**Bài 1: PHP Inclusion via phpinfo**

Đây là 1 bài ctf trong battle cookie giới thiệu thêm 1 kĩ thuật mới trong chuyên đề file inclusion.

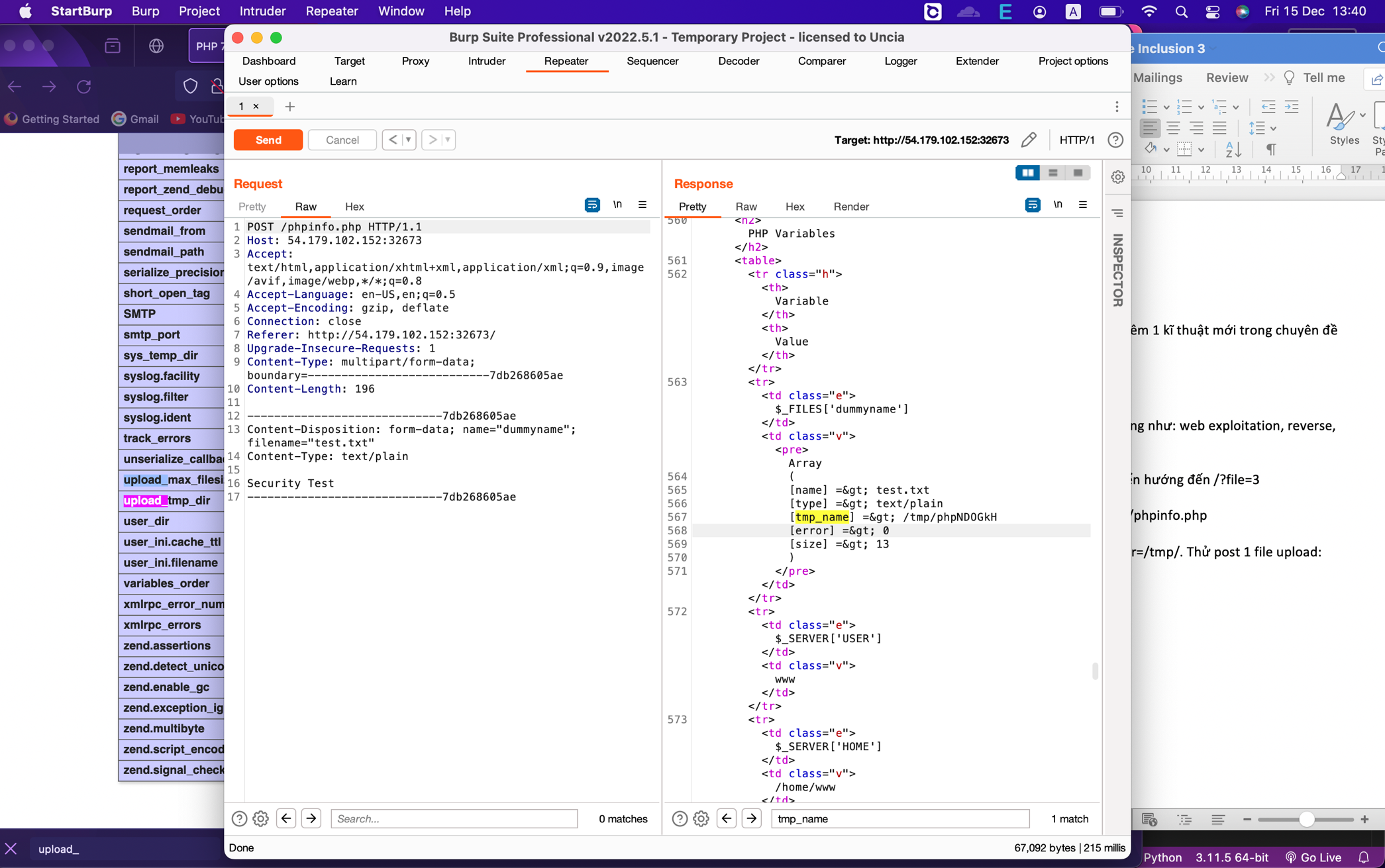
**Cách 1: LFI to RCE via phpinfo()**

Trang web giống như 1 diễn đàn CTF có các mảng như: web exploitation, reverse, pwn, forensics,..

