Authentic 2 - Development #63831

inclure un indicateur de force à la saisie d'un mot de passe

12 avril 2022 11:17 - Frédéric Péters

Statut:	Fermé	**Début:**	12 avril 2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Corentin Séchet	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Dans les reco NIST, après #63830,

> Verifiers SHOULD offer guidance to the subscriber, such as a password-strength meter [Meters], to assist the user in choosing a strong memorized secret. This is particularly important following the rejection of a memorized secret on the above list as it discourages trivial modification of listed (and likely very weak) memorized secrets [Blacklists].
> [Meters] → https://pages.nist.gov/800-63-3/sp800-63b.html#meters → https://www.ndss-symposium.org/ndss2014/programme/very-weak-very-strong-analyzing-password-strength-meters/

Révisions associées

Révision f372225e - 31 août 2022 14:52 - Corentin Séchet

misc: use a template for NewPasswordInput (#63831)

Révision 5de83a83 - 07 septembre 2022 11:58 - Corentin Séchet

misc: add password strength meter in NewPasswordInput (#63831)

Révision 4bb8877f - 07 septembre 2022 11:59 - Corentin Séchet

misc: generate hints from zxcvbn report (#63831)

Historique

#1 - 12 avril 2022 11:40 - Frédéric Péters

Cité dans le papier, https://github.com/dwolfhub/zxcvbn-python, qui pourrait éventuellement être aussi utile pour #63830 (histoire d'avoir une cohérence entre validation et mesure de la force).

#2 - 14 juin 2022 11:34 - Corentin Séchet

- Assigné à mis à Corentin Séchet

#3 - 27 juin 2022 17:39 - Corentin Séchet

J'ai pushé une branche avec ce que j'ai fait pour l'instant, mais il y a plusieurs loups là dessus :

- La librairie zxcvbn utilise gettext, mais ne fourni pas les traductions en français. Il faudrait les maintenir nous même, je ne sais pas s'il y a un moyen satisfaisant de faire ça.
- Après discussions avec Thomas J. sur l'ergonomie : c'est compliqué de présenter les règles en dur qui existent déjà (minuscules / majuscules / chiffres) et des conseils venant de zxcvbn qui apparaissent en fonction de ce qu'on a tapé (par exemple : "ajoutez un mot ou deux", "évitez les séquences"). J'ai mis tous les retours au même niveau et c'est assez déroutant puisqu'on a pas de retour clair sur le fait que le mot de passe est valide ou non.
- D'après Thomas J. il faudrait ajouter la possibilité d'afficher / masquer le mot de passe via un bouton.

Après discussion, on évoquait la possibilité de supprimer les anciens critères et de se baser uniquement sur une force minimale de mot de passe venant de zxcvbn.

#4 - 27 juin 2022 17:49 - Frédéric Péters

> La librairie zxcvbn utilise gettext, mais ne fourni pas les traductions en français. Il faudrait les maintenir nous même, je ne sais pas s'il y a un moyen satisfaisant de faire ça

On peut dupliquer les chaines et les faire porter par le .po/.mo d'authentic.

> Après discussions avec Thomas J. sur l'ergonomie : c'est compliqué de présenter les règles en dur qui existent déjà (minuscules / majuscules / chiffres) et des conseils venant de zxcvbn qui apparaissent en fonction de ce qu'on a tapé (par exemple : "ajoutez un mot ou deux", "évitez les séquences"). J'ai mis tous les retours au même niveau et c'est assez déroutant puisqu'on a pas de retour clair sur le fait que le mot de passe est valide ou non.

Pour moi totalement on devrait pouvoir fonctionner soit avec les anciens critères "par habitude", soit avec cette unique validation globale, conforme aux recommandations NIST; pas tenter le mix. (ce qui devrait déjà être ok juste via la config).

> D'après Thomas J. il faudrait ajouter la possibilité d'afficher / masquer le mot de passe via un bouton.

Ce serait un autre ticket. (qui peut citer le paragraphe un peu plus bas dans 5.1.1.2 du document du NIST).

#5 - 28 juin 2022 17:35 - Benjamin Dauvergne

Frédéric Péters a écrit :

> > La librairie zxcvbn utilise gettext, mais ne fourni pas les traductions en français. Il faudrait les maintenir nous même, je ne sais pas s'il y a un moyen satisfaisant de faire ça
>
> On peut dupliquer les chaines et les faire porter par le .po/.mo d'authentic.

Il me semble que Django n'utilise pas catalogue des messages systèmes donc ça ne suffirait pas je pense, il faudrait monkeypatcher zxcvbn.feedback._ pour que ça appelle l'implémentation gettext de Django en plus.

