backend LDAP d'authentic juste avant la trace. En général ça indique que l'AD n'est pas accessible sans login/mdp et que seul le backend LDAP est aftif; donc le reset de mot de passe est impossible, il vaut mieux le désactiver.

#9 - 22 avril 2022 11:14 - Benjamin Dauvergne

- Fichier 0001-forms-fail-cleanly-if-LDAP-user-cannot-be-retrieved-.patch ajouté

- Statut changé de Solution validée à Solution proposée

Ce dernier patch prend en compte le cas remonté par brenard.

#10 - 25 avril 2022 10:41 - Benjamin Dauvergne

- Fichier 0001-forms-fail-cleanly-if-LDAP-user-cannot-be-retrieved-.patch ajouté

Retiré le if user: inutile puisqu'il est toujours là.

#11 - 25 avril 2022 10:55 - Benjamin Renard

Benjamin Dauvergne a écrit :

> Si la recherche a échoué il devrait y avoir un log d'erreur de la part du backend LDAP d'authentic juste avant la trace. En général ça indique que l'AD n'est pas accessible sans login/mdp et que seul le backend LDAP est aftif; donc le reset de mot de passe est impossible, il vaut mieux le désactiver.

Je viens de reproduire l'erreur et après vérification, je n'ai aucune erreur LDAP avant l'exception. Je ne vois pas trop dans quelle situation le reset du mdp ne serait pas possible sur l'AD : quand tu parles de login/mdp, tu parles de ceux de l'utilisateur ou ceux d'un compte de service j'imagine ? Dans mon cas, j'ai bien un compte de service, donc le compte doit être trouvable normalement, non ?

Par ailleurs, j'ai testé ensuite de mettre ton premier puis ton second patch et le second ne passe pas, car je me retrouve avec l'erreur et l'exception suivante :

```
avril 25 10:44:59 srv-idp-prod-02 authentic2[18880]: 192.168.66.1 - r:7F2E1DC557F0 INFO password reset failed
for user "None": account is from ldap but it could not be retrieved
avril 25 10:44:59 srv-idp-prod-02 authentic2[18880]: 192.168.66.1 - r:7F2E1DC557F0 ERROR Internal Server Error
: /accounts/password/reset/
                                                    Traceback (most recent call last):
                                                      File "/usr/lib/python3/dist-packages/django/core/handle
rs/exception.py", line 34, in inner
                                                        response = get_response(request)
                                                      File "/usr/lib/python3/dist-packages/django/core/handle
rs/base.py", line 115, in _get_response
                                                        response = self.process_exception_by_middleware(e, re
quest)
                                                      File "/usr/lib/python3/dist-packages/django/core/handle
rs/base.py", line 113, in _get_response
                                                        response = wrapped_callback(request, *callback_args,
**callback_kwargs)
                                                      File "/usr/lib/python3/dist-packages/django/views/decor
ators/clickjacking.py", line 15, in wrapped_view
                                                        resp = view_func(*args, **kwargs)
                                                      File "/usr/lib/python3/dist-packages/django/views/gener
ic/base.py", line 71, in view
                                                        return self.dispatch(request, *args, **kwargs)
                                                      File "/usr/lib/python3/dist-packages/django/views/gener
ic/base.py", line 97, in dispatch
                                                        return handler(request, *args, **kwargs)
                                                      File "/usr/lib/python3/dist-packages/django/views/gener
ic/edit.py", line 142, in post
                                                        return self.form_valid(form)
                                                      File "/usr/lib/python3/dist-packages/authentic2/views.p
y", line 835, in form_valid
                                                        form.save()
                                                      File "/usr/lib/python3/dist-packages/authentic2/forms/p
asswords.py", line 95, in save
                                                        login_url = utils_misc.get_token_login_url(user)
                                                      File "/usr/lib/python3/dist-packages/authentic2/utils/m
isc.py", line 751, in get_token_login_url
```

```
                                                    token = Token.create('login', {'user': user.pk})
                                                AttributeError: 'NoneType' object has no attribute 'pk'
```

Ici, il semble que ce soit *ldap_user = utils_misc.authenticate(user=user)* qui retourne *None*, donc *user* n'est pas toujours défini.