Khi mình chọn web exploitation, trang sẽ chuyển hướng đến /?file=3

Tìm phpinfo() script 🡪 /?file=phpinfo.php hay /phpinfo.php

Bạn sẽ thấy file\_uploads=On và upload\_tmp\_dir=/tmp/. Thử post 1 file upload:



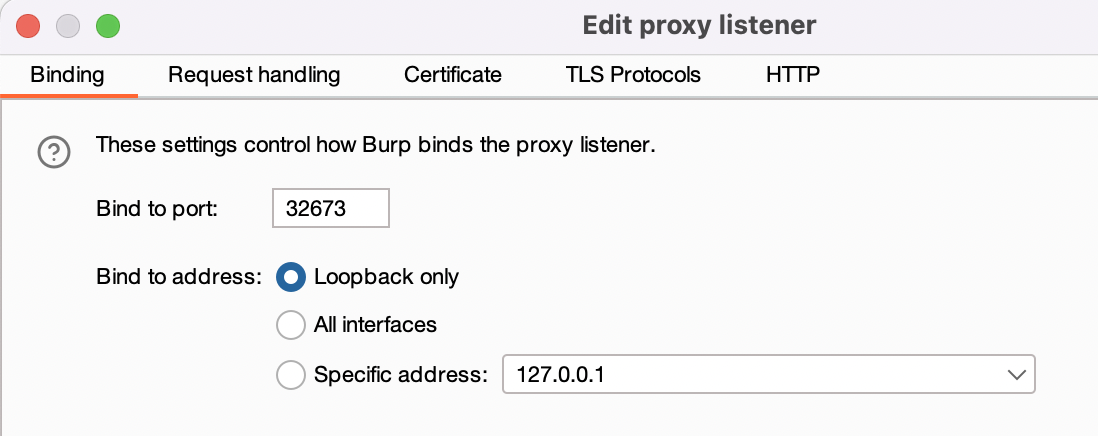
Tải phpInfoLFI.py về🡪 cấu hình

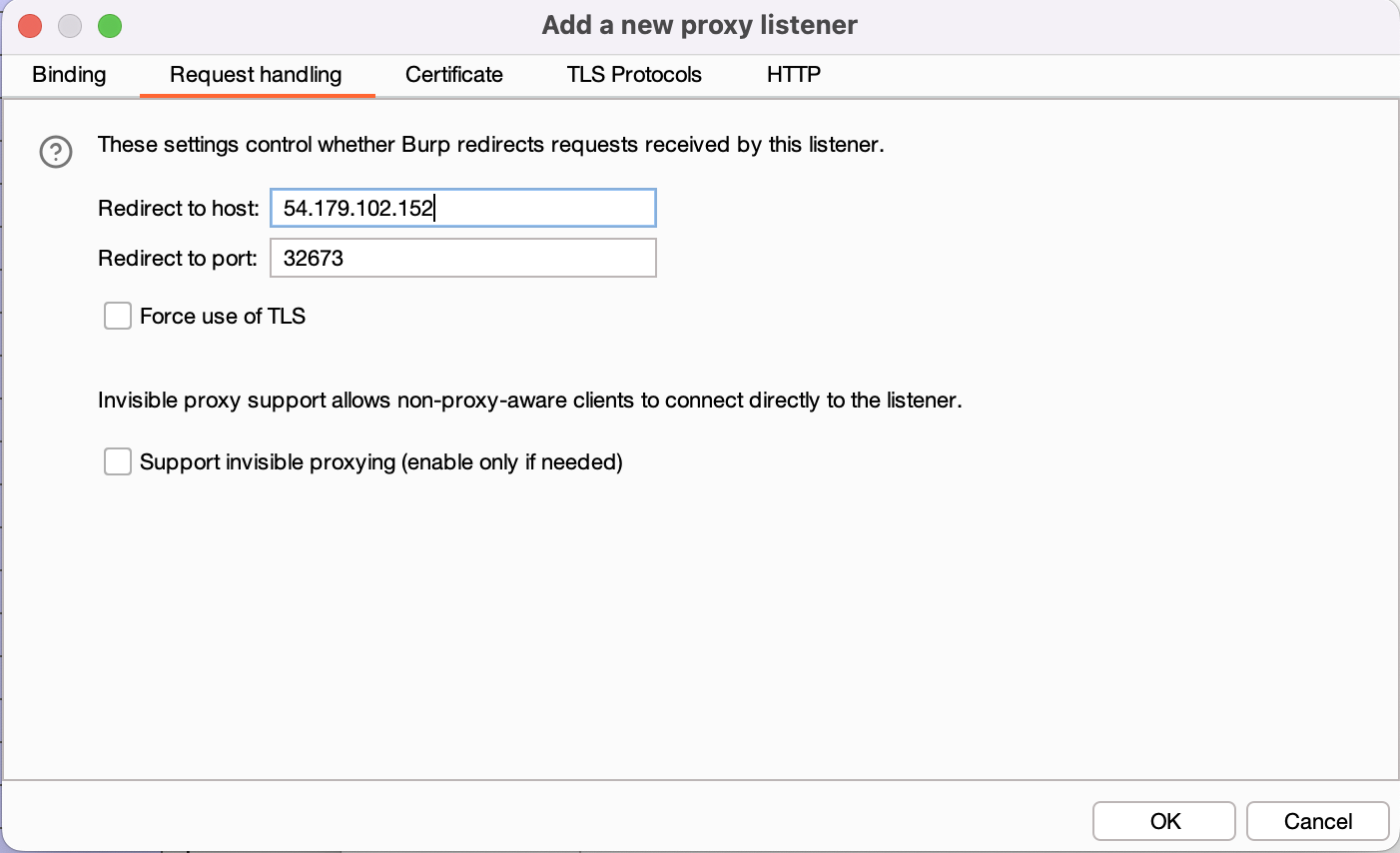
Nếu để padding=5000 bạn sẽ không tìm được tên của file tạm vì request header quá dài. Maximum ứng dụng cho phép là 4000.