> > Après discussions avec Thomas J. sur l'ergonomie : c'est compliqué de présenter les règles en dur qui existent déjà (minuscules / majuscules / chiffres) et des conseils venant de zxcvbn qui apparaissent en fonction de ce qu'on a tapé (par exemple : "ajoutez un mot ou deux", "évitez les séquences"). J'ai mis tous les retours au même niveau et c'est assez déroutant puisqu'on a pas de retour clair sur le fait que le mot de passe est valide ou non.

Pour moi les deux choses ne sont pas au même niveau, il y a les contraintes dures et les conseils liés à la force, ce sont deux choses distinctes. Il faudrait revoir ça et que l'API renvoie séparément, les checks comme actuellement, la force et les conseils pour améliorer celle-ci.

Au niveau affichage on pourrait ne pas afficher la force et les conseils tant que tout ne valide pas et une fois que ça valide ne plus afficher les contraintes valides et uniquement la force et les conseils (après ça peut faire arbre de noël quand on édite un peu vite...).

#6 - 28 juin 2022 17:45 - Frédéric Péters

> Pour moi les deux choses ne sont pas au même niveau, il y a les contraintes dures et les conseils liés à la force, ce sont deux choses distinctes. Il faudrait revoir ça et que l'API renvoie séparément, les checks comme actuellement, la force et les conseils pour améliorer celle-ci.

J'invite à lire le document du NIST, il y a juste une reco sur la longueur, et ensuite "Verifiers SHOULD NOT impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorized secrets."; de là ma perspective de la désactivation des critères pour au final avoir une seule indication.

#7 - 28 juin 2022 18:10 - Benjamin Dauvergne

Frédéric Péters a écrit :

> J'invite à lire le document du NIST, il y a juste une reco sur la longueur, et ensuite "Verifiers SHOULD NOT impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorized secrets."; de là ma perspective de la désactivation des critères pour au final avoir une seule indication.

Ça me va d'en faire la politique par défaut mais :

1. certains clients n'en ont rien à faire du NIST et se référeront à d'autres autorités techniques qui diront autre chose (genre l'ANSSI ou la dernière lubie de leur RSSI)
2. il y aura toujours donc au moins un critère absolu qui sera la longueur et on ne peut pas le présenter gentiment sous forme de hint, ça doit être en rouge (ne serait-ce que pour l'accessibilité) après ça me va qu'on renvoie la présentation ainsi :

- si les critères booléens ne valident pas, un score de zéro et des conseils en rouge concernant ces critères
- si les critères booléens valident, on affiche juste le score et les conseils

Pour la configuration par défaut on met comme seul configuration le score et la longueur dans /manage/authenticators et au niveau des OUs et on laisse au fin fond des settings les histoires de minuscules, majucules&co pour les psychorigides.

Il faudrait surtout voir comment conserver le paramétrage actuels pour les instances actuelles mais avoir le nouveau paramétrage dans les nouvelles instances (sinon on ne migrera jamais vers ça).

#8 - 28 juin 2022 18:15 - Frédéric Péters

Ok quand j'écrivais : « on devrait pouvoir fonctionner soit avec les anciens critères "par habitude", soit avec cette unique validation globale » ça n'était pas pour dire qu'il fallait par défaut cette validation globale.

#9 - 29 juin 2022 12:42 - Corentin Séchet

- Fichier 0001-misc-add-password-strength-meter-63831.patch ajouté

- Fichier authentic_screenshot.png ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

Benjamin Dauvergne a écrit :

> Il me semble que Django n'utilise pas catalogue des messages systèmes donc ça ne suffirait pas je pense, il faudrait monkeypatcher zxcvbn.feedback._ pour que ça appelle l'implémentation gettext de Django en plus.

On peut peut-être repasser les chaînes dans le gettext Django de notre côté ?

> Pour moi les deux choses ne sont pas au même niveau, il y a les contraintes dures et les conseils liés à la force, ce sont deux choses distinctes. Il faudrait revoir ça et que l'API renvoie séparément, les checks comme actuellement, la force et les conseils pour améliorer celle-ci.
>
> Au niveau affichage on pourrait ne pas afficher la force et les conseils tant que tout ne valide pas et une fois que ça valide ne plus afficher les contraintes valides et uniquement la force et les conseils (après ça peut faire arbre de noël quand on édite un peu vite...).

Ce que j'ai fait hier (avant de lire vos commentaires, donc le patch n'est pas à prendre comme une proposition aboutie), c'est d'afficher uniquement la force et les conseils si le paramètre A2_PASSWORD_POLICY_MIN_STRENGTH est défini, utiliser l'ancien système sinon. L'API renvoie donc des choses différentes selon les paramètres, ce qui est discutable. Par contre, l'ancien système restera tel quel tant que le paramètre A2_PASSWORD_POLICY_MIN_STRENGTH n'est pas défini.

