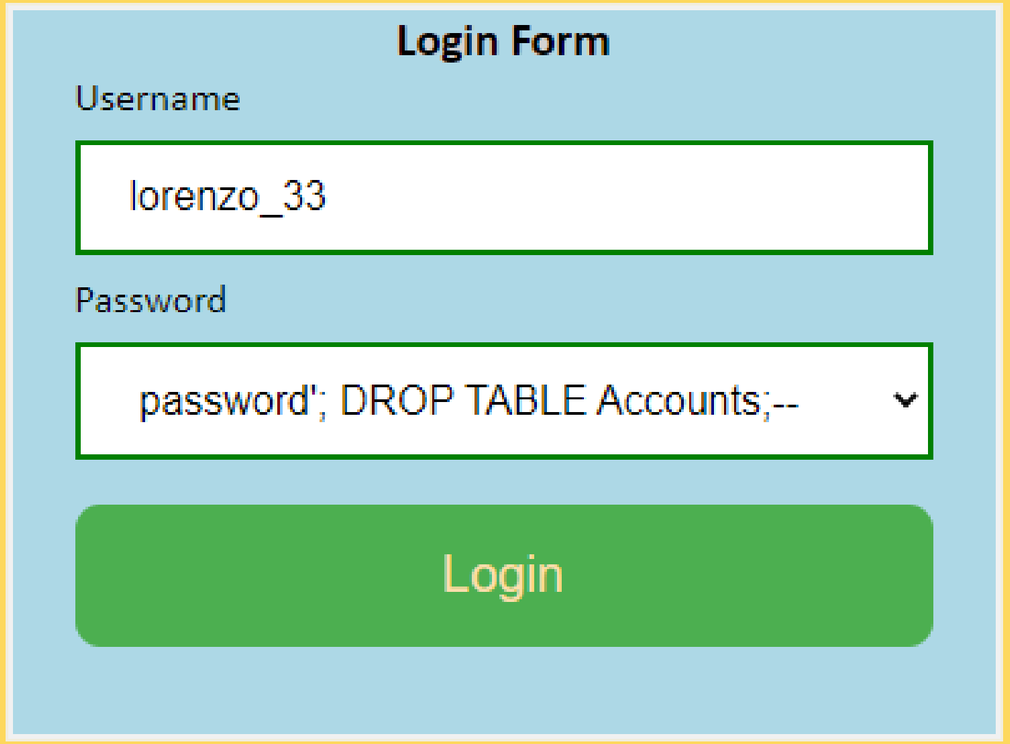
Détail implémentation



WebApp

Ce challenge cyber a pour objectif d'exploiter une injection SQL.
On a donc besoin d'une webapp (php/apache) qui satisfera les exigences suivantes :

- Une page de connexion défaillante (permettant une injection sql)
- Plusieurs pages de navigations
- Un formulaire non sécurisé permettant un upload de fichier dans une des pages

Base de données

Pour une injection SQL, on doit avoir une BDD. Ici ce sera une bdd MySQL classique qui contiendra des données prédéfinies.

Docker

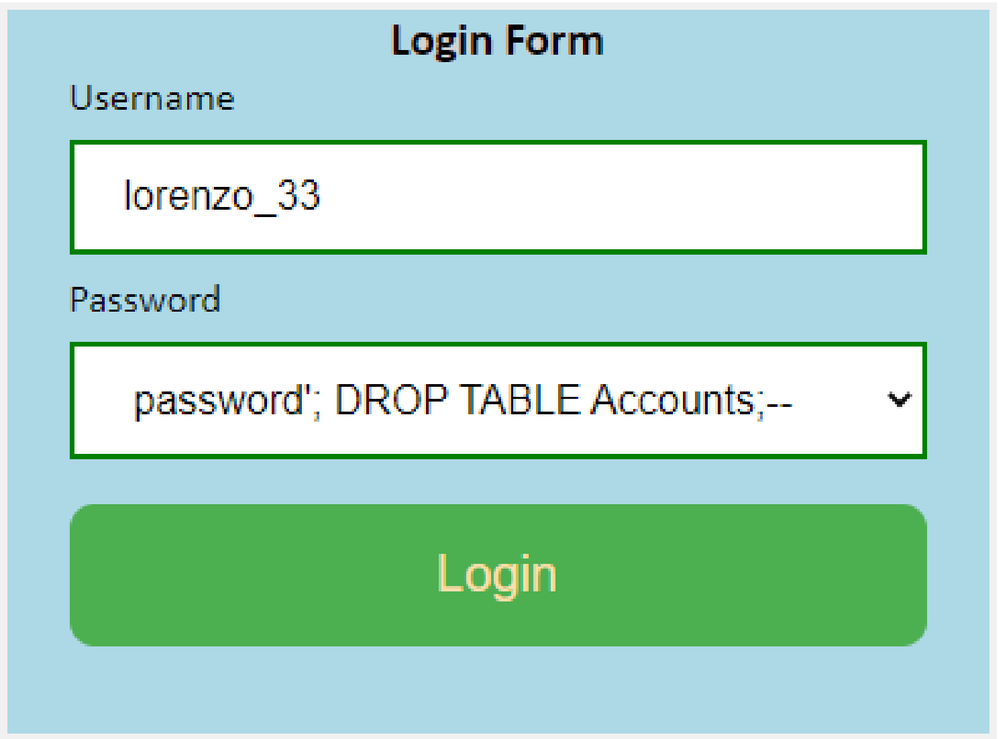
Les 2 services seront montés avec un docker compose

Prérequis

Il n’y a que 2 prérequis pour rendre ce challenge réalisable :

- La base de données est remplie avec les bonnes informations
- Le flag est placé dans le système (normalement à l’emplacement /home/data) et est accessible par tout le monde

Scénario



- Le challenger se rend sur la webapp et arrive sur la page de connexion
- Il effectue une injection SQL dans le champ vulnérable
- Il trouve dans la base de données les mots de passe d’accès à la webapp

- Il se connecte et arrive sur le site
- En naviguant sur le site il trouve un formulaire non sécurisé qui permet l’upload de fichier
- En utilisant cet upload de fichier il va pouvoir utiliser un web shell ou un path traversal
- Il trouve le flag “données_sensibles.txt” à l’emplacement “/home/data”