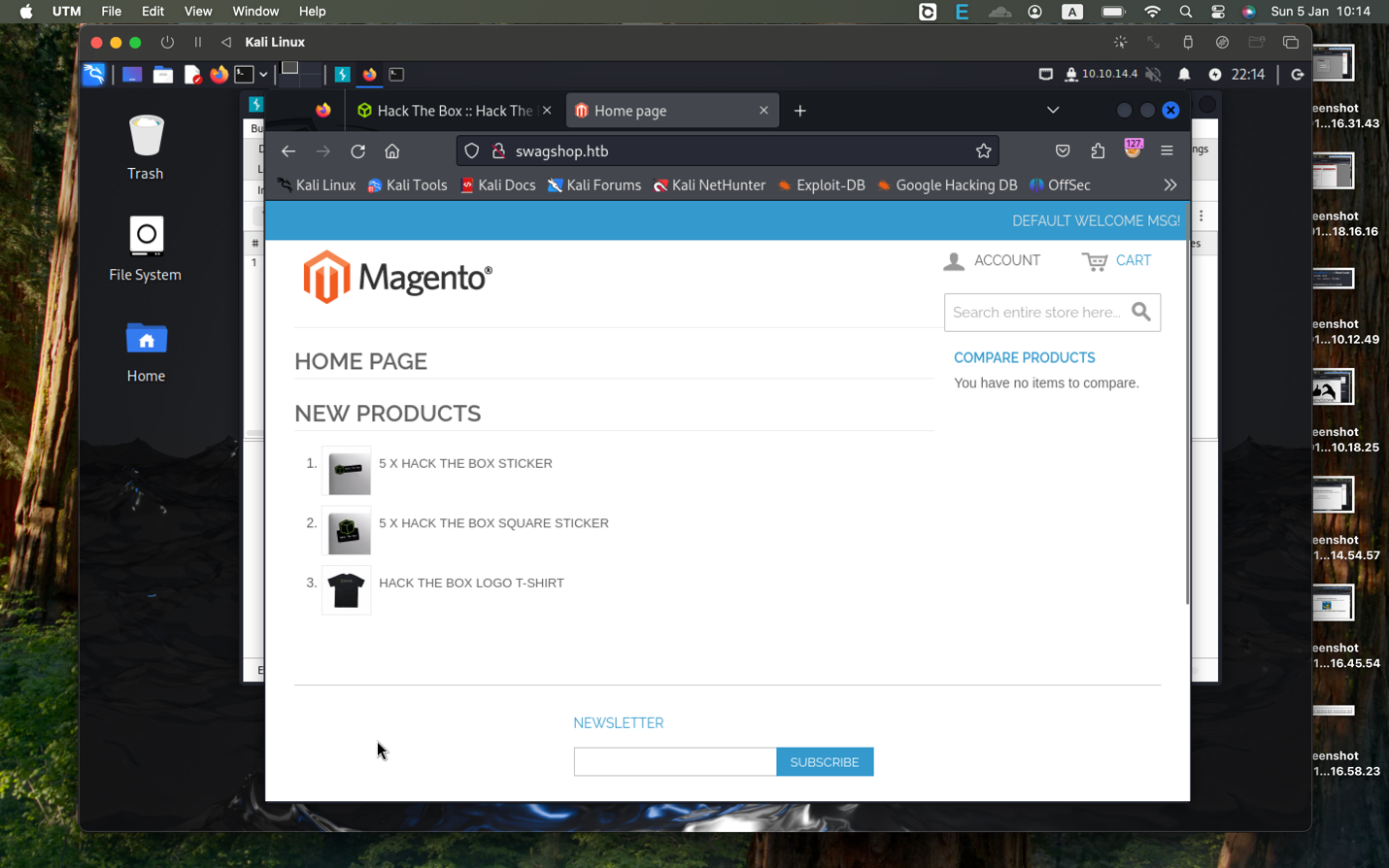


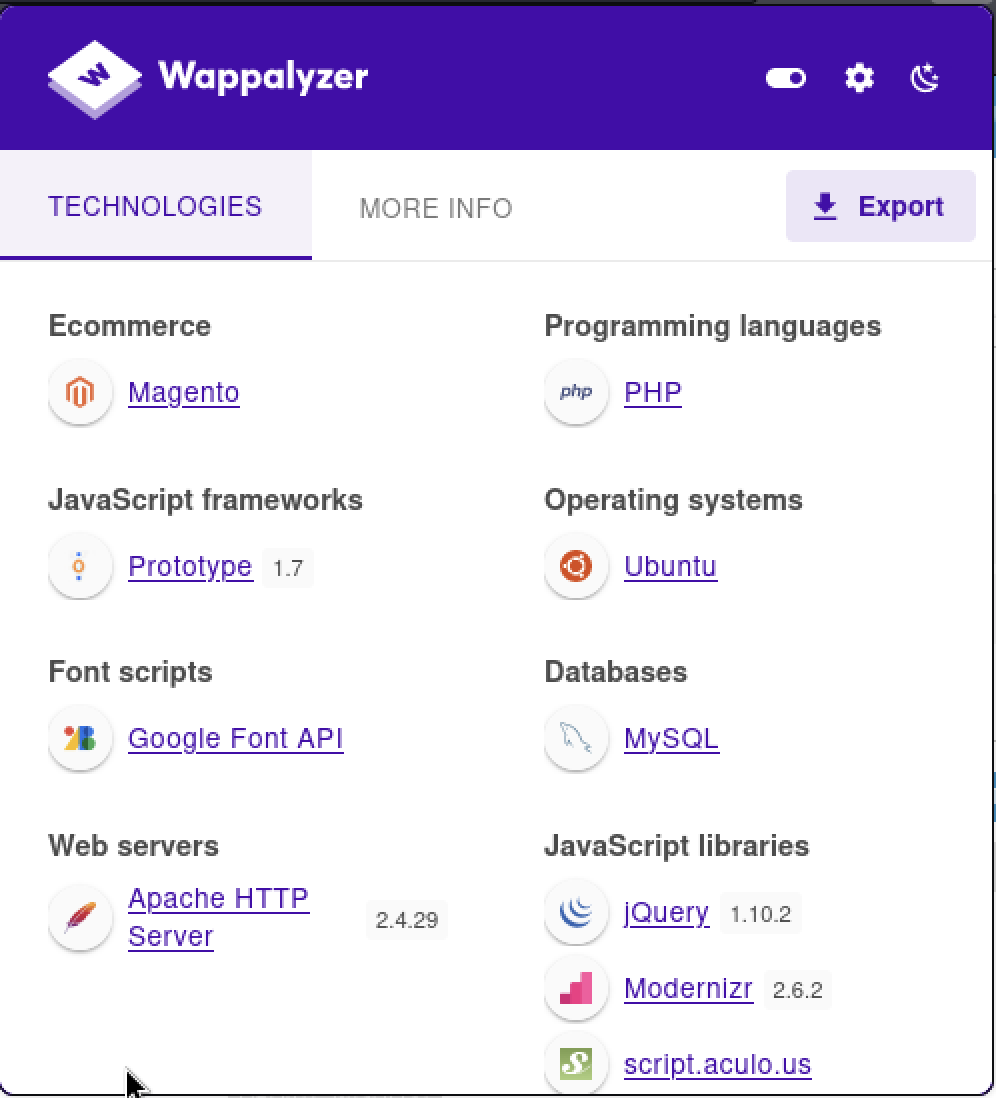
Giao diện trang web



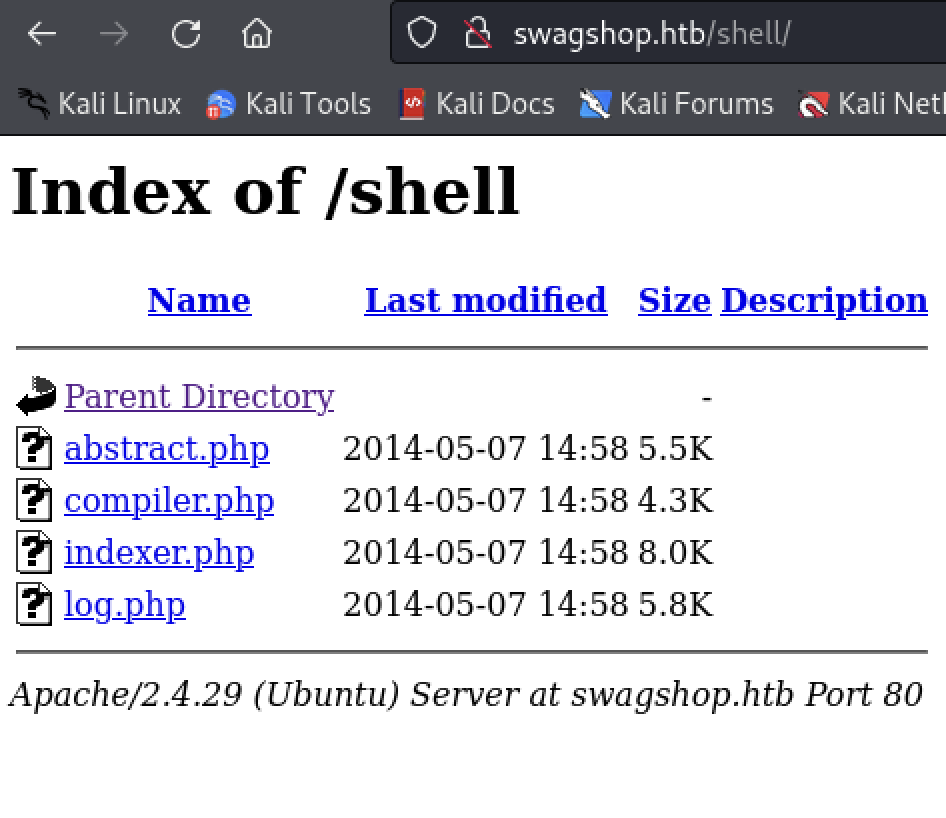
Ít dịch vụ như vậy chỉ có khai thác lỗ hổng web

Khổ nỗi trang web nhiều chức năng quá, thăm dò lỗ hổng sẽ vất vả đây