> 2. il y aura toujours donc au moins un critère absolu qui sera la longueur et on ne peut pas le présenter gentiment sous forme de hint, ça doit être en rouge (ne serait-ce que pour l'accessibilité) après ça me va qu'on renvoie la présentation ainsi :
> si les critères booléens ne valident pas, un score de zéro et des conseils en rouge concernant ces critères
> si les critères booléens valident, on affiche juste le score et les conseils

Si pas d'objection, je peux partir là dessus.

Note à côté : la fonction password_help_text et les styles associés deviennent conséquents, je ne sais pas si ça serait possible et s'il vaudrait mieux de bouger tout ça dans un gabarit.

#10 - 25 juillet 2022 14:50 - Benjamin Dauvergne

- Statut changé de Solution proposée à En cours

Corentin Séchet a écrit :

> Benjamin Dauvergne a écrit :
>
> > Il me semble que Django n'utilise pas catalogue des messages systèmes donc ça ne suffirait pas je pense, il faudrait monkeypatcher zxcvbn.feedback._ pour que ça appelle l'implémentation gettext de Django en plus.
>
> On peut peut-être repasser les chaînes dans le gettext Django de notre côté ?

Oui il faut essayer ça va certainement marcher, reste que ce ne sera pas évident de maintenir les chaînes de notre coté si elles bougent dans zxcbn.

> Ce que j'ai fait hier (avant de lire vos commentaires, donc le patch n'est pas à prendre comme une proposition aboutie), c'est d'afficher uniquement la force et les conseils si le paramètre A2_PASSWORD_POLICY_MIN_STRENGTH est défini, utiliser l'ancien système sinon. L'API renvoie donc des choses différentes selon les paramètres, ce qui est discutable. Par contre, l'ancien système restera tel quel tant que le paramètre A2_PASSWORD_POLICY_MIN_STRENGTH n'est pas défini.

Ok.

> 2. il y aura toujours donc au moins un critère absolu qui sera la longueur et on ne peut pas le présenter gentiment sous forme de hint, ça doit être en rouge (ne serait-ce que pour l'accessibilité) après ça me va qu'on renvoie la présentation ainsi :
> si les critères booléens ne valident pas, un score de zéro et des conseils en rouge concernant ces critères
> si les critères booléens valident, on affiche juste le score et les conseils

> Si pas d'objection, je peux partir là dessus.

Go.

> Note à côté : la fonction password_help_text et les styles associés deviennent conséquents, je ne sais pas si ça serait possible et s'il vaudrait mieux de bouger tout ça dans un gabarit.

Oui tu as raison, ça peut mériter un PasswordInput spécifique avec son template qui va bien, ce sera plus facile à maintenir.

#11 - 02 septembre 2022 10:45 - Corentin Séchet

- Fichier 0001-misc-use-a-template-for-NewPasswordInput-63831.patch ajouté

- Fichier 0002-misc-add-password-strength-meter-in-NewPasswordInput.patch ajouté

- Fichier 0003-misc-generate-hints-from-zxcvbn-report-63831.patch ajouté

- Statut changé de En cours à Solution proposée

Nécessite #63830

Patches :

1. Utilisation d'un gabarit pour NewPasswordInput

2. Le contrôle à proprement parler

- Si A2_PASSWORD_POLICIY_MIN_STRENGTH n'est pas défini, on garde l'ancien système, en front comme en back. Sinon on affiche uniquement le nouveau contrôle
- On teste la longueur du mot de passe, si elle est trop courte on ne teste pas la force, on la met à 0 et on demande d'entrer un mot de passe plus long.

3. Création des hints d'après le rapport de zxcvbn. En fait, la méthode qui génère les hints dans zxcvbn est assez bidon. J'ai préféré le faire nous même : les traductions seront gérées proprement comme ça et on peut utiliser la formulation qu'on veut.

A l'usage, je me demande si forcer une longueur même avec le test de force ne fait pas double emploi : de toutes façons c'est testé par zxcvbn, un mot de passe "good" ne peut pas être en dessous de 8 caractères par ex. Ça permettrait aussi d'avoir les hints dès que l'utilisateur commence à taper son mot de passe, i.e ne pas attendre qu'il ai finit de taper "P@ssword1" pour lui dire que c'est pas un très bon choix.

Je me demande si ça ne serait pas plus clair d'afficher un seul hint à la fois, et de laisser le hint lorsque le mot de passe est suffisamment fort (pas en erreur) et afficher les hints pour renforcer encore plus le mot de passe.

Je vais faire le patch pour paramétrer ça dans les OU dans un autre ticket, celui-ci est déjà assez gros.