Include 1 file .txt vẫn thực thi được mã.

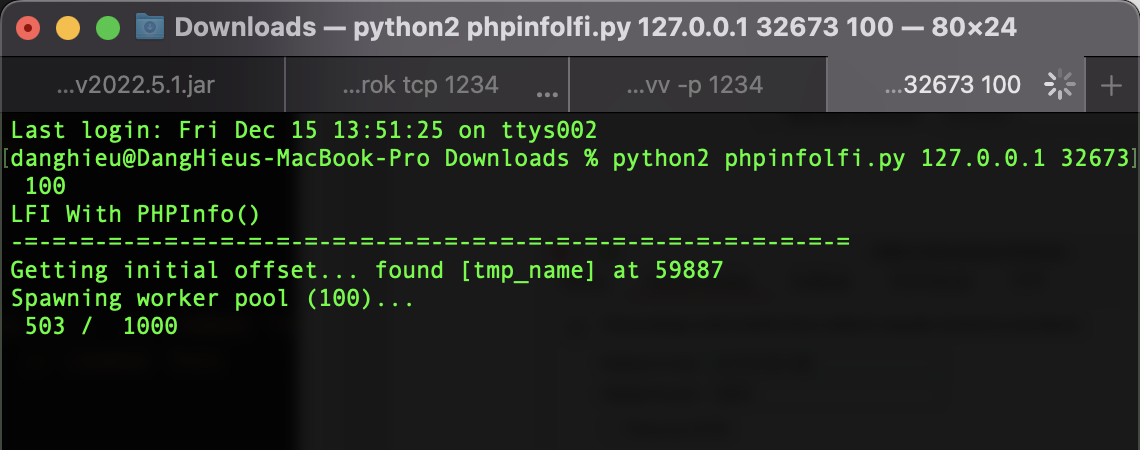
Thay đổi script php là reverse-shell.