Avec ton premier patch, je n'ai plus d'erreur et j'ai la page m'indiquant qu'un mail m'a été envoyé avec des instructions.

#12 - 25 avril 2022 13:29 - Benjamin Dauvergne

Tu as du mélangé les patchs, le dernier ne peut pas avoir user = None puisque c'est ldap_user = misc.authenticate(....

#13 - 25 avril 2022 14:33 - Benjamin Renard

Benjamin Dauvergne a écrit :

> Tu as du mélangé les patchs, le dernier ne peut pas avoir user = None puisque c'est ldap_user = misc.authenticate(....

Oui mais en ligne 86, on a *user = ldap_user* et comme expliqué ça semble être *misc.authenticate()* qui retourne *None*.

#14 - 25 avril 2022 15:58 - Benjamin Dauvergne

- Fichier 0001-forms-fail-cleanly-if-LDAP-user-cannot-be-retrieved-.patch ajouté

Ouaip mea culpa, le code est affreux, dernière version j'espère.

#15 - 25 avril 2022 17:28 - Benjamin Renard

Benjamin Dauvergne a écrit :

> Ouaip mea culpa, le code est affreux, dernière version j'espère.

:) C'est mieux, mais j'ai eu à présent une nouvelle erreur 500 :

```
avril 25 16:16:04 srv-idp-prod-02 authentic2[23187]: 192.168.66.1 - r:7F21EF8BAC50 ERROR Internal Server Error
: /accounts/password/reset/
                                                Traceback (most recent call last):
                                                  File "/usr/lib/python3/dist-packages/django/core/handle
rs/exception.py", line 34, in inner
                                                    response = get_response(request)
                                                  File "/usr/lib/python3/dist-packages/django/core/handle
rs/base.py", line 115, in _get_response
                                                    response = self.process_exception_by_middleware(e, re
quest)
                                                  File "/usr/lib/python3/dist-packages/django/core/handle
rs/base.py", line 113, in _get_response
                                                    response = wrapped_callback(request, *callback_args,
**callback_kwargs)
                                                  File "/usr/lib/python3/dist-packages/django/views/decor
ators/clickjacking.py", line 15, in wrapped_view
                                                    resp = view_func(*args, **kwargs)
                                                  File "/usr/lib/python3/dist-packages/django/views/gener
ic/base.py", line 71, in view
                                                    return self.dispatch(request, *args, **kwargs)
                                                  File "/usr/lib/python3/dist-packages/django/views/gener
ic/base.py", line 97, in dispatch
                                                    return handler(request, *args, **kwargs)
                                                  File "/usr/lib/python3/dist-packages/django/views/gener
ic/edit.py", line 142, in post
                                                    return self.form_valid(form)
                                                  File "/usr/lib/python3/dist-packages/authentic2/views.p
y", line 835, in form_valid
                                                    form.save()
                                                  File "/usr/lib/python3/dist-packages/authentic2/forms/p
asswords.py", line 94, in save
                                                    login_url = utils_misc.get_token_login_url(user)
                                                  File "/usr/lib/python3/dist-packages/authentic2/utils/m
isc.py", line 752, in get_token_login_url
                                                    return make_url('token_login', kwargs={'token': token
.uuid_b64url}, absolute=True)
                                                  File "/usr/lib/python3/dist-packages/authentic2/utils/m
isc.py", line 347, in make_url
                                                    raise TypeError('make_url() absolute cannot be used w
ithout request')
```

```
                                                    TypeError: make_url() absolute cannot be used without req
uest
```

