

# CHAT SECURISE

## Membres du groupe :

- Baptiste MOMUT : [baptiste.momut.etu@univ-lille.fr](mailto:baptiste.momut.etu@univ-lille.fr)
- Louis JERONIMO : [louis.jeronimo.etu@univ-lille.fr](mailto:louis.jeronimo.etu@univ-lille.fr)

## Description du projet :

Notre chat sécurisé est un chat de groupe, c'est-à-dire que tout le monde communique dans le même groupe. Chaque personne voulant communiquer doit être authentifiée dans la base de données h2 associée.

## Compte rendu :

Les principales difficultés que nous avons rencontrées sont des problèmes avec le chiffrement et le déchiffrement RSA qui étaient finalement dus à une mauvaise utilisation des méthodes développées. De plus nous avons mis du temps à développer le mécanisme empêchant l'injection SQL et le XSS. Le dernier problème majeur auquel nous avons été confrontés était le mécanisme de hachage avec Salt pour les mots-de-passe. Le fait que ce mécanisme engendre l'utilisation du chiffrement base64 nous a posé quelques problèmes. Nous avons appris à bien utiliser les différentes méthodes de chiffrement et de déchiffrement (RSA, base64) et aussi à mieux connaître les technologies permettant d'éviter les injections SQL et le XSS. Nous avons aussi découvert la méthode de hachage avec Salt qui est un bon moyen de sécuriser les mots-de-passe. Ce qui nous a plu est le fait de voir comment il est possible de sécuriser les communications avec des technologies assez simples d'utilisation. Aucun point négatif n'est à sortir de ce projet.

## Etat d'avancement :

Nous aurions aimé avoir un auto-refresh de la page lorsqu'un message est reçu mais nous n'avons pas réussi à implémenter cette fonctionnalité. Outre cela, nous avons mené à bout chaque implémentation que nous souhaitions au démarrage du projet.

## Mode d'emploi :

À la racine du projet :

WINDOWS :

```
javac -cp .\lib\*; .\webapps\chat\WEB-INF\classes\*.java .\webapps\chat\WEB-INF\classes\pojos\*.java .\webapps\chat\WEB-INF\classes\util\*.java
```

LINUX

```
javac -encoding ISO-8859-1 -cp './lib/*:' ./webapps/chat/WEB-INF/classes/*.java  
./webapps/chat/WEB-INF/classes/pojos/*.java ./webapps/chat/WEB-INF/classes/util/*.java
```

Dans /lib : `java -jar h2-1.4.199.jar`

Dans la base jdbc:h2:~/chat -> utilisateur : « sa » mot de passe : « »

Create table users(LOGIN VARCHAR, SALT NVARCHAR(45),MDP NVARCHAR(45)) ;

Dans /bin : `chmod u+x catalina.sh`

`./catalina.sh run`

Dans un navigateur web : `localhost :8080/chat/login.html`