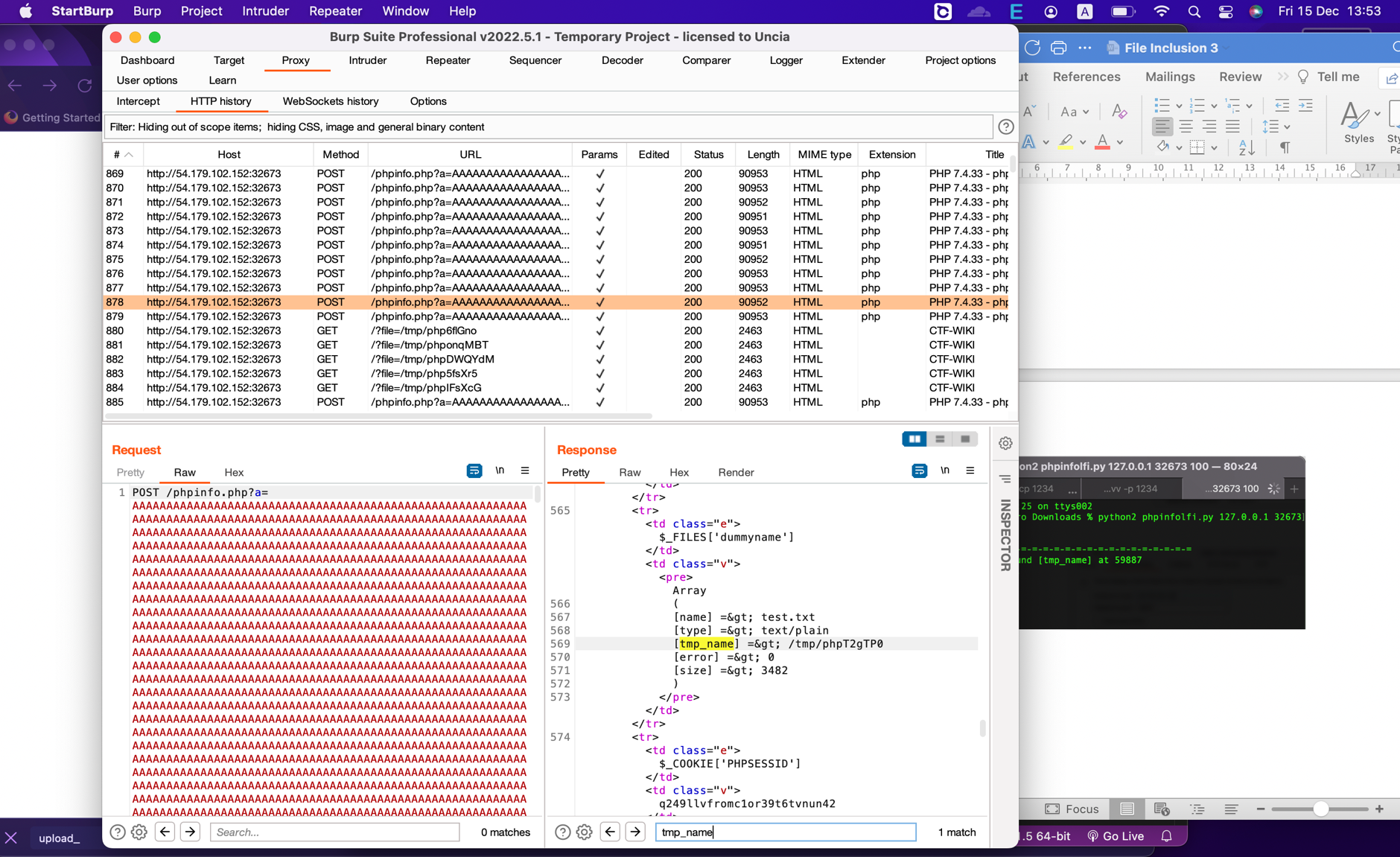
Làm sao để bắt đầu ra của script python trên burp suite?





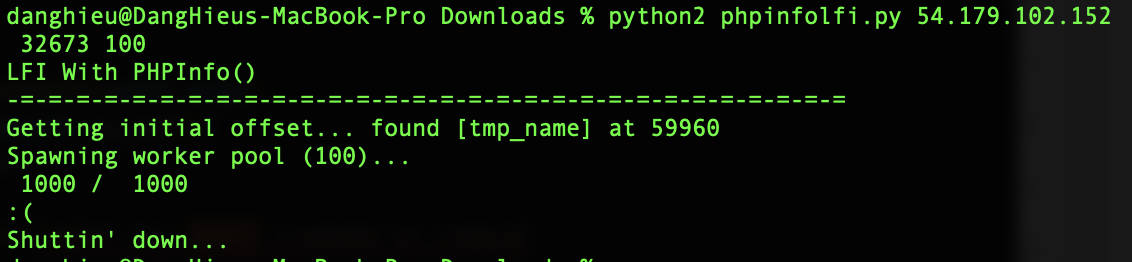
Nó sẽ ánh xạ 127.0.0.1:32673 🡪 54.179.102.152:32673





Lưu ý: nếu bạn muốn reverse shell thì để đúng host là 54.179.102.152

Nếu thực thi được lệnh thành công, nó sẽ báo “Got it!Shell created in /tmp/g”, ngược lại là “Shut down”.