Công nghệ web sử dụng

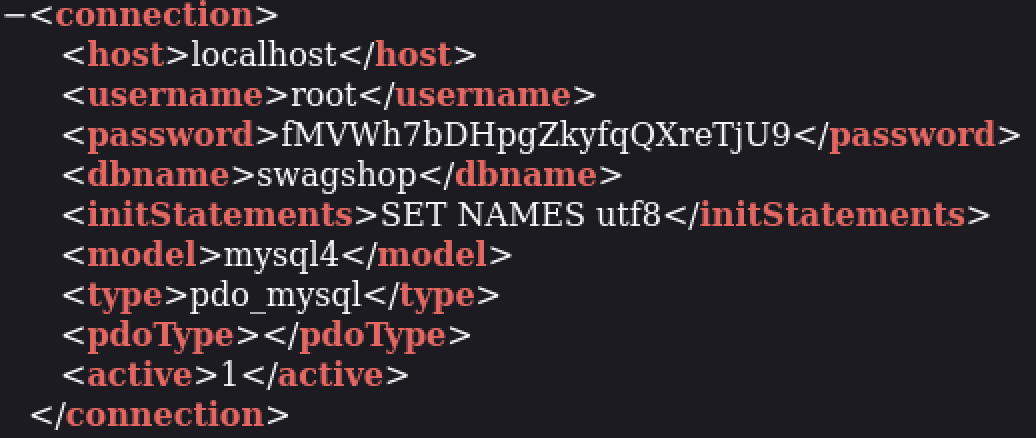


Trang web bị lỗi index, thư mục lộ tập tin nhạy cảm

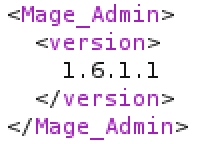


Mình tìm được tệp chứa mật khẩu kết nối dịch vụ mysql:

