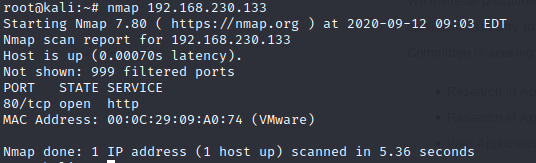
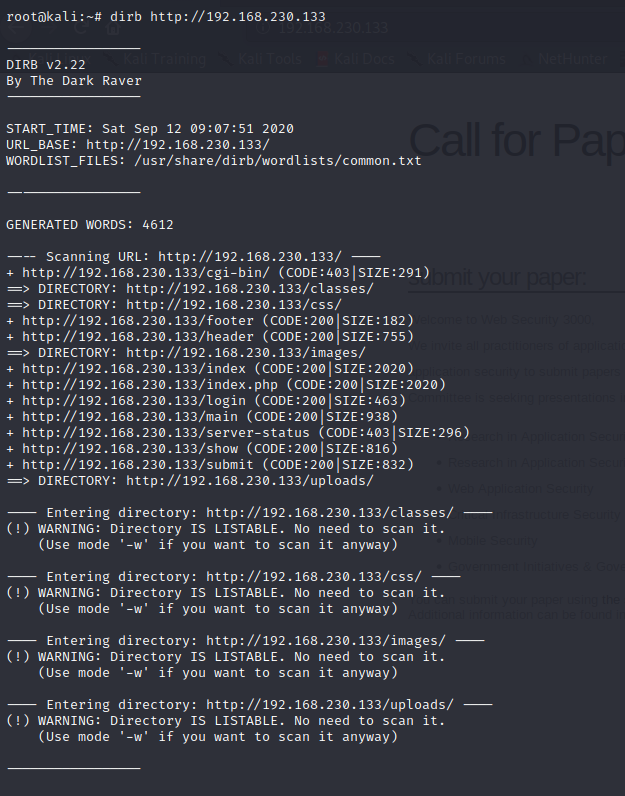
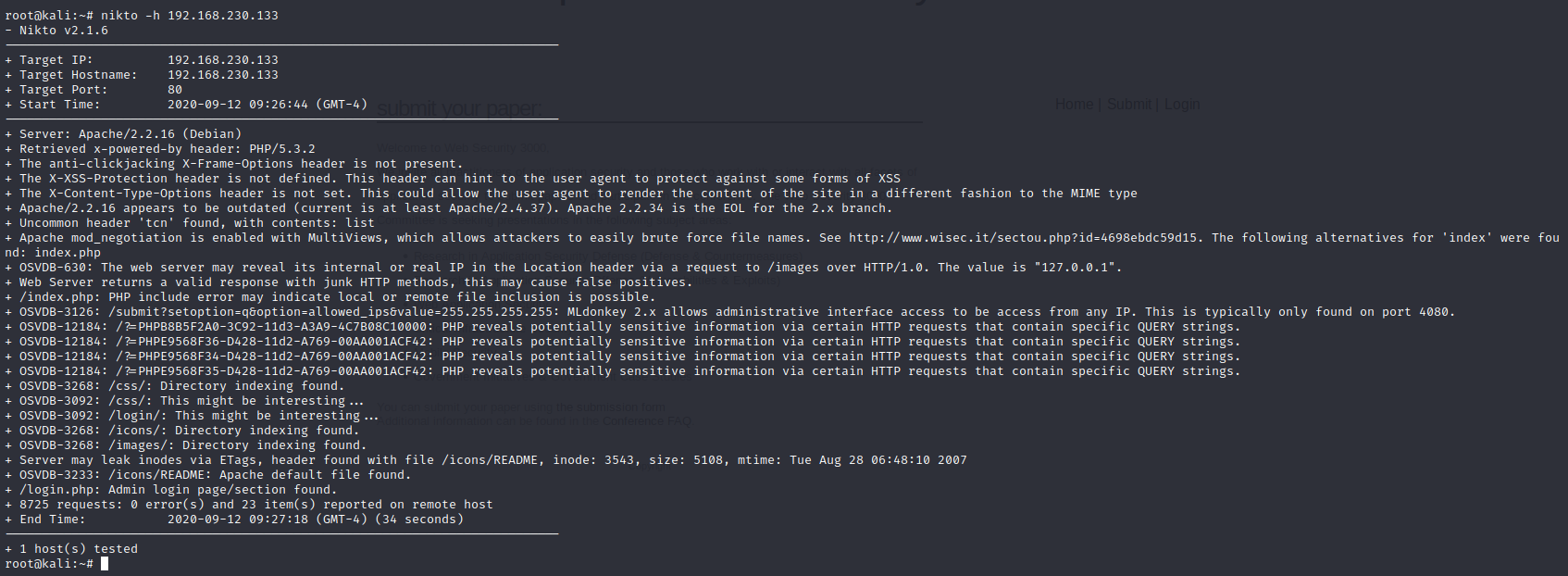
Xác định các dịch vụ đang chạy trên máy chủ 192.168.230.133



