

Rapport d’audit

Cyber Sécurité



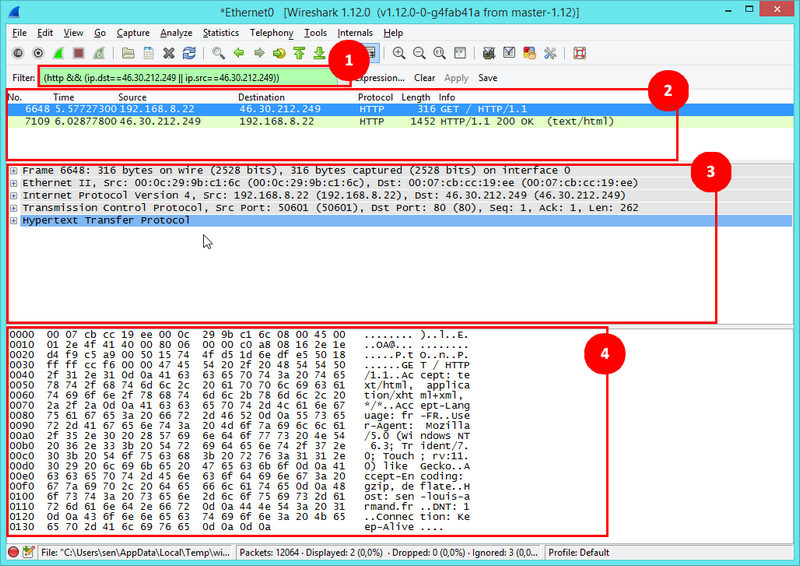
29 février 2024

Martins da cruz

Benjamin

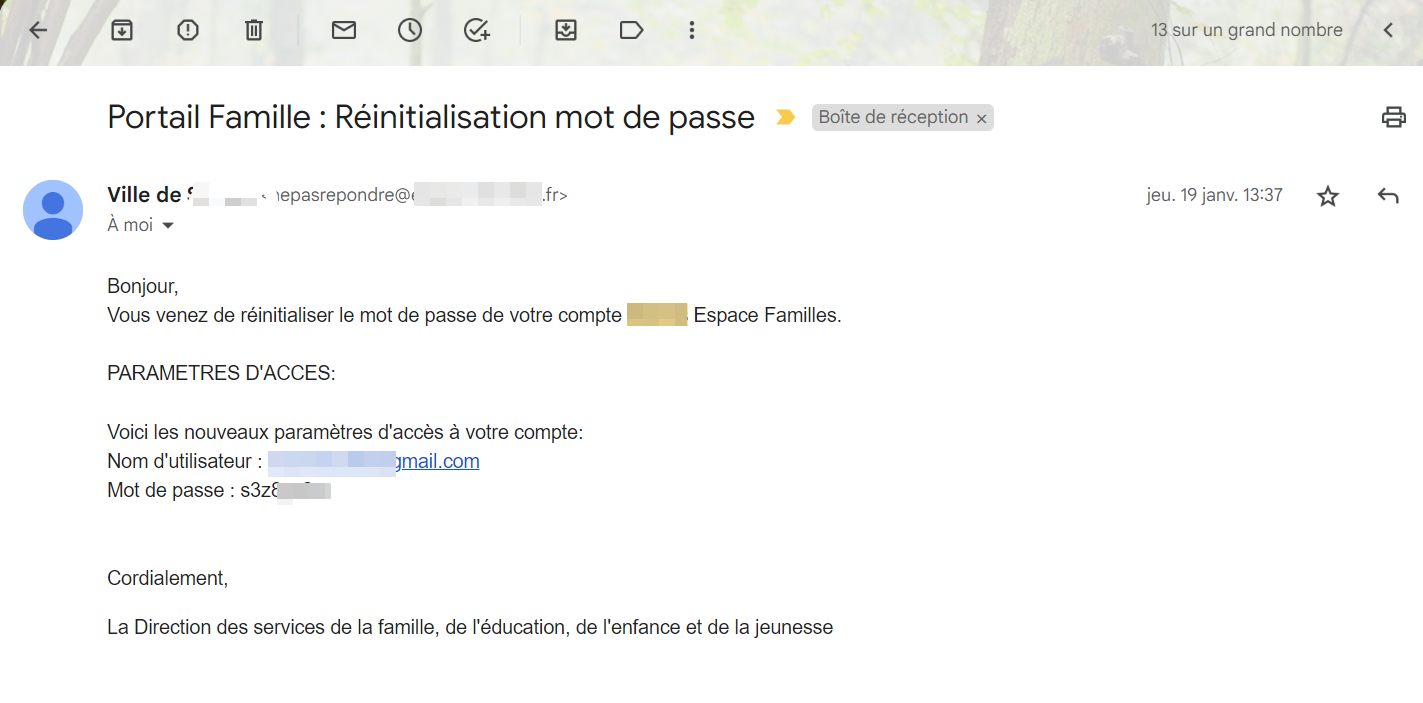
Audit de sécurité de la base de données et du site