Tại sao lại không chạy được?

Mình nghĩ muốn win race condition, request phải lớn hơn đầu ra của phpinfo script nhưng padding=4000 là chưa đủ nên không chạy được.

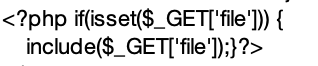
Đây có thể là lỗi của tác giả hoặc do mình thiết xót gì đó. Buộc mình phải chuyển sang 1 hướng tấn công khác.

**Cách 2: LFI to RCE via php://filter**

Đầu tiên mình dùng filter để đọc file php:

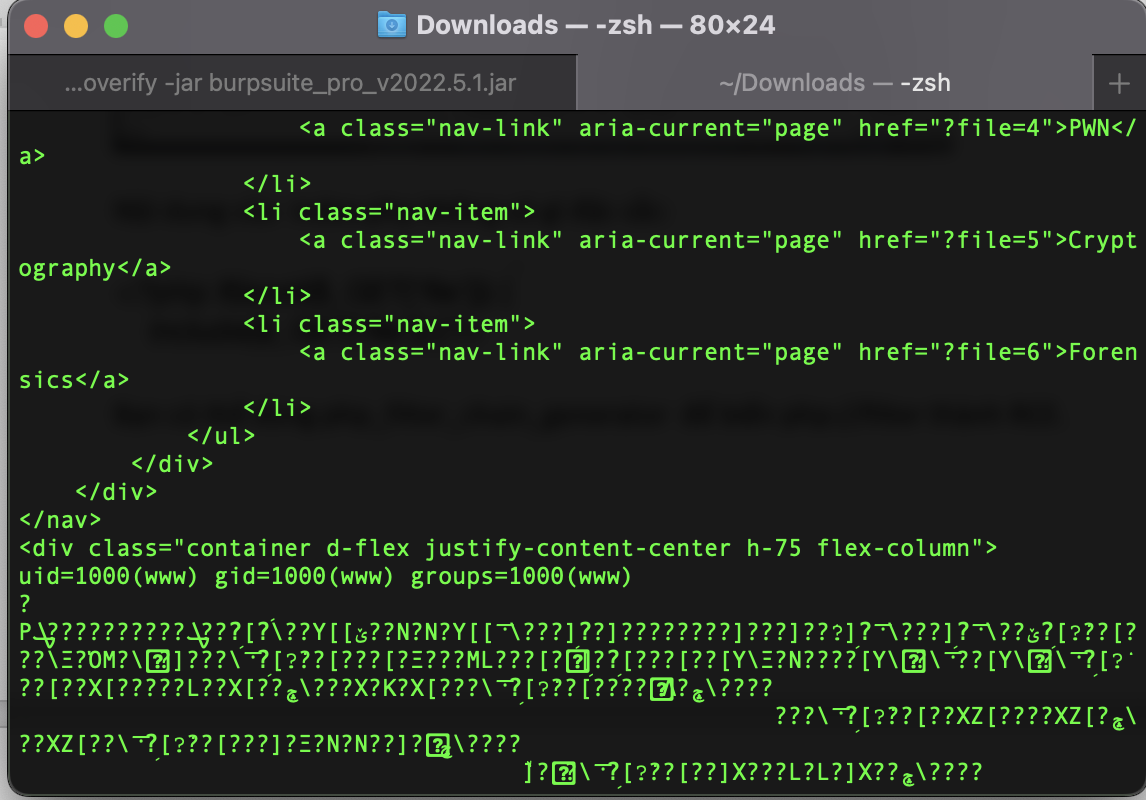


Nội dung của index.php không có gì đặc sắc:



Bạn có thể dùng php\_filter\_chain\_generator để biến php://filter thành RCE.

Payload rất dài. Mình sao chép vào Burpsuite nhưng nó không chạy. Phải dùng lệnh curl:



Nếu lần sau bạn gặp lại dạng này, nhớ dùng script sẽ nhanh hơn. (LFI2RCE.py)

**Flag:CHH{PHP1nfO\_Brut3fORC3\_tmP\_d8f76a5644ab4ad13a6890e4f5c03ac1}**