Pour le coup, c'était réglable dans la configuration en définissant la variable *SITE_BASE_URL*. Ça serait cool d'ajuster l'erreur retournée par la méthode *make_url()* pour quelques choses du genre :

make_url() absolute cannot be used without request and without SITE_BASE_URL defined in configuration

Cela dit, maintenant l'application se comporte correctement, mais je ne savais toujours pas pourquoi l'utilisateur était introuvable dans l'AD… J'ai fini par comprendre mon problème : le backend d'authentification *authentic2.backends.ldap_backend.LDAPBackendPasswordLost* n'était pas actif (absent de *AUTHENTICATION_BACKENDS*). Ce serait cool d'avoir un message d'erreur explicite pour ça et au passage de gérer correctement l'utilisateur qui n'a pas d'email. Ci-dessous un exemple qui est déjà plus pratique :

```
        for user in active_users:
            if user.userexternalid_set.exists():
                ldap_user = utils_misc.authenticate(user=user)  # get LDAPUser
                if isinstance(ldap_user, LDAPUser):
                    can_reset_password = utils_misc.get_user_flag(
                        user=ldap_user, name='can_reset_password', default=ldap_user.has_usable_password()
                    )
                    message = 'account is from ldap and password reset is forbidden'
                    if can_reset_password and not ldap_user.email:
                        can_reset_password = False
                        message = 'account is from ldap, password reset is granted, but user have no email'
                elif 'authentic2.backends.ldap_backend.LDAPBackendPasswordLost' not in settings.AUTHENTICATION
_BACKENDS:
                    can_reset_password = False
                    message = 'account is from ldap but the authentic2.backends.ldap_backend.LDAPBackendPasswo
rdLost authentication backend is not enabled. Add it in AUTHENTICATION_BACKENDS to enable.'
                else:
                    can_reset_password = False
                    message = 'account is from ldap but it could not be retrieved'
                if not can_reset_password:
                    log_message = 'password reset failed for user "%r": %s' % message
                    logger.info(log_message, user)
                    login_url = utils_misc.get_token_login_url(user)
                    utils_misc.send_templated_mail(
                        user, ['authentic2/password_reset_ldap'], {'login_url': login_url}
                    )
                    continue
```

Dans le cas d'un utilisateur sans email, c'est pas idéal, car c'est invisible pour lui au final (on dit qu'on lui envoie un mail, mais on le fait pas, car on peut pas). Je sais pas trop ce qu'on pourrait faire sans trop dévoiler sur l'utilisateur. À minima, je me dis que ce serait cool d'avoir une trace dans le journal des évènements de l'utilisateur pour qu'un admin est facilement l'info. Qu'en penses-tu ? Il faudrait peut-être juste avoir un truc pour éviter le floading ici.

#16 - 25 avril 2022 17:41 - Benjamin Renard

- Fichier 0001-password-reset-Fix-error-reporting-when-A2_USER_CAN_.patch ajouté

Je sais pas si tu veux ça dans un ticket dédié, mais on a également un problème dans la vue avec la gestion des erreurs quand *A2_USER_CAN_RESET_PASSWORD_BY_USERNAME* est actif : on tente de mettre l'erreur sur le champ *email* alors que le champ est *email_or_username* dans ce cas. Ci-joint un patch qui corrige ça.

#17 - 26 avril 2022 13:09 - Benjamin Dauvergne

Benjamin Renard a écrit :

> Je sais pas si tu veux ça dans un ticket dédié, mais on a également un problème dans la vue avec la gestion des erreurs quand *A2_USER_CAN_RESET_PASSWORD_BY_USERNAME* est actif : on tente de mettre l'erreur sur le champ *email* alors que le champ est *email_or_username* dans ce cas. Ci-joint un patch qui corrige ça.

Met ça dans un autre ticket, stp, ainsi je pourrai le valider et le pousser dans son coin.