I



On constate sur cette capture de packets entrants/sortants, une communication entre l’appareil et le site internet louis-armand.fr via le navigateur Mozilla Firefox.

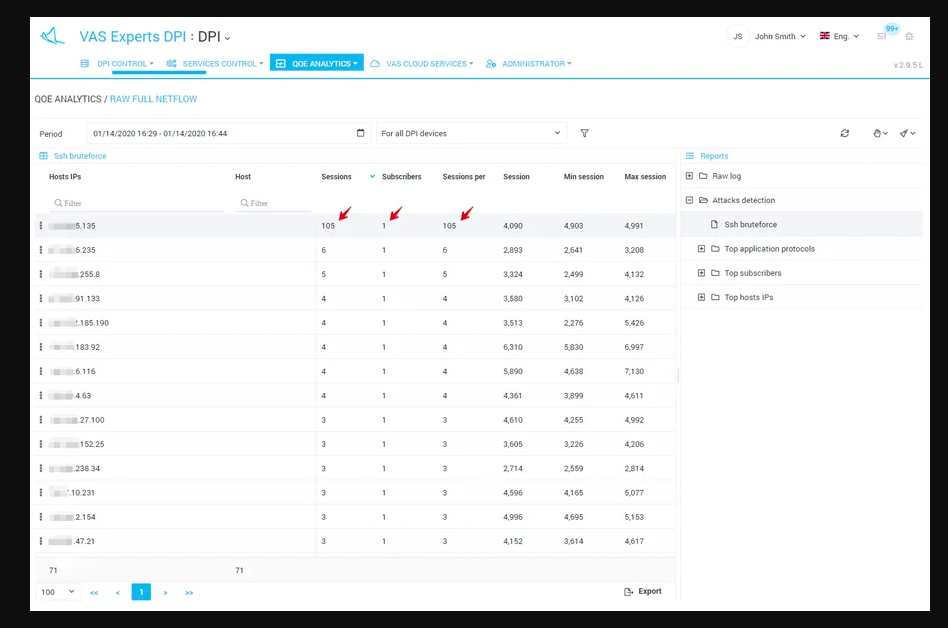
II



Sur cette capture d’écran du mail de réinitialisation de mot de passe, on constate que des données confidentielles sont transmises en clair.

Il est fortement déconseillé de transmettre quelconques identifiants de connexion par mail lors d’une réinitialisation de mot de passe, au lieu de cela, nous conseillons un lien de redirection permettant à la création d’un nouveau mot de passe.

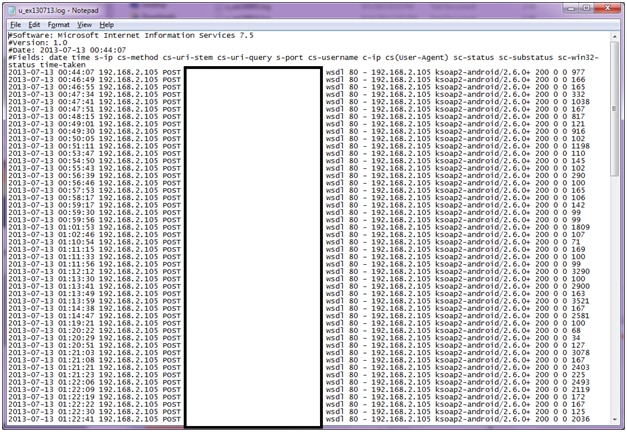
III



Cette capture montre une quantité élevée de tentative de connexions

À des fins de sécurité pour les comptes des utilisateurs du site internet, il est recommandé de mettre en place une limite de tentatives de connexion dans le temps par adresse IP.

