Rapport :

[CVE-2023-23752](https://nvd.nist.gov/vuln/detail/CVE-2023-23752) décrit un contournement d'authentification qui permet à un attaquant de divulguer des informations privilégiées. Les exploits publics se concentrent sur la fuite des informations d'identification de la base de données MySQL de la victime - une perspective peu intéressante (nous pensions), car exposer la base de données à Internet est une mauvaise configuration dangereuse. L'accès à la base de données permet à l'attaquant de modifier le Joomla! Mot de passe du super utilisateur.

Recommandations:

Ouvrez votre invite de commande en mode administrateur

Faire : gem install httpx docopt paint et installer ruby

Entrez dans le dossier exploit-CVE-2023-23752-master et dans le sous dossier exploit-CVE-2023-23752-master

Faire : docker compose up -d

Une fois terminer allez sur le lein localhost:4242 ou <http://127.0.0.1:4242/installation/index.php>.

Et faites les configurations suivantes

Nom du site :  [CVE-2023-23752](https://nvd.nist.gov/vuln/detail/CVE-2023-23752)

Prénom superuser : John

Nom superuser : Doe

Mot de passe : root@12345 ou ce que vous voulez

Mail : [john.doe@secret.corp](mailto:john.doe@secret.corp)

DB type: mysqli

DB host: mysql

DB user: root

DB password: demo-ppZ5hnvK2ZEpR9yhRKA7

DB name: joomla\_db

DB prefix: krukc\_

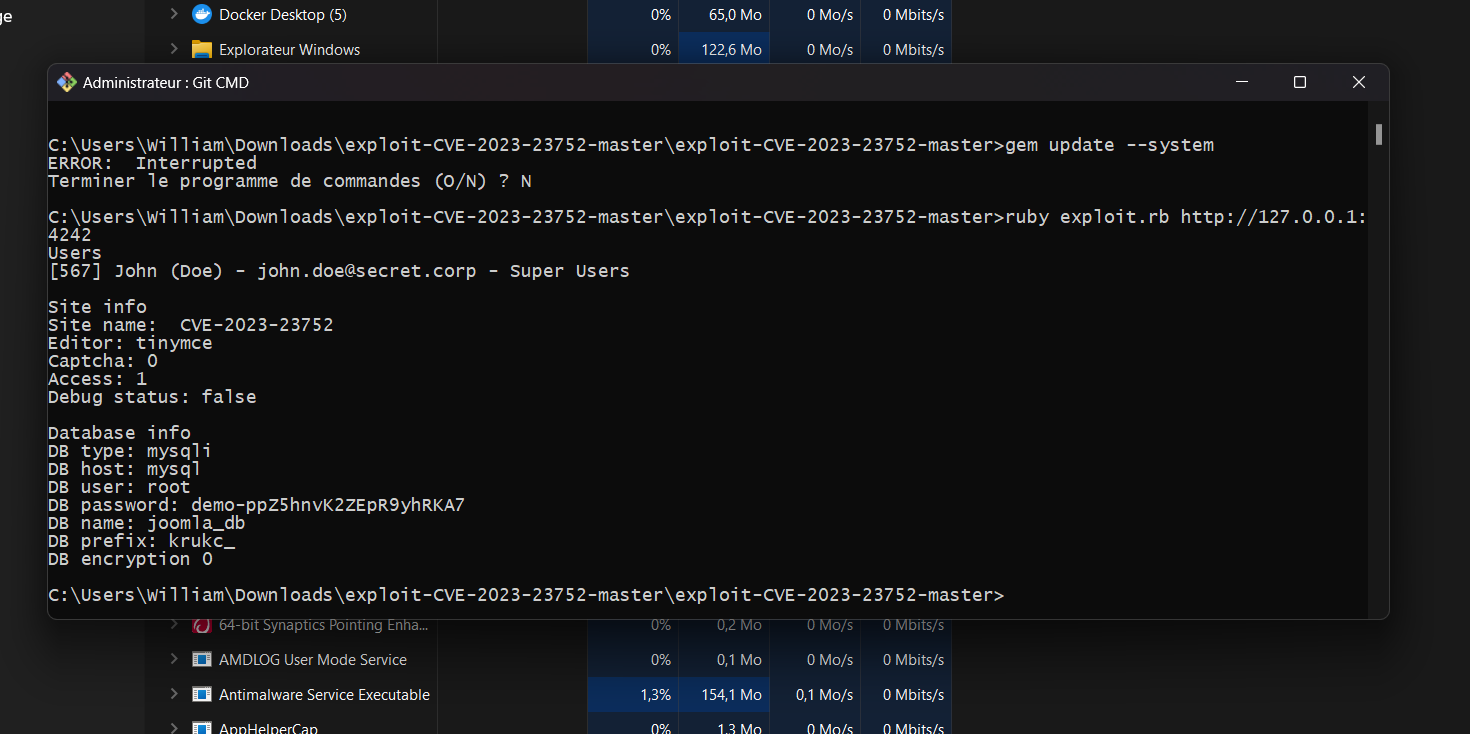
Validez les informations

Vous aurez la page suivante

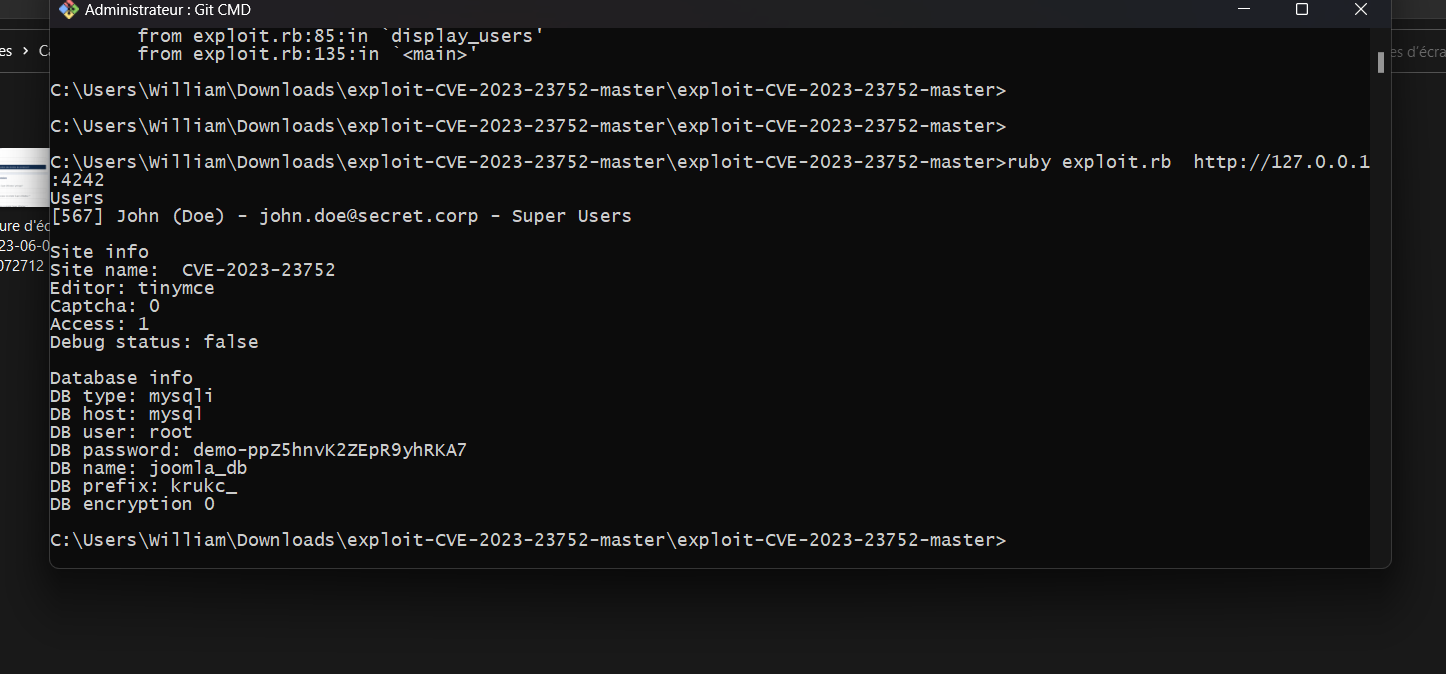
****

Entrez dans le dossier exploit-CVE-2023-23752-master et dans le sous dossier exploit-CVE-2023-23752-master et faites : ruby exploit.rb -h pour voir les options de exploit.rb

Vous devez avoir la page suivante



Ensuite tapez : ruby exploit.rb <http://127.0.0.1:4242>



Exploit.rb extrai les informations de la base de données.