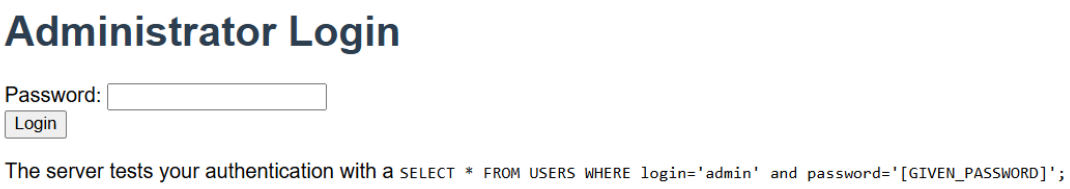
Web - SQLInjection - 75 points

Kévin DUVERGER

Table des matières

1 Résolution SQLInjection :

Tentons une nouvelle fois de nous connecter au serveur web (sur `http://146.59.227.136:23419`) :



Comme le dit le titre du challenge, le but est probablement de faire une injection SQL.

L'idée est ici que le champ n'est pas protégé et que l'on peut rentrer ce que l'on veut.
On pourrait donc rentrer la chaîne suivante dans le formulaire :

```
' OR 'hack3d'='hack3d
```

Ce qui transformerait la requête de la manière suivante :

```
SELECT * FROM USERS WHERE login='admin' and password='' OR 'hack3d'='hack3d'
```

Et fait en sorte que la requête soit toujours valide, ce qui nous permet de nous authentifier ! Notez d'ailleurs que vous auriez pu mettre n'importe quelle chaîne entre les guillemets (autre que `hack3d` ici).