Université FERHAT ABBAS SETIF I
Faculté des sciences
Département d'informatique
1ère année Master GL, IDTW

Sécurité des Applications Web

Epreuve de rattrapage du 14 juin 2017

(Durée: 1h30)

Questions

1. Donnez la définition d'une **vulnérabilité**, une **menace**, un **risque**, une **contre mesure** ? **(2 points)**
2. Pourquoi la désactivation de JavaScript sur le navigateur d'un utilisateur ne lui permet pas de se prémunir contre certaines attaques XSS ? **(2 points)**
3. Citez deux règles à respecter pendant la conception d'une application web pour en assurer la sécurité. **(2 points)**
4. Comment peut-on contourner les mécanismes de sécurité implémentés en JavaScript au niveau de la page web? **(1.5 points)**
5. Comment peut-on usurper l'identité de l'utilisateur d'une application web ? **(1.5 points)**
6. Citez deux exemples de données devant être filtrées par une expression régulière. **(1 point)**
7. Qu'est-ce que le filtrage de données par liste blanche ? **(1 point)**
8. Citez deux fonctions permettant d'injecter du code PHP dans un script. **(2 points)**
9. L'utilisation de la fonction *mysqli_real_escape_string($connection, $string)* permet d'échapper les chaînes de caractères fournies par l'utilisateur pour se prémunir des injections SQL. Comment éviter les injections SQL quand la donnée devant être fournie par l'utilisateur est un nombre ? **(1 point)**
10. Citez deux fonctions de hachage standards et deux algorithmes cryptographiques symétriques standards. **(2 points)**
11. Quel est l'intérêt de signer l'empreinte d'un message plutôt que le message lui même ? **(1 point)**
12. La signature numérique d'un message permet-elle d'en garantir la confidentialité ? l'intégrité ? **(1 point)**
13. Pour sécuriser les communications entre un site web grand public et le navigateur des utilisateurs est-il préférable d'opter pour une solution SSL/TLS ou SSH ? Pourquoi ? **(2 points)**

Bon courage