Exercice Sécurité – Attaquer une application web

Dans cet exercice, vous allez jouer le rôle d'un hacker qui essaie d'attaquer un site. On vous fournit le fichier `Exercice-81-yabe.tar.gz` qui contient une mauvaise implémentation[1] du logiciel Yabe correspondant à l'application décrite dans le tutoriel du Framework Play que vous allez utiliser dans votre projet. Déballez l'archive fournie, allez dans le sous-répertoire `yabe`, installez les modules nécessaires (`/opt/play/play deps`), et lancez le serveur avec la commande `/opt/play/play run`[2] (si nécessaire, changez au préalable le port 9000 en un autre port dans `conf/application.conf`).

Pour jouer le jeu correctement, faites comme si le code s'exécutait sur un site distant : ne regardez pas le code source, essayez de vous débrouiller juste avec votre client (navigateur) en observant les réponses du serveur à vos requêtes. (Pour réinitialiser l'état du serveur, il suffit de le relancer.)

Pour cet exercice, vous fournirez comme résultat les quatre textes/codes qu'on vous demande d'écrire dans la suite.

A - Modification du texte des commentaires (injection JavaScript)

L'auteur du site a cru bien faire en permettant d'inclure des tags HTML dans les commentaires des billets. Cela permet, p.ex. sur la page http://localhost:9000/posts/1 d'ajouter un commentaire ayant pour contenu

```
<strong>I agree.</strong>
```

ce qui se traduira par un troisième commentaire affiché en gras.

Néanmoins, ce mécanisme permet bien d'autres choses... En utilisant la balise `<script>`, ajoutez un commentaire en apparence anodin (« Yes, this seems to be right. ») mais qui en réalité modifie (à l'affichage) le texte du commentaire de Mike en « I am a drooling idiot. » Vous pouvez remarquer que le site inclut la bibliothèque JQuery dans chaque page...

→ *Résultat attendu* : le texte complet (avec toutes les balises) de votre commentaire

Indication :

Utilisation des méthodes jquery – find, empty, append, ...

B - Vol de session, vol d'identité (vol de cookie)

Vous constatez que le site suit votre session grâce à un cookie. Vous avez alors l'idée que vous pourriez vous faire passer pour l'un des auteurs du site (ou même un administrateur) en lui volant son cookie de session : p.ex. si vous connaissiez la valeur du cookie de Bob, vous pourriez envoyer son cookie à la place du vôtre, pour être reconnu en tant que lui.

1. Pour cela, vous créez dans un billet dont Bob est l'auteur, un commentaire anodin qui ajoute un script caché à la page : désormais, lorsque quelqu'un crée un nouveau commentaire, au moment de l'envoyer au serveur, votre script attache au message saisi un élément `<span>` invisible contenant le cookie de l'utilisateur. De cette manière, tous les commentaires après celui-ci trahiront l'identité numérique de l'auteur du commentaire.
2. Ensuite, sous une autre identité, vous créez un commentaire qui polémique avec le billet de Bob. (Puisque votre script précédent marche, ce commentaire contiendra donc un élément `<span style=...>votre-cookie-de-session</span>`.)
3. Sous encore une nouvelle identité, vous créez un troisième commentaire où vous demandez à Bob s'il est d'accord avec les critiques précédentes.

---

1 Mauvaise du point de vue de la sécurité.

2 Utilisez play 1.2.5 ou supérieur avec Java 6.

4. Vous n'avez plus qu'à attendre la réponse de Bob, pour visualiser son cookie et le lui voler.

→ Fournissez le texte/code du commentaire décrit au point 1. Décrivez la technique permettant de récupérer la session de Bob.

Indications :

Accès aux cookies en javascript : document.cookie

La version de JQUERY est plus ancienne que celle utilisée dans les TP précédents, regardez la gestion des évènements avec `live`

C - Injections SQL

Las d'attendre que Bob daigne répondre, vous vous attaquez à l'identification au site (http://localhost:9000/login). Surpris, vous constatez que les champs `username` et `password` du formulaire d'authentification sont probablement utilisés tels quels dans une requête SQL du genre

```
"select ... from ... where password='" + password + "' and username='" + username + "'"
```

1. Vous savez que le mél de Bob est `bob@gmail.com`. Quelle valeur devez-vous saisir dans le champ password pour être à coup sûr logué en tant que lui ?
2. Si vous ne connaissez pas le mél de Bob, pouvez-vous au moins imaginer une manière de remplir les champs `username` et `password` qui détruit la table `User` dans la base de données ? (indication : on peut enchaîner plusieurs commandes SQL avec `;`)
3. Avec la même technique que précédemment, ajouter un utilisateur de votre choix.

→ Fournissez les deux couples de textes login/password que vous avez trouvés.

Indications :

Penser aux conditions avec un OR