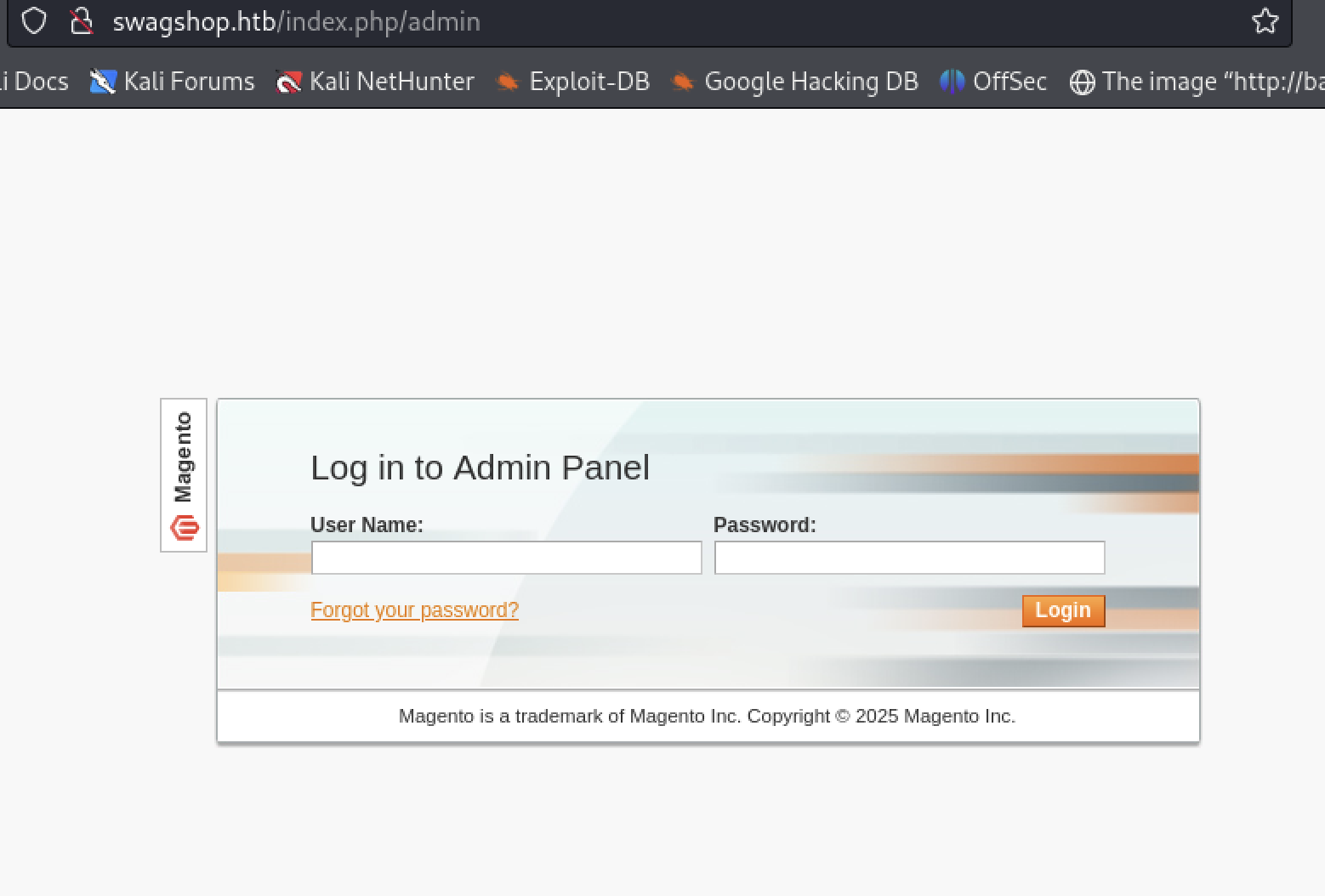
app/etc/local.xml



/app/code/core/Mage/Admin/etc/config.xml

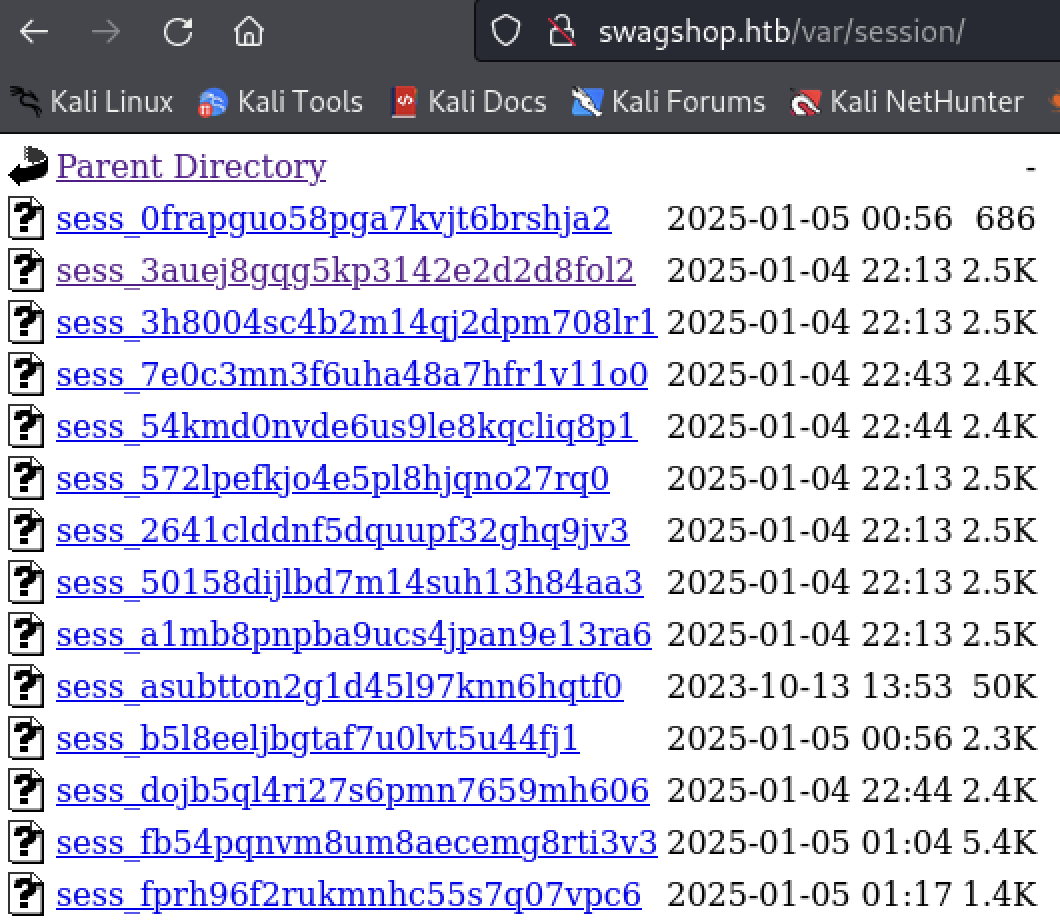


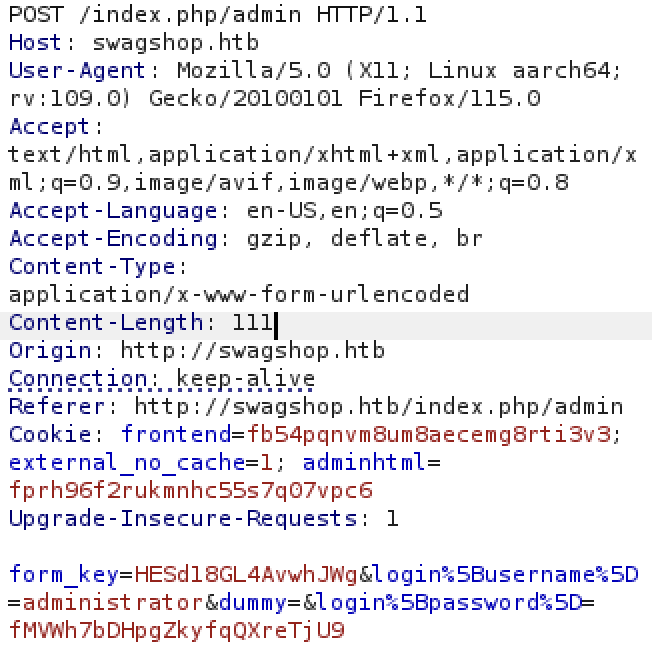
Mình nhờ ChatGPT tìm các tệp chứa phiên bản của magento thì tìm được trang admin



Dùng tài khoản trên đăng nhập nhưng không được

Mình tìm được các phiên của người dùng trên /var/session, có thể là admin





Bạn thấy cookie frontend=fb54pqnvm8um8aecemg8rti3v3 và

adminhtml=fprh96f2rukmnhc55s7q07vpc6 có trong /var/session

Rất đáng để thử hết các phiên. Nhưng mình không biết thay các phiên như thế nào cho nhanh

Mình biết magento phiên bản khá cũ nên tìm được 2 CVE trên mạng.

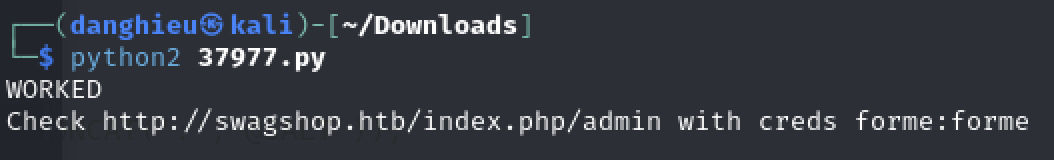
Có 1 khai thác thành công: Magento eCommerce - Remote Code Execution

