BÀI TẬP CTF

Bảo mật web và ứng dụng – NT213.M21.ANTN

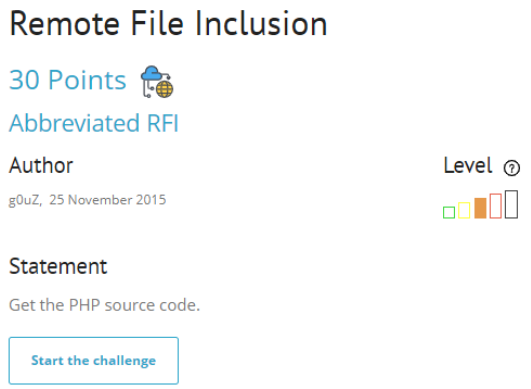
Giảng viên hướng dẫn: *Đỗ Hoàng Hiển*

Sinh viên thực hiện: *19520199 – Lê Tôn Nhân*

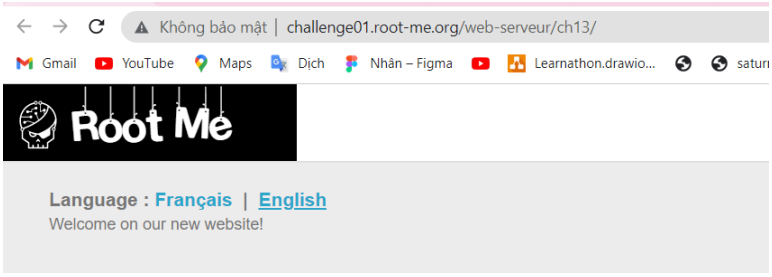
Challenge 4: Remote File Inclusion (level medium)

Link challenge: https://www.root-me.org/en/Challenges/Web-Server/Remote-File-Inclusion

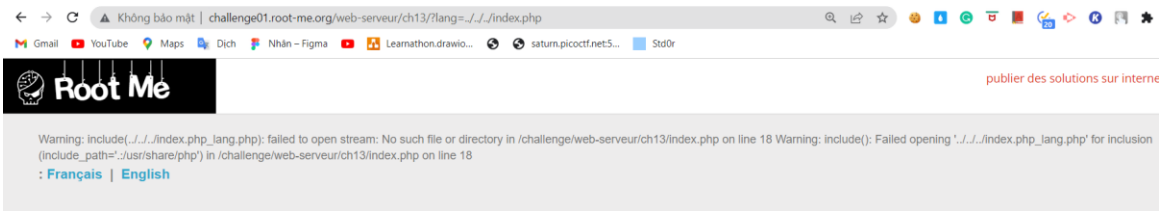
- Thử thách yêu cầu ta lấy mã nguồn PHP



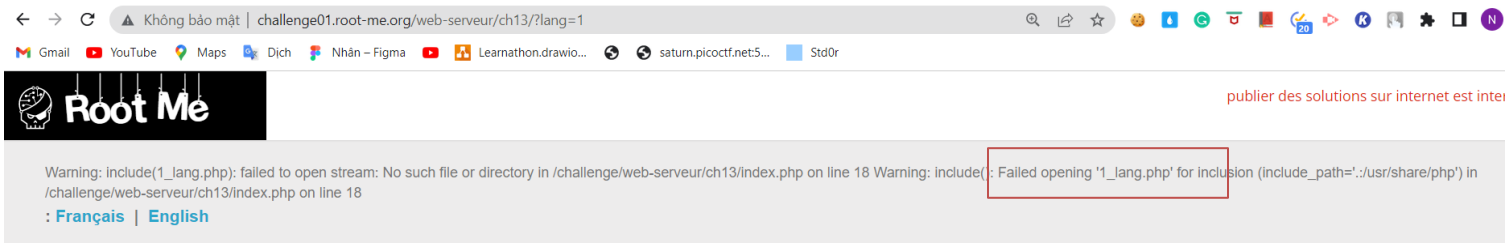
- Truy cập vào challenge ta được trang web như bên dưới



