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

Sécurité des Applications Web

Examen du 26 mai 2018

(Durée: 1h30)

L'utilisation du stylo rouge est interdite

Questions

1. Définissez de manière claire et concise une **vulnérabilité**, un **exploit**, une **contre mesure**, un **périmètre de sécurité**. **(2 pts)**
2. Citez quatre bonnes pratiques de sécurité à adopter pendant la conception d'une application web. **(2 pts)**
3. Citer deux vulnérabilités potentielles au niveau matériel, et deux vulnérabilités potentielles au niveau système d'exploitation, pour une application web classique. **(2 pts)**
4. Citez une manière de se prémunir du vol de session. **(0,5 pt)**
5. Expliquez de manière concise en quoi consiste une attaque **CSRF (Cross Site Request Forgery)**. **(1,5 pts)**
6. Citez trois méthodes de protection des cookies. **(1,5 pts)**
7. Les attaques par injection SQL représentent une menace pour **(0,5 pt)**
    a. La confidentialité des données
    b. L'intégrité des données
    c. Les deux
8. Citez deux manières de se prémunir des injections SQL. **(1 pt)**
9. Quelles sont les deux politiques de filtrages pouvant être utilisée par les pares feux (firewalls) ? Laquelle des deux est la plus contraignante ? **(1,5 pts)**
10. Qu'est-ce qu'une zone démilitarisée (DMZ) dans un réseau ? **(1pt)**
11. Expliquez en vous aidant d'un schéma le processus de signature et de vérification de signature d'un message envoyé d'un expéditeur A vers un destinataire B. **(2 pts)**
12. Quel est le principal défaut des algorithmes de chiffrement à clé publique (asymétriques) ? **(1 pt)**
13. Quel protocole est sensible aux attaques de type homme du milieu (man in the middle) ? **(1 pt)**
    a. Echange de clés Diffie-Hellman
    b. SSL/TLS
    c. Les deux
14. Citez deux avantages à l'utilisation d'un tunnel SSH. **(1 pt)**
15. Le protocole SSL/TLS permet de garantir **(0,5 pt)**
    a. La confidentialité des données échangées
    b. L'intégrité des données échangées
    c. Les deux
16. Pourquoi le protocole d'échange de clés Diffie-Hellman n'est pas adapté pour la génération d'une clé de chiffrement pour l'envoi d'un courrier électronique chiffré ? **(1 pt)**

Bon courage