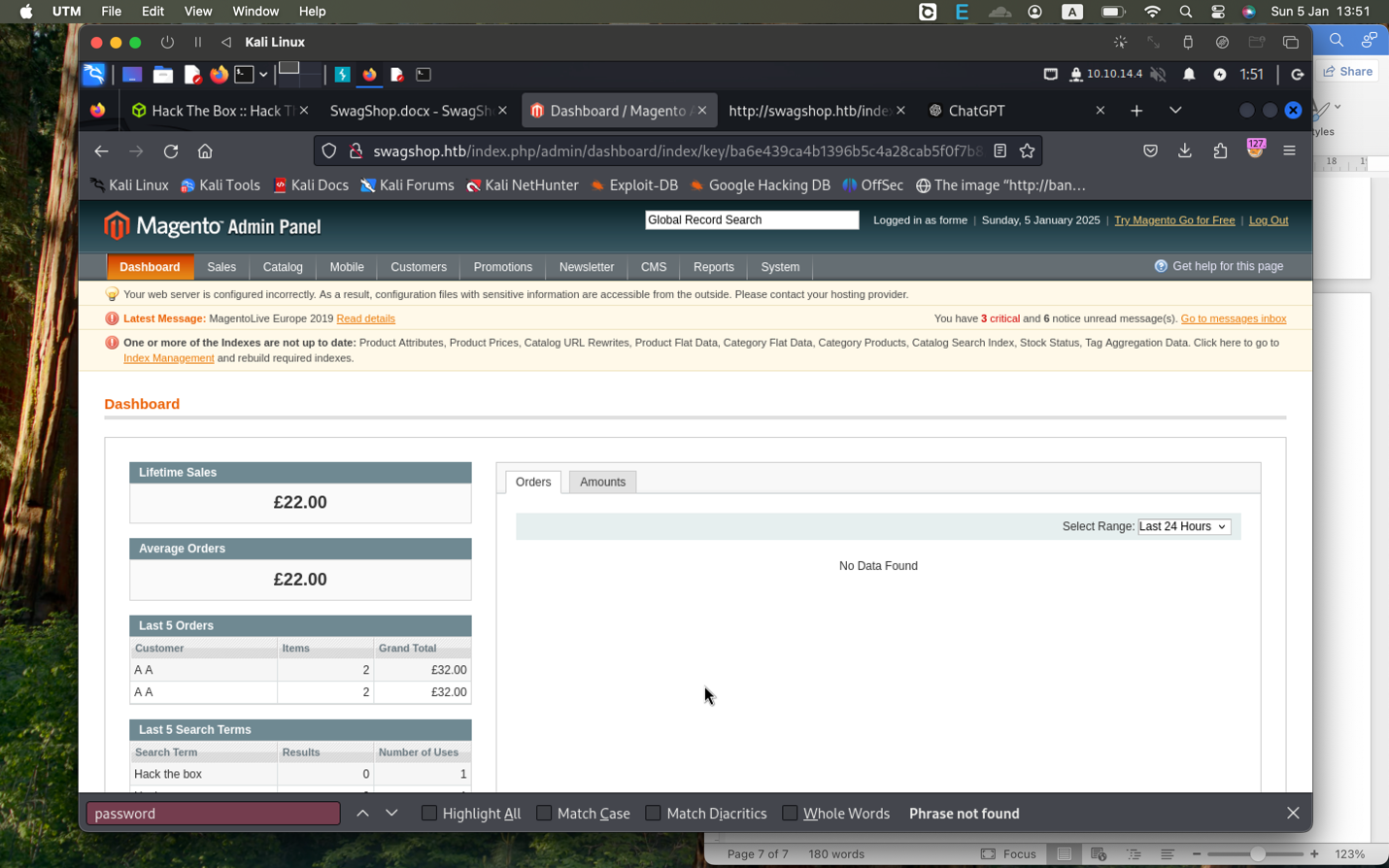
Bạn phải chỉnh sửa lại đường dẫn admin

target = "http://swagshop.htb/index.php"

target\_url = target + "/admin/Cms\_Wysiwyg/directive/index/"

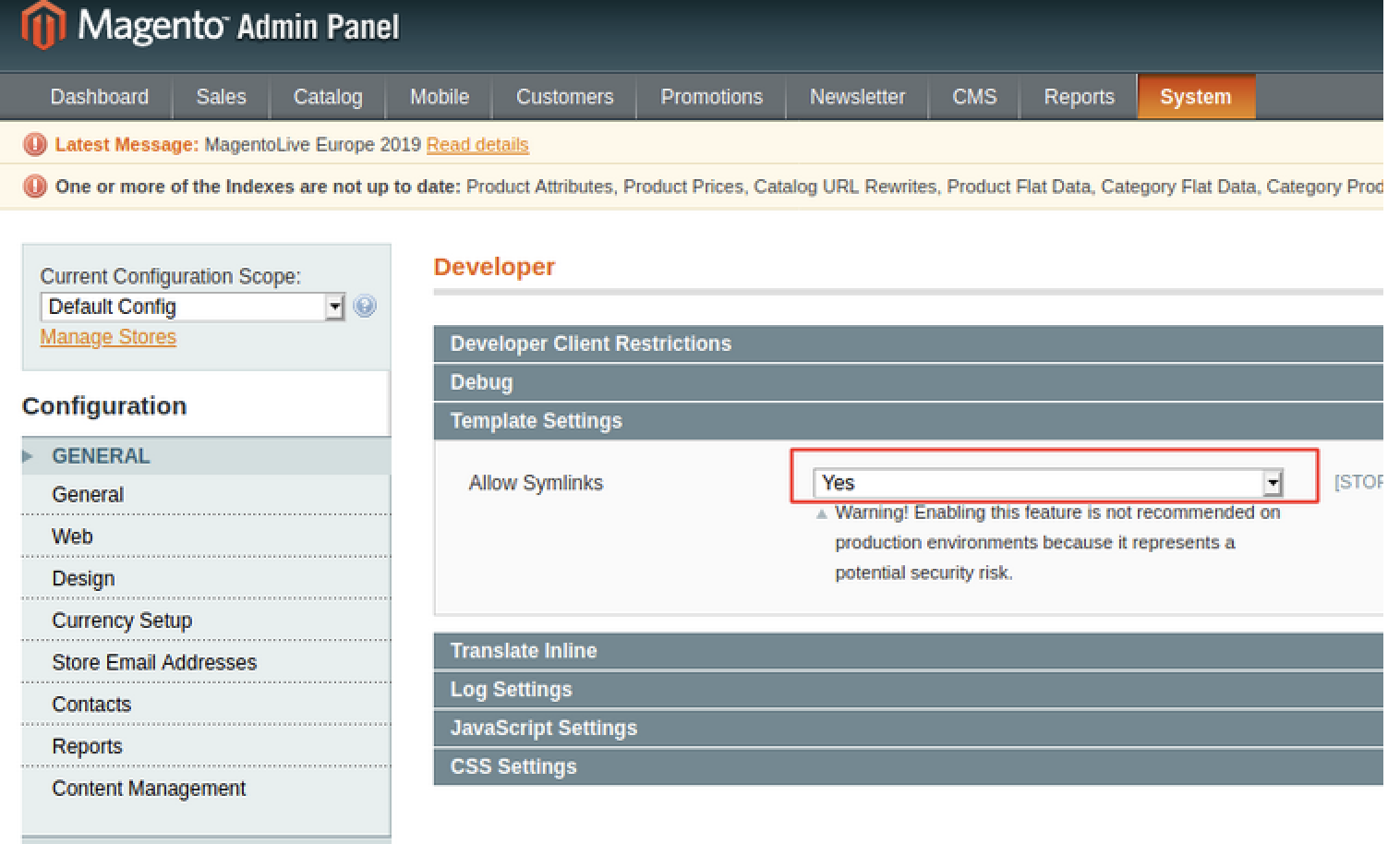
Chạy khai thác, tạo được 1 tài khoản admin





Bây giờ chúng ta đang ở Magento Admin Panel. Có nhiều cách để lấy shell nhưng chúng ta quyết định khai thác lỗ hổng File Upload.