#18 - 27 avril 2022 11:29 - Benjamin Renard

Benjamin Dauvergne a écrit :

> Benjamin Renard a écrit :
>
> > Je sais pas si tu veux ça dans un ticket dédié, mais on a également un problème dans la vue avec la gestion des erreurs quand *A2_USER_CAN_RESET_PASSWORD_BY_USERNAME* est actif : on tente de mettre l'erreur sur le champ *email* alors que le champ est *email_or_username* dans ce cas. Ci-joint un patch qui corrige ça.

> Met ça dans un autre ticket, stp, ainsi je pourrai le valider et le pousser dans son coin.

Fait : https://dev.entrouvert.org/issues/64607

#19 - 28 avril 2022 16:12 - Benjamin Dauvergne

- Fichier 0002-forms-fail-cleanly-if-LDAP-user-cannot-be-retrieved-.patch ajouté

- Fichier 0001-forms-show-error-if-all-accounts-for-reset-have-no-e.patch ajouté

J'ai séparé la question de l'absence d'un compte avec une adresse mail dans un premier patch, pour retourner l'information à l'utilisateur dans ce cas. Dans le deuxième patch on ne fait que logger le problème si parmi les comptes trouvés seulement certains n'ont pas d'email. J'ai du ajouter un booléen "email_sent" pour dans le cas où aucune notification par mail ne partirait envoyer un mail d'information à l'email soumise pour l'informer qu'aucun compte n'existe.

#20 - 28 avril 2022 16:27 - Benjamin Renard

Benjamin Dauvergne a écrit :

> J'ai séparé la question de l'absence d'un compte avec une adresse mail dans un premier patch, pour retourner l'information à l'utilisateur dans ce cas. Dans le deuxième patch on ne fait que logger le problème si parmi les comptes trouvés seulement certains n'ont pas d'email. J'ai du ajouter un booléen "email_sent" pour dans le cas où aucune notification par mail ne partirait envoyer un mail d'information à l'email soumise pour l'informer qu'aucun compte n'existe.

Top, je viens de faire le test des deux et ça marche nikel.

#21 - 28 avril 2022 17:47 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

Ok je m'autovalide suite à ce bon retour, je pousserai ça vendredi et quand pylint sera content.

#22 - 29 avril 2022 12:17 - Benjamin Dauvergne

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

```
commit 0cfd6ba7b58b695b2967dfd7f261e9d9887af341
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Wed Mar 23 06:59:28 2022 +0100

    forms: fail cleanly if LDAP user cannot be retrieved (#62866)

commit 0148257950db873db09a5c2532fe99452ae69c26
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Thu Apr 28 15:57:30 2022 +0200

    forms: show error if all accounts for reset have no email (#62866)
```

#23 - 04 mai 2022 09:14 - Transition automatique

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

#24 - 10 juillet 2022 04:42 - Transition automatique

Automatic expiration

Fichiers

0001-forms-fail-cleanly-if-LDAP-user-cannot-be-retrieved-.patch	4,93 ko	23 mars 2022	Benjamin Dauvergne
0001-forms-fail-cleanly-if-LDAP-user-cannot-be-retrieved-.patch	5,46 ko	22 avril 2022	Benjamin Dauvergne
0001-forms-fail-cleanly-if-LDAP-user-cannot-be-retrieved-.patch	5,16 ko	25 avril 2022	Benjamin Dauvergne
0001-forms-fail-cleanly-if-LDAP-user-cannot-be-retrieved-.patch	5,12 ko	25 avril 2022	Benjamin Dauvergne
0001-password-reset-Fix-error-reporting-when-A2_USER_CAN_.patch	2,36 ko	25 avril 2022	Benjamin Renard
0002-forms-fail-cleanly-if-LDAP-user-cannot-be-retrieved-.patch	6,36 ko	28 avril 2022	Benjamin Dauvergne
0001-forms-show-error-if-all-accounts-for-reset-have-no-e.patch	2,79 ko	28 avril 2022	Benjamin Dauvergne