#12 - 02 septembre 2022 11:02 - Benjamin Dauvergne

- Statut changé de Solution proposée à En cours

Corentin Séchet a écrit :

> Je me demande si ça ne serait pas plus clair d'afficher un seul hint à la fois, et de laisser le hint lorsque le mot de passe est suffisamment fort (pas en erreur) et afficher les hints pour renforcer encore plus le mot de passe.

Si on parle de la validation JS, oui un seul à la fois vu que ça se met à jour dynamiquement et qu'ils sortent ordonnée ça devrait donner un truc stable, et une fois que ça valide en JS, afficher tous les hints en orange.

> Je vais faire le patch pour paramétrer ça dans les OU dans un autre ticket, celui-ci est déjà assez gros.

Ok.

Ça m'a l'air tout bon.

#13 - 05 septembre 2022 16:48 - Corentin Séchet

- Fichier 0001-misc-add-password-strength-meter-in-NewPasswordInput.patch ajouté

- Fichier 0002-misc-generate-hints-from-zxcvbn-report-63831.patch ajouté

- Statut changé de En cours à Solution proposée

Les deuxième et troisième patchs modifiés :

- Si le champ est vide, on affiche rien
- Si le mot de passe n'est pas assez fort, on affiche une erreur avec un conseil
- Si le mot de passe n'a pas le score maximum mais est suffisamment fort, on affiche une notice avec un conseil
- Si le mot de passe a la force maximum, on n'affiche rien

#14 - 06 septembre 2022 10:03 - Corentin Séchet

- Statut changé de Solution proposée à En cours

Au final je revois le deuxième patch pour mieux préparer https://dev.entrouvert.org/issues/68745

#15 - 06 septembre 2022 12:13 - Benjamin Dauvergne

&--to-weak {

--too-weak ?

#16 - 07 septembre 2022 13:36 - Corentin Séchet

- Fichier 0001-misc-use-a-template-for-NewPasswordInput-63831.patch ajouté

- Fichier 0002-misc-add-password-strength-meter-in-NewPasswordInput.patch ajouté

- Fichier 0003-misc-generate-hints-from-zxcvbn-report-63831.patch ajouté

- Statut changé de En cours à Solution proposée

J'ai mieux séparé l'ancien et le nouveau système : j'ai ajouté un endpoint "password-strength" à l'API. Le test pour savoir si le mot de passe est suffisamment fort lorsqu'on le tape est fait en JS, ça simplifie le patch #68745. C'est mieux testé et j'ai remplacé --to-weak par --nok.

#17 - 07 septembre 2022 17:11 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

#18 - 12 septembre 2022 11:52 - Corentin Séchet

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

```
commit 4bb8877f3b03255113a9a488cab26037ef45f895
Author: Corentin Séchet <csechet@entrouvert.com>
Date:   Thu Sep 1 23:17:48 2022 +0200

    misc: generate hints from zxcvbn report (#63831)

commit 5de83a83d21b6c5c78afe309ad44720bc0bfc568
Author: Corentin Séchet <csechet@entrouvert.com>
Date:   Thu Sep 1 00:55:49 2022 +0200

    misc: add password strength meter in NewPasswordInput (#63831)

commit f372225e6d324310edeb17ff141647221b690b25
Author: Corentin Séchet <csechet@entrouvert.com>
Date:   Wed Aug 31 14:12:09 2022 +0200

    misc: use a template for NewPasswordInput (#63831)
```

#19 - 14 septembre 2022 17:14 - Transition automatique

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

#20 - 20 novembre 2022 04:42 - Transition automatique

Automatic expiration

Fichiers

0001-misc-add-password-strength-meter-63831.patch	11,7 ko	29 juin 2022	Corentin Séchet
authentic_screenshot.png	19,5 ko	29 juin 2022	Corentin Séchet
0001-misc-use-a-template-for-NewPasswordInput-63831.patch	6,68 ko	02 septembre 2022	Corentin Séchet
0002-misc-add-password-strength-meter-in-NewPasswordInput.patch	14,4 ko	02 septembre 2022	Corentin Séchet
0003-misc-generate-hints-from-zxcvbn-report-63831.patch	5,61 ko	02 septembre 2022	Corentin Séchet
0002-misc-generate-hints-from-zxcvbn-report-63831.patch	5,62 ko	05 septembre 2022	Corentin Séchet
0001-misc-add-password-strength-meter-in-NewPasswordInput.patch	14,9 ko	05 septembre 2022	Corentin Séchet
0001-misc-use-a-template-for-NewPasswordInput-63831.patch	6,68 ko	07 septembre 2022	Corentin Séchet
0002-misc-add-password-strength-meter-in-NewPasswordInput.patch	17,7 ko	07 septembre 2022	Corentin Séchet
0003-misc-generate-hints-from-zxcvbn-report-63831.patch	5,64 ko	07 septembre 2022	Corentin Séchet