Objectifs

Ecrire et manipuler des Java Server Pages (JSP).

1 Exercice

L'avantage de Tomcat c'est qu'il accepte aussi bien des Servlets que des JSP. Les JSP se placent au même endroit que les pages HTML. Bien faire attention à la configuration des variables `JAVA_HOME`, et `CLASSPATH` pour que tout fonctionne parfaitement.

1. Une page html est aussi une jsp ! Ecrire une page `test.html` classique (`<h1>Hello world </h1>`) et renommez là en `test.jsp`. Testez l'accès à cette JSP.
2. Après avoir créé un objet `Compteur` avec deux méthodes `incr()` et `toString()`, écrire une JSP qui contient un compteur propre à chaque utilisateur (objet prédéfini `session`) et un compteur global à tous les utilisateurs (objet prédéfini `application`). La page devra afficher la valeur de ces deux compteurs à chaque utilisateur qui s'y connecte (*Vous avez chargé cette page 3 fois sur les 12 chargements au total*). Testez la avec votre voisin. [1]

3. Ecrire une page HTML de *login* qui permet à un utilisateur de s'identifier. Cette page lancera une JSP qui teste dans une base de données si c'est la première connexion de l'utilisateur. Si c'est le cas, la JSP rangera alors dans la table `login` le login de l'utilisateur avec sa date de connexion (objet `java.util.Date`) et l'adresse IP de la machine qu'il utilise (méthode `getRemoteAddr`). Quelques lignes lui souhaiteront la bienvenue. Dans le cas contraire, ces données seront mises à jour dans la table `login` pour cet utilisateur. La JSP affichera alors quelques lignes précisant la date de la dernière connexion de cette personne. Cet exercice nécessite bien sûr de créer une table `login(nom,mdp,dat,ip)`.
   Trois types de messages doivent donc pouvoir être affichés :
   `Bonjour Mr xxx, bienvenu sur ce site`
   `Bonjour Mr xxx, votre derniere connexion date de hh:mm:ss de la machine 0.0.0.0`
   Toute erreur sera automatiquement propagée dans une `errorPage` (donc pas de `try-catch` dans vos pages.

4. Ecrire une JSP simplifiée de gestion d'une boutique d'achats en ligne s'appuyant sur une table `produits(num,libelle,prix)`. Il n'y a qu'une seule page générée à l'aide d'une JSP. Cette page est coupée en deux parties : la première qui présente le panier du client (initialement vide) et la seconde qui présente les produits disponibles issus de la base dans des liens `href`. L'utilisateur doit pouvoir cliquer sur l'un des articles pour le rajouter à son panier personnel.

2 Déploiement et piratage

1. Tomcat arrêté, récupérer et décompresser le fichier `tp309.zip`
2. Quelle commande Unix permet de savoir dans quelles pages sont réalisées les connexions ? .....
   .....
3. Quelle commande Unix permet de remplacer le nom de l'utilisateur par le votre ? .....
   .....
4. Sans éditer aucun fichier, modifiez l'ensemble des pages de manière à bien régler le driver, l'url, le login, le mot de passe nécessaires au bon fonctionnement de ce site.
5. N'oubliez pas de créer la table et les données nécessaires (voir `README`) et compilez les servlets !
6. Testez l'injection XSS. En tant que jean, saisir dans le champs `adresse` la donnée suivante : `<script>location="http://ww`
   Reconnectez vous en tant que paul et testez les pages
7. Testez l'injection SQL. Saisir dans les deux champs login et mdp `' OR '1'='1`
   Vous constatez que l'on se connecte au site avec le login **du 1er utilisateur de la base**, qui est en général l'administrateur !!

1. Attention : si vous utilisez un objet, quand vous recharger la JSP, une erreur ClassCastException se produit. Cela vient du fait que l'ancienne instance de l'objet est toujours persistante. Il faut donc redémarrer le serveur.

8. Vous êtes un nouvel utilisateur. Comment faire pour être directement inscrit à la création avec un compte `admin` inscrit physiquement dans la base ? .....
.....

9. Corrigez ce site afin que plus aucune attaque XSS ou SQL ne soit possible. On utilisera pour cela la classe `StringEscapeutils` de la librairie Apache https://commons.apache.org/proper/commons-text/, ainsi que des `preparedStatement` avec des `setters`.