SECURITE DES APPLICATIONS WEB – TP N°01

OBJECTIF

- Comprendre le principe d'une injection SQL

APPLICATION A UTILISER

- Une application vulnerable est mise à votre disposition : https://vulnerable.cleverapps.io/login
- Vous connaissez l'adresse mail de l'administrateur mais pas son mot de passe
  - mail : gdupont@vulnerable.fr
  - mot de passe : **inconnu**
- Mais vous vous dites que peut-être que l'application est vulnérable aux injections SQL et que la connaissance du mot de passe est inutile
- Voici la requête effectuée par la DAO qui est à l'origine de la vulnérabilité :

```
String query = "SELECT * FROM users WHERE username = '" + username +
"' AND password = '" + password + "'";
```

TP

- **Pas de chat GPT, ni Google.**
- Trouvez un moyen d'injecter du SQL de manière à berner la DAO et vous connecter sans connaitre le mot de passe de l'admin, ou en proposant un mot de passe bidon qui sera ignoré.
- Réfléchissez à ce que vous pourriez faire sur la base de vos connaissances SQL.
- Si vous ne trouvez pas, vous pouvez utiliser votre joker auprès du formateur qui vous fournira un indice !