Chạy dirb



Chạy nikto



Nikto đã xác định PHP include error có thể cho biết các tệp cục bộ trên máy chủ.

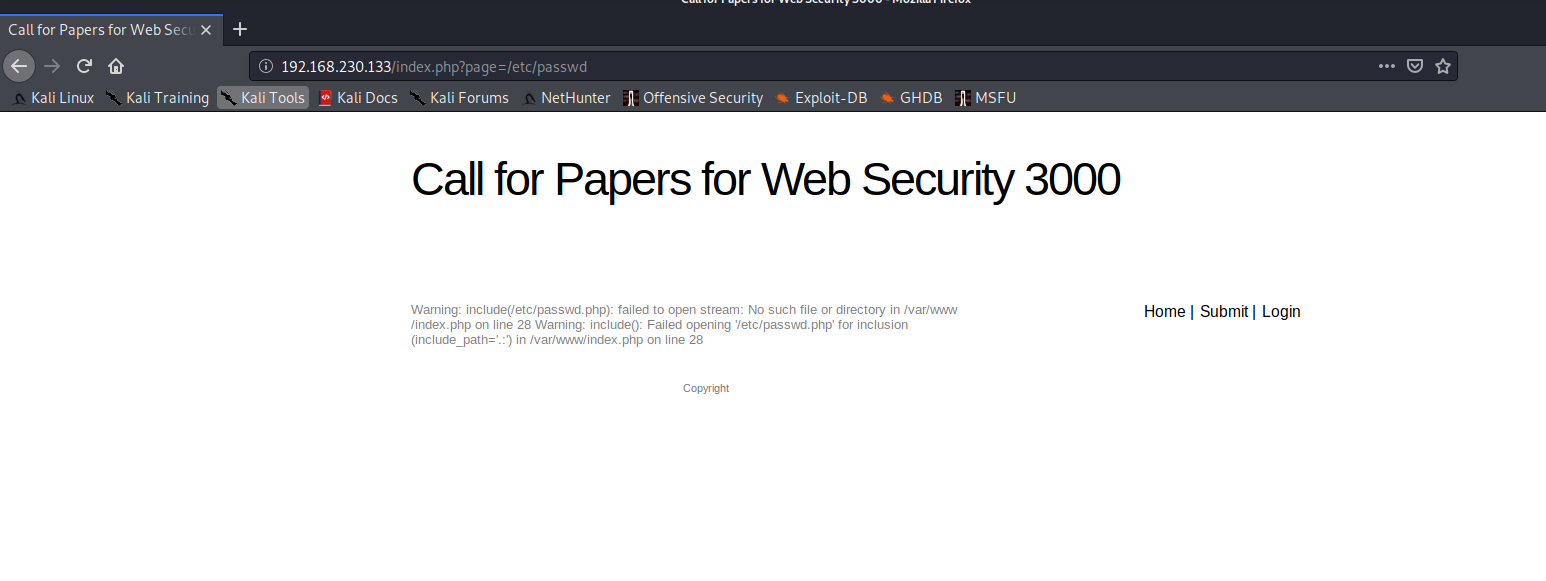
Các liên kết trang như sau:

