Attaques d'applications Web

1 Environnement de travail

Vous disposez d'une machine virtuelle (VirtualBox) sur laquelle est installée *Trisquel* (GNU/Linux basé sur Ubuntu). Tout les logiciels nécessaires (*WebScarab* et *Webgoat*) au TP sont déjà installés. *Webgoat* est une plateforme d'entraînement créée par l'OWASP (Open Web Application *Security Project*). Celle-ci permet d'apprendre à faire des attaques web en restant dans la légalité. NE REPRODUISEZ PAS SE QUE VOUS APPRENEZ ICI SUR DES SITE WEB NE VOUS APPARTENANT PAS. L'application est a utiliser à l'aide d'une interface web. Les attaques possibles sont les injections SQL, l'étude de faille XSS, la manipulation de paramètres HTTP, … Lorsque vous aurez réussi une attaque, l'interface affichera un message allant dans ce sens et une icône verte sera affichée en face du nom de l'attaque réalisée.

Pour lancer l'application, ouvrez un terminal est déplacé vous à laide de la commande **cd** dans le répertoire **/home/introsecu/webgoat** et exécuter la commande suivante :

java -jar WebGoat-6.0.1-war.exec.jar

Ensuite, il vous suffit d'ouvrir le navigateur internet et entrer dans l'url

localhost:8080/WebGoat/

et identifiez vous avec l'identifiant **guest** et le mot de passe **guest**.

Dans certains exercices, il vous faudra utiliser *WebScarab* pour intercepter les requêtes et les modifier. Pour lancer *WebScarab,* faites un clic droit sur le .jar présent dans **/home/introsecu/webscarab** et utiliser l'entrée nommée **java** du menu. Une fois *WebScarab* lancé, allez à l'onglet *Intercept* sélectionner *POST* et *GET* en maintenant le bouton *ctrl* du clavier et cocher la case *Intercept Request.*

2 But du TP

Le but de ce TP est de vous montrer des attaques simples contre des sites web vulnérables. Vous jouerez le rôle de **black hat**. Une fois connecté à l'interface *WebGoat* vous ferez les attaques présentes dans les sous-menus suivants :

- *Injection Flaws*
  - *numeric SQL Injection*

- *String SQL Injection*
- *stage1*

- *authentication flaws*
  - *password strenght*
  - *multilevel login 1*
- *Lab cross site scripting*
  - *stored xss attack*
- *Insecure communication*

Pour résoudre les attaques, vous pouvez vous aider des indices (*hints*). Les solutions de certaines attaques sont aussi disponible. Cependant, chercher d'abord par vous même avant de les utiliser pour bien comprendre les enjeux de la sécurité web (ainsi que pour le plaisir:)).

3 Exercice 1

Pour commencer, il faut d'abord que vous trouviez le mot de passe de la session. Pour ce faire, nous allons considérons que nous avons un accès physique à la machine (ceci n'est que très rarement le cas dans la réalité). Tout d'abord, démarrer la machine virtuelle sur un *live CD*. Un avantage des *live CD* Linux (notamment Ubuntu) est qu'il est possible d'installer des programmes sur la session *live*. Pour réaliser cet exercice, vous allez tout d'abord installer le programme **john** (*john the ripper*) présent dans les dépôts :

sudo apt-get install john

Il n'y a pas de mot de passe lorsque l'on demande les droits temporaires du super utilisateur. Le programme *john the ripper* vient avec le programme **unshadow**. Ce programme va nous permettre de réunir en seul fichier les fichiers **passwd** et **shadow** présents dans **/etc**. Le fichier *passwd* contient les informations sur les utilisateurs sous la forme :

UserName:Password:uuid:guid:commentaire:home:shell

Le fichier *shadow* contient les mots de passe codés des utilisateurs. Vous allez utiliser la commande **unshadow** pour concaténer les deux fichiers présents sur la partition *physique* (la machine virtuelle), les fichiers se trouvent dans (une fois la partition montée) **/media/nom_partition/etc** :
sudo unshadow /media/nom_partition/etc/passwd /media/nom_partition/etc/shadow > pass.db

Ensuite, il suffit d'utiliser la commande *john* sur le fichier *pass.db* :

john pass.db

Cette utilisation de la commande *john* permet de faire du brut force. Bien entendu, retrouver un mot de passe robuste par cette méthode prendrait beaucoup trop de temps (mois, années). *John the ripper* possède de nombreuses options à privilégier selon les cas. Ici, nous nous contenterons

d'utiliser le brut force. Pour voir les résultats trouvés, il faut exécuter la commande :

john -show pass.db

Question :

Que pouvez-vous conclure ?

4 Exercice 2 :

Réaliser les attaques mentionnées dans la section 2.

Question 1 :

Que concluez-vous sur la robustesse des mots de passe (qu'est-ce qu'un mot de passe robuste, que faut-il éviter, faut-il changer un mot de passe régulièrement ? Si oui, tout les combien de temps) ?

Question 2 :

Donner et expliquer comment les attaques réalisées fonctionnent ?