Các tệp đã tải lên không thể truy cập được ở dạng thô, điều này sẽ ngăn chúng ta thực thi chúng. Điều này có thể bị bỏ qua bằng cách cho phép symlinks trong Developer Settings (System🡪Configuration🡪Developer🡪Template Settings)



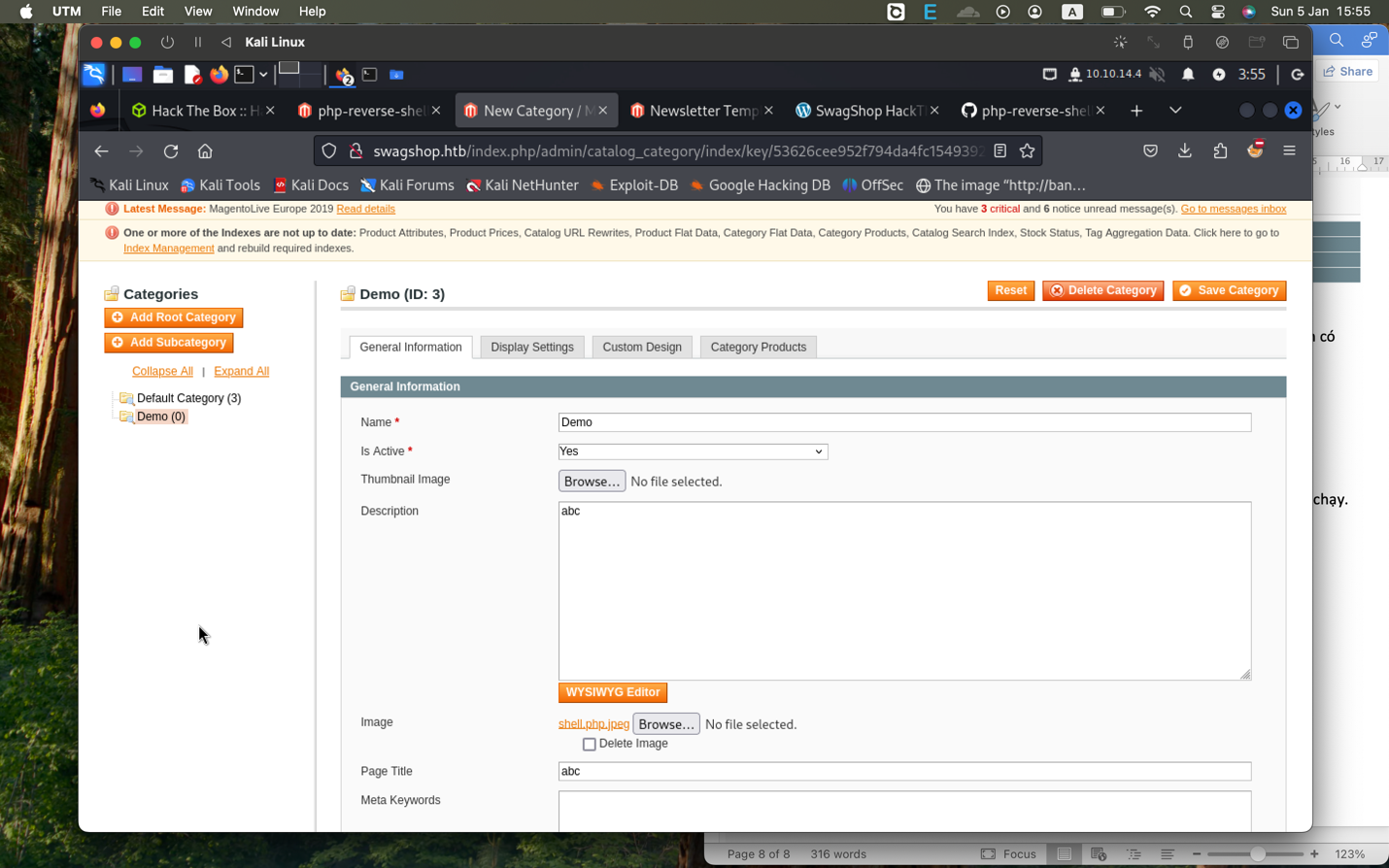
Magento có sẵn tính năng hạn chế tải các tập tin độc hại, chỉ cho tải tập tin có đuôi là .png, .jpeg, .gif

Mình có thể vượt qua bằng cách làm xáo trộn phần mở rộng tệp:

