Exercises corrigés

Essentiel du cours

- Critères de la sécurité informatique
- Sources de menaces
- Pourquoi l'internet est un facteur aggravant ?
- Architecture d'une application web
- Pourquoi les applications web sont vulnérables ?
- Pourquoi sécuriser les applications est la tâche la plus difficile ?
- Problèmes de la sécurité web
- Les 10 classes de vulnérabilités (principe)
- Comment sécuriser son parc applicatif ?

Exercice 1 : Les URLs utilisées dans le cadre d'une application Web sont du type :

http://www.domaine.dz/chemin/fichier.ext?param1=x&param2=y

Une telle URL est composée de plusieurs parties :
- ***http://*** : protocole utilisé
- ***www.domaine.dz***: adresse du serveur
- ***chemin*** : arborescence de répertoires sur le serveur Web
- ***fichier.ext*** : fichier lu ou exécuté (son extension *.ext* est très importante)
- ***param1*** et ***param2*** : paramètres d'exécution, interprétés soit au niveau des composants métiers, soit directement au niveau de la base de données.

Chacune de ces parties est susceptible d'être attaquée, donner un exemple d'attaque pour chaque partie de l'URL.

Corrigé

Les URLs utilisées dans le cadre d'une application Web sont du type :

http://www.domaine.dz/chemin/fichier.ext?param1=x&param2=y

Attaques de chaque partie de l'URL :

Protocole: *on peut par exemple essayer de remplacer le protocole https:// par http:// afin de désactiver une authentification par certificat client.*

Serveur: *on peut le remplacer par son adresse IP ou par les noms de domaines d'autres sites hébergés sur le même serveur, afin d'avoir accès à d'autres parties du site.*

Chemin: *on peut tenter de naviguer dans l'arborescence pour accéder à des parties du site non autorisées ou pour remonter dans l'arborescence par l'utilisation de « /../../», ou en utilisant des vulnérabilités particulières (le bug Unicode d'IIS, par exemple).*

Fichier : *son extension va déterminer de quel type d'exécutable il s'agit: CGI, scripts ASP, HTR ou autre code exécutable. Plusieurs types de fichiers ont connu des vulnérabilités attachées à leur mode d'exécution, et en particulier à leur interpréteur.*

Paramètres: *la manipulation des noms de paramètres et de leur contenu peut conduire à des effets dangereux. Exemples d'attaques sur les paramètres : attaques des entrées des utilisateurs, attaques par injection de code, SQL, …*

Exercice 2 : Répondre par vrai ou faux

1. Implémenter votre application web en utilisant des requêtes préparées est efficace pour les attaques par SQL injection.
2. La validation des formulaires côté client est aussi sécuritaire que la validation côté serveur ; la seule différence est qu'elle se fait sur la machine du client.

Corrigé

1. ***Réponse : VRAI**, les requêtes préparées sont envoyées en séparant code SQL et données.* ***(1.5 pts)***
2. ***Réponse : FAUX**, la validation côté serveur est plus sécuritaire.* ***(1.5 pts)***

Exercice 3 : Répondre à ces questions

1- Vous exécutez un scanner de vulnérabilités sur votre site web. L'outil que vous utilisez affiche qu'il n'a trouvé aucune vulnérabilité sur votre site. Pouvez-vous conclure que votre site est sécurisé?

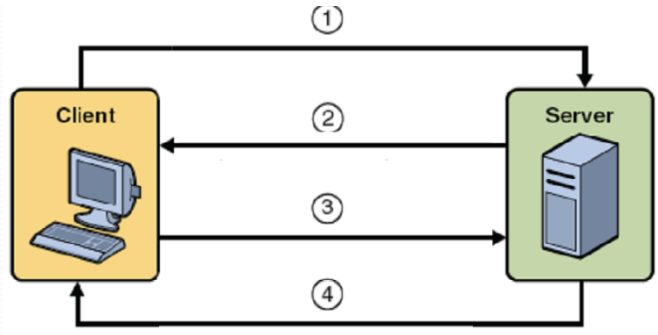
2- Concernant la sécurité web, pourquoi on suppose toujours que l'utilisateur peut visiter un site conçu par un attaquant?

Corrigé

1- ***Réponse :** Comme il y a plusieurs scanners de vulnérabilités dans le web, ils peuvent donner des résultats ambigüs. La seule manière de dire qu'un site est sécurisé est l'analyse détaillée du développeur de l'application web.* ***(1.5 pts)***

2- ***Réponse :** Parcequ'il est toujours possible qu'un attaquant conçoive un site très semblable au site de l'utilisateur et que ce dernier peut ne pas remarquer qu'il est en fait différent de son site usuel.* ***(1.5 pts)***

Exercice 4 : Le schéma suivant présente le scénario type du premier accès authentifié (*username:password*)



Q1- Décrire les étapes 1, 2, 3 et 4 du schéma.

Q2- Pourquoi les accès suivants ne demandent plus l'authentification.

Corrigé

R1- Description des étapes

1- *Demande d'une ressource protégée*
2- *Demande d'authentification (username:password)*
3- *Envoie (username:password)*
4- *Envoie de la ressource demandée*

R2- *Si l'authentification lors du premier accès est réussie une session est ouverte, les accès suivants appartiennent à la même session et ne demandent plus l'authentification.*

Préparé par Dr T. Mehenni