w.c.s. - Development #34601

CNIL, complexité du code de suivi

08 juillet 2019 11:38 - Benjamin Dauvergne

Statut:	Fermé	**Début:**	08 juillet 2019
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Planning:**	Non

Description

Actuellement 8 caractères parmi BCDFGHJKLMNPQRSTVWXZ (20 caractères), donc log(20^8)/log(2) = 34.. bits d'entropie.

Si on se réfère à la page[1] de la CNIL concernant les mots de passe, en considérant que le code de suivi est un mot de passe servant aussi d'identifiant, on devrait avoir 12 caractères avec majuscule, minuscule, chiffres et caractères spéciaux, mais comme ce ne sont pas les utilisateurs qui choisissent je pense qu'on peut enlever les caractères spéciaux en ayant une assez bonne entropie, si on ajoute du throttling avec temps d'attente exponentiel (on ne pourra se baser que sur l'IP, on a pas d'autre identifiant pour fixer le compteur de throttling) on peut descendre à 8, soit log((2*26+10)**8)/log(2) = 47 bits d'entropie.

À voir si on préfère allonger le code, ajouter de nouveaux caractères ou jouer sur la force du throttling, par exemple limiter à 10 échec consécutifs par heure et par /24 (et en IPv6 je ne sais pas trop, il me semble qu'on ne sert pas nos sites en IPv6 pour l'instant...).

[1] https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires

Demandes liées:

Lié à Publik - Project management #34599: Suivi du respect des contraintes CNIL	**Nouveau**	**08 juillet 2019**
Lié à Publik - Development #34459: possibilité de code de suivi plus long	**Nouveau**	**01 juillet 2019**
Lié à Publik - Development #58837: Sécurité du code de suivi/d'accès	**Fermé**	**01 mai 2022**

Historique

#1 - 08 juillet 2019 11:38 - Benjamin Dauvergne

- Lié à Project management #34599: Suivi du respect des contraintes CNIL ajouté

#2 - 08 juillet 2019 11:40 - Frédéric Péters

- Lié à Development #34459: possibilité de code de suivi plus long ajouté

#3 - 08 juillet 2019 12:52 - Benjamin Dauvergne

- Sujet changé de CNIL, longueur du code de suiv à CNIL, complexité du code de suivi

Je renomme en complexité du code de suivi puisqu'il y a déjà un ticket sur la longueur elle même.

#4 - 08 juillet 2019 13:40 - Benjamin Dauvergne

Thomas signale que la crainte de la CNIL concerne des attaques force-brute distribuées, dans ce cas une possibilité et d'ajouter une preuve de travail (PoW) pour limiter la possibilité de distribuer l'attaque, ou en tout cas rendre son coup prohibitif (chaque essaie par IP coûtant plus cher en calcul, voir impossible si les bots sont "idiots", i.e. n'utilisent pas un navigateur).

Prévoir un jeton CSRF aussi sur la vue pour interdire les attaques JS distribuées.

#5 - 08 juillet 2019 23:08 - Benjamin Dauvergne

J'ajoute encore d'autre possibilité toujours dans l'idée de bloquer des attaques brute force distribuées :

- bloquer les ips à partir d'une blocklist DNS (noeud de sortie Tor, IP connues pour spam/botnet, etc..)
- poser un cookie signé longue durée dès qu'une interaction réussie (création d'une demande, login, soumission correcte d'un code suivi), ce cookie désactive toutes les protections pour ce client

#6 - 09 juillet 2019 09:31 - Paul Marillonnet

Benjamin Dauvergne a écrit :

ajouter une preuve de travail (PoW)

Qu'est-ce que tu verrais "dans la vraie vie", i.e. une solution qui ne pénalise pas l'usager honnête du système ?

#7 - 09 juillet 2019 10:56 - Benjamin Dauvergne

En période d'attaque il faut pénaliser tout le monde, sauf ceux qu'on connaît déjà (d'où l'idée du cookie), dès qu'on fait un essaie raté on invalide le cookie, donc même un attaquant aurait récolté un ou des cookies à l'avance ne pourra faire qu'un essai par cookie avant de se faire bloquer.

#8 - 09 juillet 2019 11:21 - Paul Marillonnet

D'ac je comprends mieux, merci.

#10 - 22 novembre 2021 14:46 - Mikaël Ates

- Lié à Development #58837: Sécurité du code de suivi/d'accès ajouté

#13 - 13 juin 2022 14:25 - Thomas Noël

- Statut changé de Nouveau à Fermé

Avantageusement remplacé par #59027