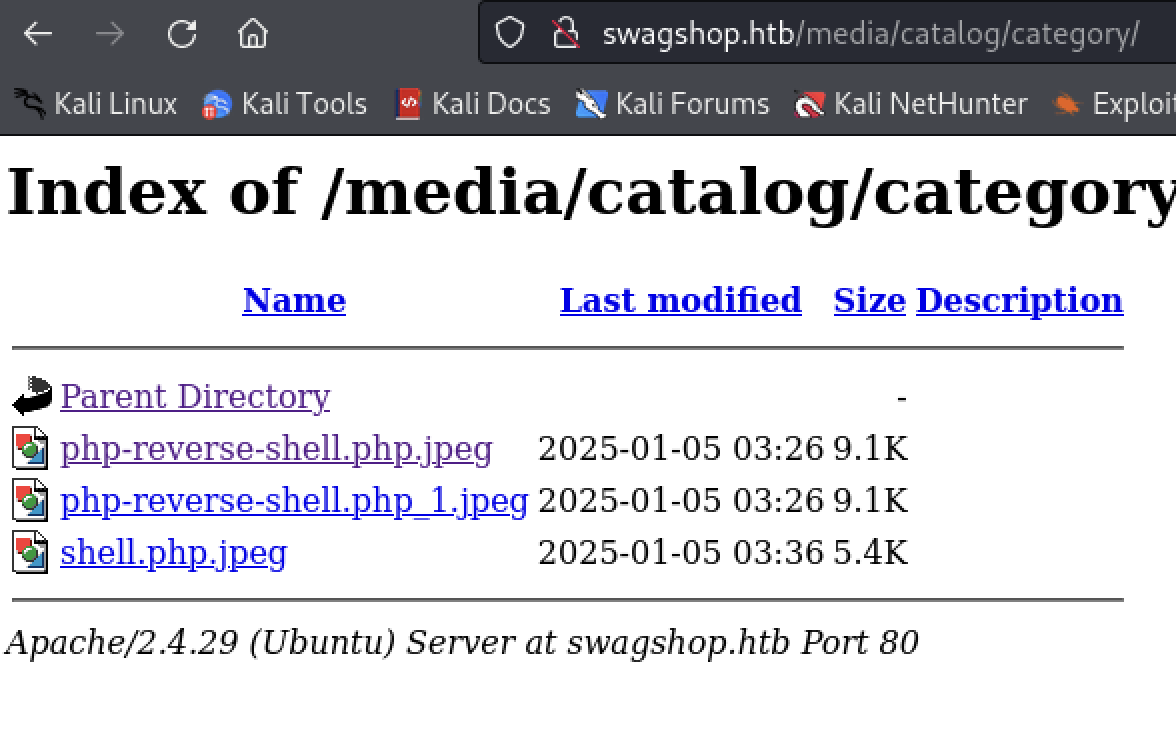
shell.php.jpeg

Payload mình dùng là php-reverse-shell của PentestMonkey

Chúng ta tạo 1 category mới, tên là Demo. Nó cần được active để payload chạy. Sau đó upload reverse shell trong mục image



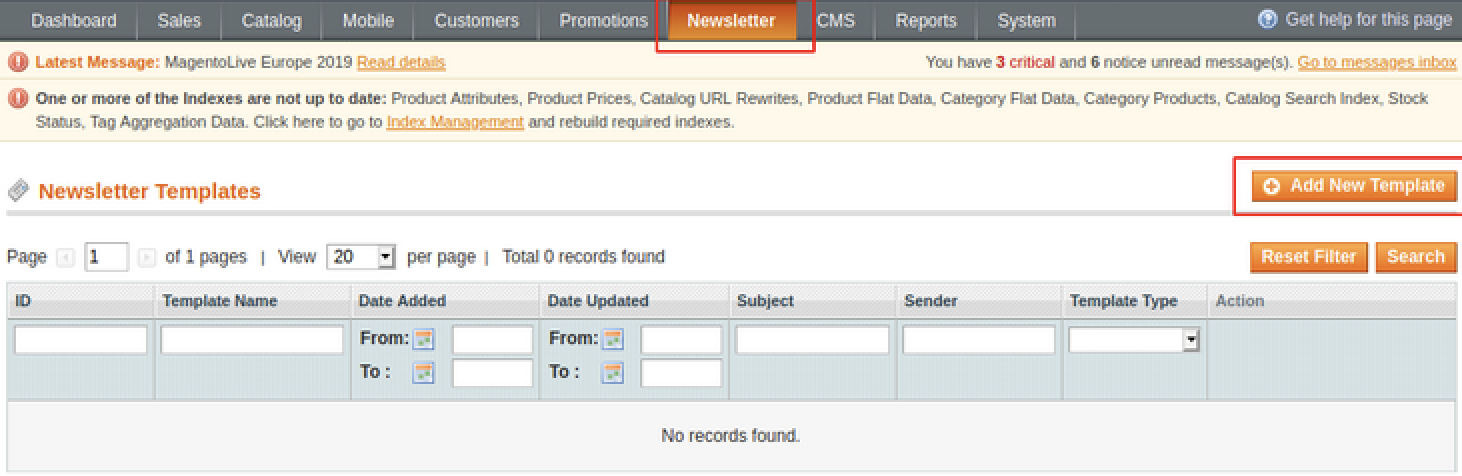
Tệp reverse-shell của chúng ta nằm ở đây



Nhưng không thực thi được. Nó chỉ lộ source code thôi

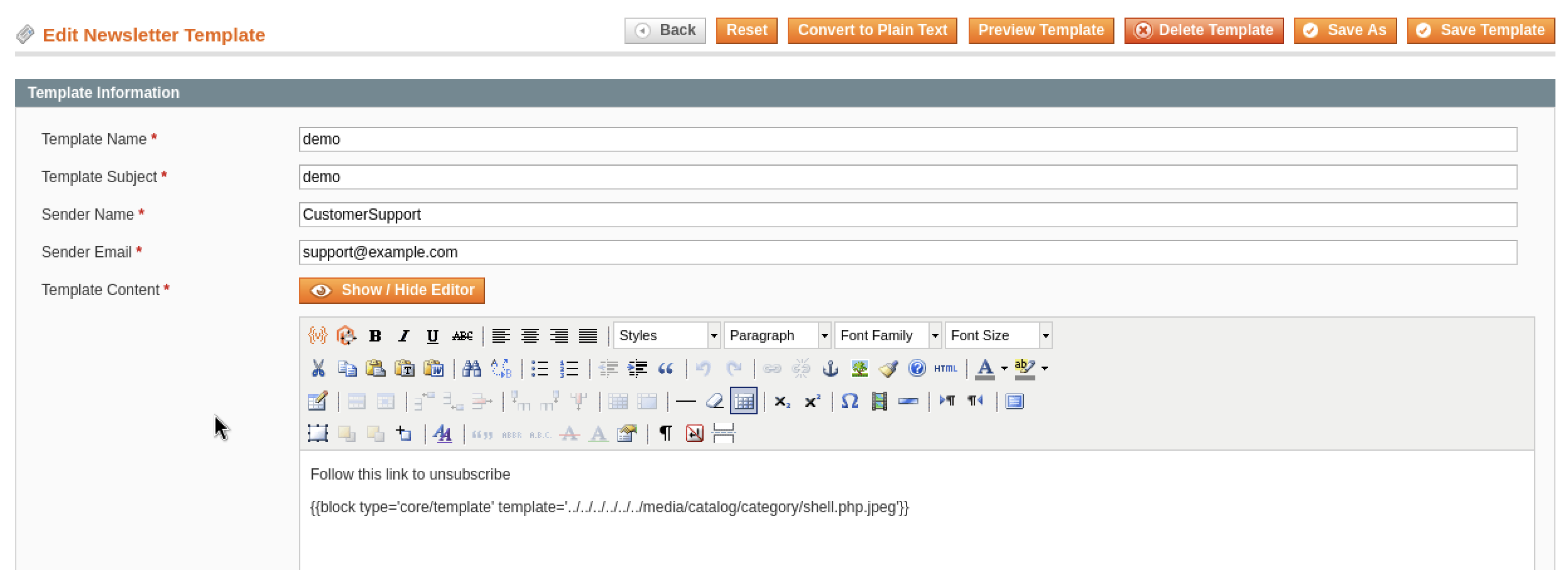
Đến đây thì mình không biết làm nữa.

