Correction TP - Hachage

SIO 1 – BLOC 3 – Cybersécurité – Thème 2 – Préserver l'identité numérique de l'organisation

1 Calcul d'empreintes avec Notepad++

1. Quelles différence constatez-vous entre MD5 et SHA-256 ?
   la longueur de l'empreinte MD5 : 128 bits ; SHA-256 : 256 bits.

2 Tentatives d'inversion dempreintes

Est-ce qu'on retrouve le mot d'origine *bonjour* ? OUI . . .

Est-ce que l'inversion de *hello* marche ? OUI . . . .

Est-ce que le site arrive à retrouver le mot de passe `m0t-2-p@ss3-l0ng-c0mpl1que` ? NON

Est-ce que l'inversion d'un mot de passe compliqué marche ? a priori non . . . .

Q.2.1 – Comme on l'a vu en cours, il est théoriquement impossible, à partir d'une empreinte, de retrouver les données d'origine. Comment peut-on expliquer le fait que le site gromweb arrive parfois à retrouver un mot à partir de son empreinte, et parfois pas ?

Le site comporte un dictionnaire de mots de passe avec des empreintes pré calculées. Il arrive donc à retrouver le mot de passe à partir d'une empreinte, dans le cas d'un mot de passe simple. Si le mdp est trop compliqué, il ne l'a pas dans son dictionnaire.

3 Calcul de l'empreinte d'un fichier

A-t-elle été modifiée par rapport à la première version du fichier ? OUI, dès qu'on modifie le fichier d'origine (ne serait-ce qu'un bit), l'empreinte change.

4 Vérification de l'intégrité d'un téléchargement

Si l'empreinte obtenue n'est pas égale à celle donnée par le site, c'est que le fichier téléchargé n'est pas identique à l'original. Il y a donc eu un problème lors du téléchargement ou le fichier téléchargé n'est pas celui d'origine : cela peut-être un fichier falsifié par un pirate.

5 Hachage de mots de passe avec Bcrypt

Explications pour le prof (pas nécessaire de tout dire aux élèves).
Avant de hacher le mot de passe, il faut préciser les paramètres suivants :
- le nombre de tours de l'algorithme (plus c'est élevé, plus le hachage sera lent ; cela sert à ralentir les attaques par force brute) ;
- le préfixe 2a ou 2b (pour indiquer les bibliothèques compatibles) ;
- un sel aléatoire (nombre aléatoire ajouté au mot de passe).

Le résultat obtenu comprend l'empreinte elle-même + tous ces paramètres (nb tours, préfixe, sel). C'est pour ça que lors de la vérification on n'a à saisir que le mot de passe, l'algorithme utilise le résultat pour trouver les paramètres et vérifier l'empreinte.

6 Deviner un mot de passe haché avec Bcrypt

Réponse : **Berlin2023**