Examen de Web sécurisé

Durée : 2h. Tout document est interdit. Barème indicatif : [9 pt]-[11 pt].
(le barème est susceptible de changer).

Toutes les réponses données doivent être justifiées. Il vous est conseillé de lire le sujet une fois en entier avant de commencer...

Exercice 1

1) [4 pt] Les attaques sur les applications web visent l'authentification, l'intégrité, la confidentialité des données, la non-répudiation. Pour chacun de ces objectifs cryptographiques,

- expliquez en une phrase ce qu'il signifie ;
- donnez un exemple concret d'attaque si la protection cryptographique n'est pas mise en oeuvre,

2) [1 pt] Quels liens existent entre ces quatre objectifs ? Qu'est-ce que le niveau de sécurité d'un système cryptographique ?

3) [2 pt] Un site web affiche un cadenas vert avec les détails suivants :

```
Détails techniques :
connexion chiffrée (clés TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, 128 bits, TLS1.2)
```

Détaillez ce que signifie chaque terme, donnez les caractéristiques de chaque algorithme. Quel est le niveau de sécurité de cette connexion ? Est-ce suffisant ?

4) [2 pt] Expliquez la différence entre les systèmes de chiffrement symétriques et asymétriques, donnez les avantages et inconvénients de chacun.

Exercice 2 Une entreprise de vente de parfums souhaite fournir à ses clients la possibilité de tracer en ligne l'origine et le déplacement géographique de ses produits. Elle vous demande de créer un site web où chaque client pourra se créer un compte.

1) [1.5 pt] Un stagiaire vous explique qu'il est interdit de stocker en clair le mot de passe des clients, et vous propose d'utiliser la fonction php `hash` avec comme paramètre `"md5"` ou `"sha256"` pour stocker les mots de passe. Qu'est-ce qu'une fonction de hachage ? Entre les deux fonctions `md5` et `sha256`, laquelle choisissez-vous et pourquoi ?

2) [2 pt] En cherchant la documentation de la fonction `hash`, vous tombez en fait sur la fonction

```
string password_hash ( string $password , integer $algo [, array $options ] )
```

Les options supportées sont :

- un sel aléatoire (par défaut, il est généré pour chaque mot de passe haché),
- un coût algorithmique (10 par défaut).

Expliquez à quoi servent chacune des deux options, en détaillant les attaques possibles et la protection apportée.

3) [2.5 pt] Pour gérer une session client sur l'application web, vous utilisez le système de cookies. Citez deux attributs particuliers que vous pouvez donner à vos cookies et expliquez qui ils protègent et de quelle(s) attaque(s) ils protègent.

4) [1 pt] Le stagiaire vous propose de mettre un script javascript dans le formulaire de création de compte forçant le client à mettre un mot de passe de plus de 8 caractères avec au moins un caractère spécial. Est-ce une bonne idée ? quels sont les risques ? Qui est protégé par cette mesure ?

5) [2 pt] Le stagiaire vous propose le script suivant pour afficher la liste des lieux de passage d'un parfum donné par son code `id` :

```
<?php
... /* Le formulaire */ ...
$id = $_POST['id'];
$requete = mysqli_query($link, "SELECT lieu, date FROM localisation WHERE id=$id");
while ($row = mysqli_fetch_row($requete) {
// on récupère les lieu et date et on affiche à l'utilisateur
}
..
```

Expliquez quelle(s) attaque(s) peuvent être mise(s) en oeuvre, quelles peuvent être les conséquences, et comment se protéger (on ne demande pas de code php).

Chaque parfum est fabriqué dans une usine, transporté par un transporteur, mis en vente dans un magasin, et l'entreprise veut avoir des garanties sur tous les lieux de passage et tous les sous-traitants ayant eu en main le parfum. Elle munit donc chaque produit d'un marqueur RFID (Radio-étiquette) contenant un code individuel static, et vous demande de créer une application sur smart-phone qui sera donnée à chaque sous-traitant. Dès qu'un sous-traitant B reçoit le produit d'un sous-traitant A, les deux scannent le code individuel du produit, et l'envoient au serveur web avec le lieu et la date (d'arrivée ou de départ).

6) [2 pt] Un sous-traitant malhonnête essaye de faire croire après coup qu'un produit n'est pas passé par lui. Quelle protection cryptographique pouvez-vous proposer pour garantir que cela ne puisse pas arriver ? Que faudra-t-il mettre en oeuvre pour cela ?