

## **Sécurité des Applications Web**

**Examen du 24 mai 2017**

**(Durée: 1h30)**

### **Questions**

1. Qu'est-ce qu'un périmètre de sécurité ? **(1 point)**
2. Qu'est ce que la protection par l'obscurité ? **(1point)** Donnez un exemple. **(0.5 point)**
3. Citez trois mesures de sécurité à appliquer au quotidien dans la gestion d'une application web. **(1.5 points)**
4. Pourquoi un utilisateur a parfois besoin d'exécuter un processus sous l'identité d'un autre utilisateur ? **(1 point)**
5. Qu'est-ce qu'une attaque XSS (Cross Site Scripting) ? **(1 point)**
6. Citez deux techniques permettant de se prémunir des injections SQL. **(1 point)**
7. Citez deux manières de limiter la taille des fichiers téléchargés (uploaded) par les utilisateurs de l'application web? **(1 point)**
8. Citez deux manières de transmettre une URL piégée à une victime. **(1 point)**
9. Quelles sont les mesures de sécurité à appliquer lors du (1) transfert d'un mot de passe du navigateur vers le serveur web, et du (2) stockage de ce mot de passe dans une base de données ? **(2 points)**
10. Pourquoi est-il important de vérifier et nettoyer les données envoyées par un utilisateur à une application web ? **(1 point)**
11. Est-il nécessaire de filtrer les **noms** des fichiers téléchargés (uploaded) par les utilisateurs pour ce prémunir des attaques XSS ? **(0.5 point)** Pourquoi ? **(1 point)**
12. Quels sont les quatre types de fichiers d'une base de données MySQL devant être protégés ? **(2 points)**
13. Citez deux avantages offerts par l'utilisation d'un tunnel SSH. **(2 points)**
14. Quels sont les avantages et les inconvénients de l'utilisation de la cryptographie symétrique et asymétrique, en terme de nombre de clés à gérer, de protocole d'échange de clés et de temps de (dé)chiffrement. **(1.5 points)**
15. Qu'est-ce qu'une politique de filtrage ouverte ? **(1 point)**

Bon courage