**TP 4 – Sécurité des applications J2EE**

# Première partie

## Installation d'une application J2EE

Dans ce TP nous allons installer une application J2EE très simple, dont l'archive est disponible à `https://amubox.univ-amu.fr/index.php/s/2CFbWK8Q5HWrZiP`. Décompressez l'archive, puis compilez le serveur avec la commande `./gradlew build`. Vous devriez avoir généré le fichier `build/libs/gs-securing-web-0.1.0.jar`.
Afin de pouvoir espionner le fonctionnement de notre serveur, nous allons lancer ce dernier dans la box vagrant utilisée lors du TP1. Pour ce faire, nous allons modifier le fichier Vagrantfile en ajoutant la ligne suivante en ligne 14 :

```
config.vm.network "forwarded_port", guest: 8080, host: 8081
```

Une fois le document sauvegardé, lancez la box avec la commande `vagrant up`.
Nous pouvons maintenant lancer notre application. Pour ce faire, copiez l'archive java générée au début du TP et transférez là dans la box via le dossier partagé entre votre session et la box. Une fois dans la box, démarrez l'application en utilisant `java -jar gs-securing-web-0.1.0.jar`.
Une fois que tout est bien démarré, vous pouvez vous connecter à l'application par un explorateur web à l'extérieur de la box en vous connectant à l'adresse `http://localhost:8081`.

**Exercice 1.** *Première connexion*

1. À coté de l'application, lancez dans la box l'outil WireShark. Quelles sont les informations que nous pouvons récupérer en rapport à notre application ?
2. En supposant que la page "hello world" représente une information sensible, quelles précautions sont nécessaires dans le développement de notre application ?

**Exercice 2.** *Connexion sécurisée*

Nous allons améliorer la sécurité de notre application en ajoutant une étape d'authentification. Pour se faire, télécharger l'archive `https://amubox.univ-amu.fr/index.php/s/S6wZCzjMp2OWLTA`, qui contient une version modifiée du code de notre application. Compilez là et lancez là sur votre box de la même façon que précédemment (n'oubliez pas de fermer la première application !).
Vous observerez que l'application demande maintenant un login et un mot de passe. Ceux-ci sont "user" et "password".

1. En utilisant WireShark, décrivez les faiblesses de sécurité de cette application, et expliquez comment les corriger.
2. Modifiez le code de l'application afin d'implémenter ces solutions.