IV

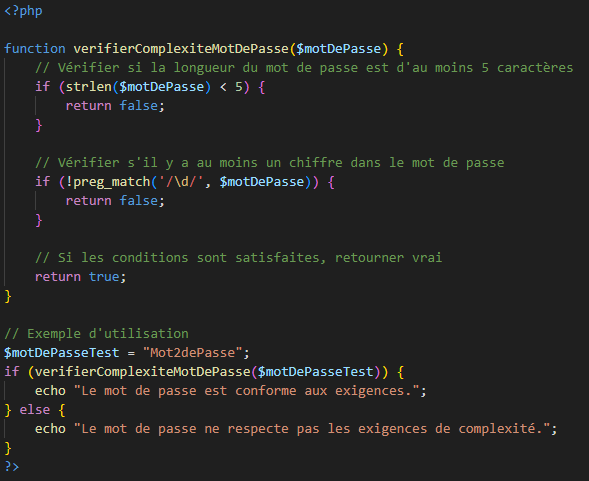


Ce fichier de logs montre un grand nombre d’appels serveur effectués pendant la nuit par un même appareil Android.

Il serait recommandé, selon le type d’appels serveur, de bloquer à l’avenir ce genre de situation.

Si un compte utilisateur semble compromit, le bloquer, temporairement, pourrait donner le temps au propriétaire du compte de le récupérer sans causer d’avantages de problèmes.

V



Ceci est le code de vérification de la complexité d’un mot de passe lors de sa création.

Les exigences de complexité sont trop faibles pour assurer la sécurité des comptes utilisateurs.

Il est recommandé pour un mot de passe de remplir les conditions suivantes :

* Au moins une majuscule
* Au moins un caractère numérique
* Au moins un caractère spécial
* Un total de minimum 8 ou 12 caractères.

Gestion de la sécurité des mots de passe : étude des possibilités

1. /Déterminez l'algorithme de hachage cryptographique utilisé.
2. /Déterminez la version en clair des mots de passe, à partir d'outils disponibles en ligne par exemple.
3. /Produisez l'empreinte hachée du mot de passe "Vive#Les#S1aux" en MD5 avec la chaîne de salage "duSel".
4. //Le hashage obtenu est : D5ssjBQDmeACB1mA1KUJGg==
5. /Produisez l'empreinte hachée du mot de passe "Vive#Les#S1aux" en SHA256 avec la chaîne de salage "duSel".

//Le hashage obtenu est : AA/PgtZN7OzoLcQZ2ixv/0JVib8nchmDlRywcGMfN+g=

1. /Produisez l'empreinte hachée du mot de passe "Vive#Les#S1aux" en SHA512 avec la chaîne de salage "duSel".
2. //Le hashage obtenu est : Q8tDBIEyOi+1d97+yAfzQgtFM1UWf86WnIiOKpnSRcJ/1V87ncgIYXALy+Otuqe8sAzi4/CoQq232WcR4YWAZg==
3. /En utilisant la fonction **password\_hash()**, générez l'empreinte du mot de passe "Vive#Les#S1aux" avec l'algorithme Bcrypt. Observez le résultat lors d'exécutions successives de votre programme.

//L’empreinte obtenue est : $2y$10$9VOu1c3d05zjPZl/NXbHueDzZwn0BdqOoZTGn5TkbBhrj3thmP8x6

/En utilisant la fonction password\_hash(), générez l'empreinte du mot de passe "Vive#Les#S1aux" avec l'algorithme Bcrypt. Quel est le temps d'exécution ? Recherchez dans le résultat la valeur du "coût" algorithmique.

//L’empreinte obtenue est : $2y$10$GymrO2d7NUHBPH1TjO.Am.nna9SwhBt0ZPzlOSIsmpD98kEnYosva

Avec une durée d’exécution de : 0.053472995758057 secondes

Et pour coüt : 10

Temps pour coût = 5 : 0.0021698474884033 secondes

Temps pour coüt = 15 : 1.6904928684235 secondes