http://192.168.230.133/

http://192.168.230.133/index.php?page=submit

http://192.168.230.133/index.php?page=login

Thử truy cập tập /etc/passwd trên máy chủ

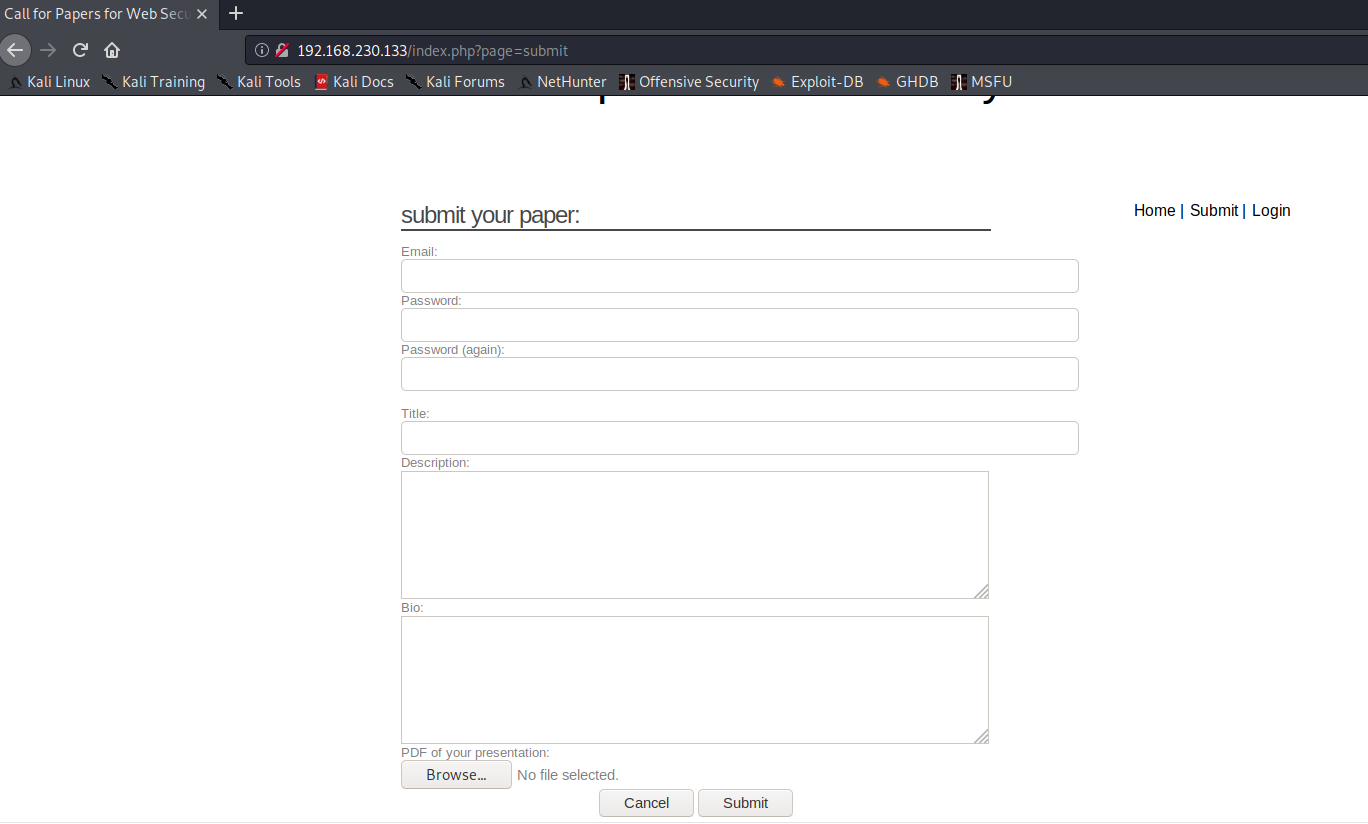


Vì passwd gắn với đuôi .php nên cần sử dụng Null byte

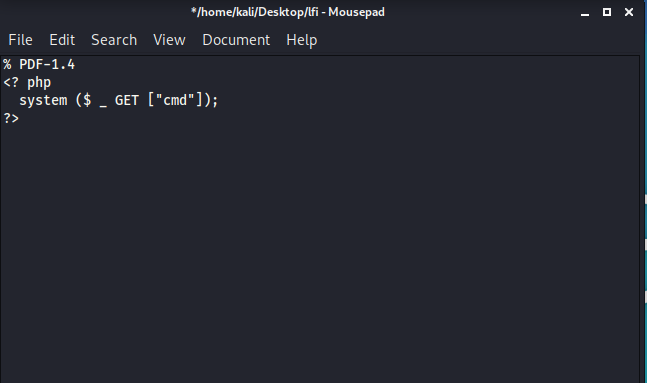


Điều này cho thấy tham số trang dễ bị ảnh hưởng bới LFI.

Khai thác LFI bằng cách tải lên một PHP shell được nhúng trong PDF.



Tạo một tệp PDF với mã PHP như sau:



Tải tệp lên trên máy chủ.