Tạo mới 1 template

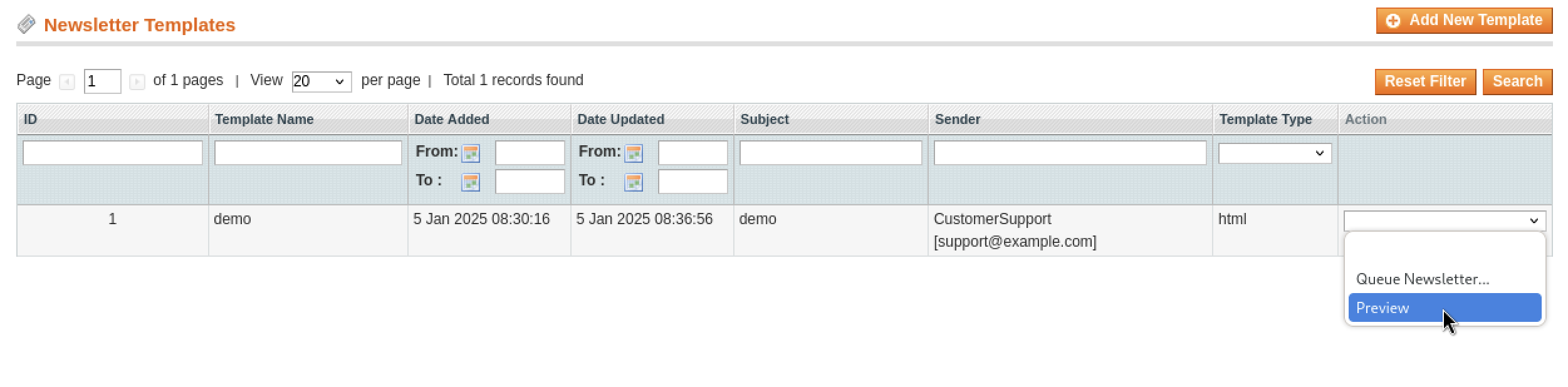


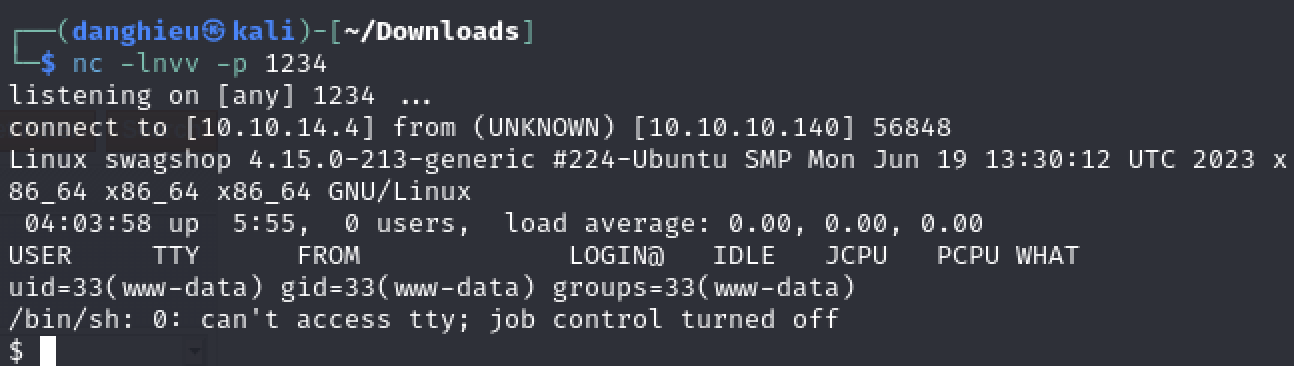
Trong Newsletter Template, thêm đường dẫn của template là reverse-shell

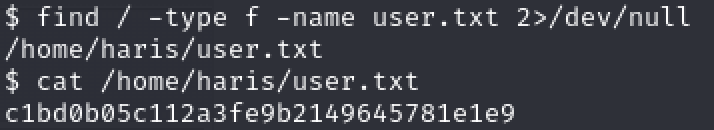
{{block type='core/template' template='../../../../../../media/catalog/category/shell.php.jpeg'}}

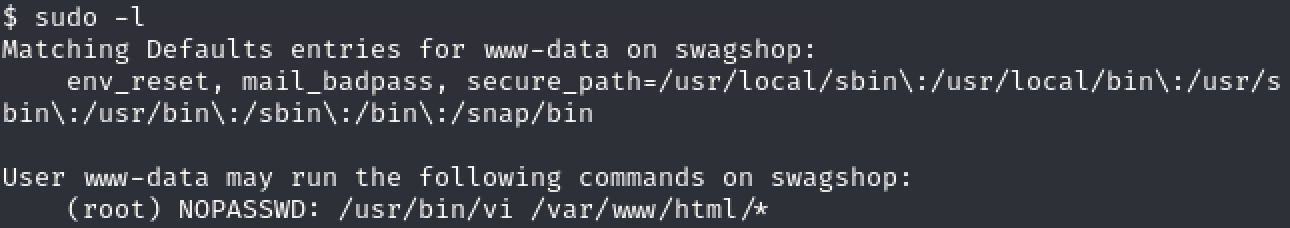


Chúng ta xem trước Newsletter mới tạo









Chạy lệnh này để leo thang đặc quyền:

sudo /usr/bin/vi /var/www/html/\* -c ':!/bin/sh' /dev/null

