

# SLH 2024-2025

## Exercices 1

### 1. Application Java Vulnérable

Vous trouverez sur CyberLearn les fichiers `Chall.java` et `Chall.class`. Ce programme permet d'envoyer de l'argent sur un compte, mais le transfert est limité à 100'000 centimes.

1. Lisez le code source et trouvez une manière d'envoyer un montant plus élevé que la limite.
2. Quelle est le nom de la vulnérabilité ? sous quelle CWE peut-on la classer ?
3. Comment pouvez-vous corriger la vulnérabilité ?


### 2. Juice Shop

Juice Shop est une application web d'apprentissage de la sécurité, contenant un grand nombre de vulnérabilités. Suivez les instructions d'installation sur <https://owasp.org/www-project-juice-shop/>.

L'utilisation du **container docker** est recommandée:

```
$ docker pull bkimminich/juice-shop  
$ docker run -p 3000:3000 bkimminich/juice-shop
```

L'application sera alors accessible sous <http://localhost:3000/>. Le scoreboard caché est disponible sous <http://localhost:3000/#/score-board>.

1. Essayez le challenge "Login Admin"; vous pouvez suivre le tutorial intégré en cliquant sur le bouton  dans le scoreboard.
2. Nous allons utiliser sqlmap pour voler le contenu de la base de données du site. sqlmap est un outil qui peut automatiser l'exploitation d'une injection SQL même dans des scénarios difficiles (side-channel basée sur le temps, etc...)
  - a. Quelle est l'utilité des paramètres `--level` et `--risk` ?
  - b. Trouvez une URL GET avec un paramètre exploitable
  - c. Trouvez le nom de la table et de ses colonnes contenant l'email et le hash des utilisateurs
  - d. Récupérez le contenu de ces deux colonnes
  - e. Tentez de cracker ces hashes

- f. Quel est le nom de la vulnérabilité exploitée ici ? Quel type de requête SQL est utilisée pour accéder aux tables ?
  - g. Comment corrigeriez-vous la vulnérabilité ?
3. Faites le challenge "View Basket".
  - a. Quel est le nom de la vulnérabilité ?
  - b. Sous quel CWE la classe-t-on ?
4. Faites le challenge "Kill Chatbot".

**Indice:** le code source du bot est peut-être à disposition quelque part sur Internet.

**Indice 2:** Soyez attentifs à la manière dont le bot utilise le nom d'utilisateur que vous lui donnez au départ.
5. Le mécanisme de dépôt d'une réclamation permet d'uploader un fichier, mais le type et la taille maximum du fichier sont limités. Trouvez une manière de contourner ces deux restrictions.

**Indice:** Il existe différents outils pour manipuler facilement une requête HTTP: les outils de debugging du navigateur (touche F12), des outils comme Insomnium<sup>1</sup>, APIDash<sup>2</sup>, HTTPYac (CLI ou plugin VSCode), Thunder Client (plugin VSCode), ou Postman.
6. N'hésitez pas à essayer d'autres challenges.

## Référence sqlmap

- wizard : Interface débutants
- u <URL>: URL cible
- banner: Récupérer la version du DBMS
- dbs: Enumérer les bases
- tables [-D <DB>]: Enumérer les tables
- columns [-T <TABLE>]: Enumérer les colonnes
- dump [-T <TABLE>] [-C <COLUMNS>]: Récupérer le contenu d'une table
- dump-all: Tout récupérer (long)
- forms: Tester automatiquement les endpoints des formulaires
- crawl <n>: Suivre les liens de profondeur n depuis l'URL de départ
- tamper: Personnaliser le comportement pour esquiver la détection (voir la doc et les scripts inclus)
- list-tampers: Liste des tampers disponibles

---

<sup>1</sup><https://github.com/ArchGPT/insomnium>

<sup>2</sup><https://github.com/foss42/apidash>