Ecole des Mines de l'Industrie et de la Géologie

EVALUATION (DUREE 2H)

Partie I : Questions de compréhension (6 points)

1. Définissez la sécurité web. Citez deux objectifs principaux. (2 pts)

.....

.....

.....

.....

.....

.....

.....

2. Expliquez ce que signifie « OWASP Top 10 ». Pourquoi est-ce important ? (1 pts)

.....

.....

.....

.....

.....

.....

3. Donnez deux exemples d'outils utilisés pour tester la sécurité des applications web. (0.5 pts)

.....

.....

4. Citez quatre bonnes pratiques de sécurité à appliquer dans le développement web. (2 pts)

.....

.....

.....

5. Quelle est la différence entre une norme et une reglementation ? Donnez un exemple de chaque. (0.5 pts)

.....

.....

.....

.....

Partie II : **QCM (10 points)**

1. **Parmi les éléments suivants, lesquels relèvent d'une attaque côté client ?** (1 pts)
   - ☐ Brute Force
   - ☑ Cross-Site Scripting
   - ☐ Injection SQL
2. **Le protocole HTTPS permet :** (1 pts)
   - ☑ De chiffrer les échanges entre client et serveur
   - ☐ D'empêcher toutes les attaques XSS
   - ☑ De garantir l'intégrité des données transmises
3. **Vrai ou Faux :** (1 pts)
   a) Les mots de passe doivent être stockés en clair dans la base de données. => **Faux**
   b) Une session doit être invalidée à la déconnexion de l'utilisateur. => **Vrai**
4. **Cochez les bonnes affirmations :** (1 pts)
   - ☑ Un test d'intrusion peut être réalisé par un auditeur externe
   - ☑ Un scanner de vulnérabilités recherche automatiquement des failles
   - ☐ Les tests de sécurité sont uniquement effectués après la mise en production
5. **Vrai ou Faux :** (1 pts)
   a) Un outil comme OWASP ZAP permet de faire des scans actifs d'une application web . => **Vrai**
   b) Les tests de sécurité ne concernent que les développeurs backend. => **Faux**

6. **Vrai ou faux :** (1 pts)

   a) Le standard **OWASP Top 10** est une réglementation légale européenne. => **Faux**
   b) PCI-DSS est obligatoire pour les systèmes qui traitent des paiements par carte bancaire. => **Vrai**

7. **Cochez les bonnes réponses :** (1 pts)

- [x] Les mots de passe doivent être hachés avec un algorithme adapté comme bcrypt
- [ ] Il est préférable d'informer l'utilisateur si son identifiant est incorrect même si son mot de passe est juste
- [x] Les paramètres utilisateurs doivent toujours être validés côté serveur
- [ ] HTTPS protège automatiquement contre toutes les attaques web

8. **Vrai ou faux :** (1 pts)

   a) Il est conseillé d'utiliser des requêtes préparées pour se protéger contre les injections SQL. => **Vrai**
   b) Une API REST sécurisée ne nécessite pas d'authentification si elle est sur un réseau privé. => **Faux**

9. **Cochez les affirmations vraies** (1 pts)

- [ ] Une injection SQL est inoffensive si l'application est en lecture seule
- [x] Une faille XSS permet l'exécution de scripts dans le navigateur de la victime
- [ ] Un CSRF peut être évité uniquement en utilisant HTTPS
- [x] Un cookie sans l'attribut `HttpOnly` peut être volé via du JavaScript

10. **Cochez les affirmations vraies :** (1 pts)

- [x] Le RGPD s'applique aux entreprises hors UE si elles traitent des données de citoyens européens
- [ ] Une adresse IP n'est pas considérée comme une donnée personnelle
- [x] La norme ISO/IEC 27001 concerne la sécurité des systèmes d'information
- [ ] Le RGPD impose de chiffrer toutes les bases de données

Partie III – Analyse d'un code vulnérable (4 points)

On vous donne le code PHP suivant pour traiter une page de connexion utilisateur :

```
<?php
        $conn = mysqli_connect("localhost", "root", "", "app");
        $user = $_POST['username'];
        $pass = $_POST['password'];
        $query = "SELECT * FROM users WHERE username = '$user' AND password = '$pass'";
        $result = mysqli_query($conn, $query);

?>
```

a) Identifiez la vulnérabilité présente dans ce code. Donnez un exemple d'exploitation. ***(2 pts)***

.....

.....

.....

.....

.....

.....

.....

.....

b) Proposez une solution pour corriger cette faille. ***(2 pts)***

.....

.....

.....

.....

.....

.....

.....

.....

.....