Authentic 2 - Support #72768

doc : documenter les forces de mot de passe configurables dans l'OU

23 décembre 2022 12:10 - Paul Marillonnet

Statut:	Nouveau	**Début:**	23 décembre 2022
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Planning:**	Non

Description

Actuellement on a le choix entre "Valeur par défaut du système" dont on ignore de quoi il s'agit, il faudrait préciser quelle est la valeur actuellement posée ;
et entre tout un éventail allant "Très faible" à "Forte" dont on ignore ce que ça implique en termes de longueur de mot de passe, de nombre de classes de caractère différentes etc.

Historique

#1 - 23 décembre 2022 12:12 - Paul Marillonnet

Il y a un travail de documentation qui irait dans https://dev.entrouvert.org/projects/espace-des-cpf/wiki/%C3%89cran_de_param%C3%A9trage_d'une_OU mais aussi peut-être préciser directement ces valeurs dans l'écran de configuration ?

#2 - 23 décembre 2022 12:29 - Anaïs Ecuvillon → en congés, retour le 30/04

Paul Marillonnet a écrit :

> mais aussi peut-être préciser directement ces valeurs dans l'écran de configuration ?

ou, je suis pour, dans tous les cas, si on doit documenter, c'est que les choix de paramétrages ne sont pas suffisamment clairs pour nous (les CPFs), donc peut-être utiliser ce qui est documenté pour modifier des intitulés ou préciser les choix possibles. ça pourra alors faire l'objet de tickets dédiés.

#3 - 23 décembre 2022 16:08 - Corentin Séchet

Valeur par défaut du système : à l'instar de "Les utilisateurs peuvent réinitialiser le mot de passe :", c'est la valeur qui est configurée dans settings.py. On peut ouvrir un ticket pour afficher la valeur configurée, effectivement.

> ce que ça implique en termes de longueur de mot de passe, de nombre de classes de caractère différentes etc.

Ça ne fonctionne pas comme ça : P@ssWordp@ssWord est probablement plus faible que bJ89z. Et c'est difficile de donner des règles à suivre *à priori* : c'est une fois le mot de passe passé dans l'algorithme de détermination de force du mot de passe qu'on est capables de dire pourquoi il est faible ou non (trop court, répétitions de caractères, mots dans le dictionnaire...). Au mieux on pourrait donner des descriptions un peu plus précises, et une estimation du nombre de tentative pour trouver le mot de passe, comme celles indiquées dans la doc de zxcvnb (la librairie qu'on utilise) :

0 # too guessable: risky password. (guesses < 10^3)
1 # very guessable: protection from throttled online attacks. (guesses < 10^6)
2 # somewhat guessable: protection from unthrottled online attacks. (guesses < 10^8)
3 # safely unguessable: moderate protection from offline slow-hash scenario. (guesses < 10^10)
4 # very unguessable: strong protection from offline slow-hash scenario. (guesses >= 10^10)

Ce que je vais déjà indiquer de ce pas dans la documentation. J'ai indiqué "Moyenne" comme bon compromis entre sécurité et facilité d'utilisation : les avis sont bienvenus sur ce choix.