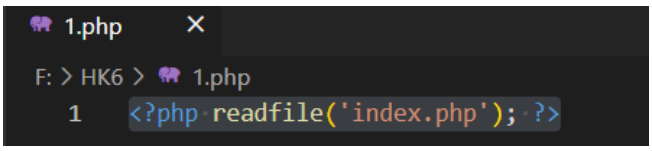
- Trang web gồm 2 tab là Francais và English
- Với các dạng bài file inclusion ta sẽ thử vào giá trị của tham số, ở đây ta sẽ thử với url là http://challenge01.root-me.org/web-serveur/ch13/?lang=../../../index.php



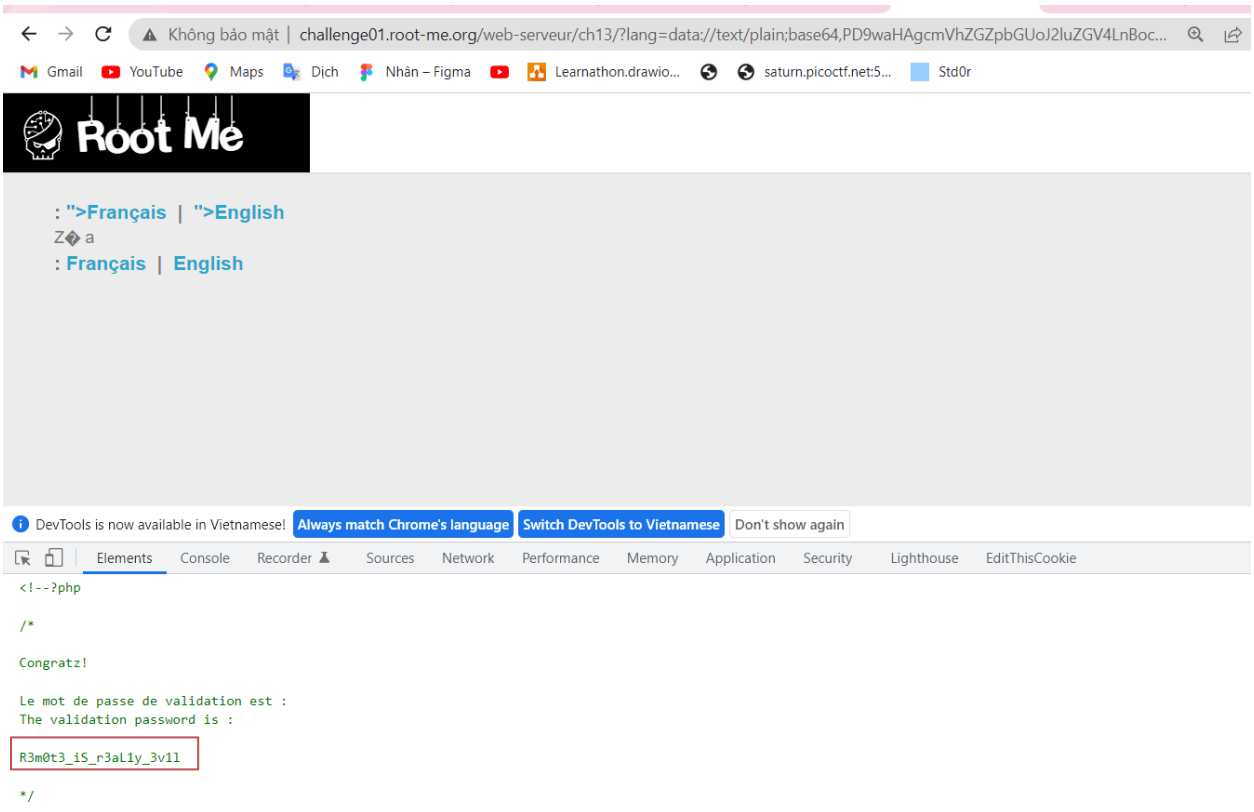
- Kết quả xuất hiên thông báo lỗi
- Thử với lang=1 ta nhận được thông báo như bên dưới



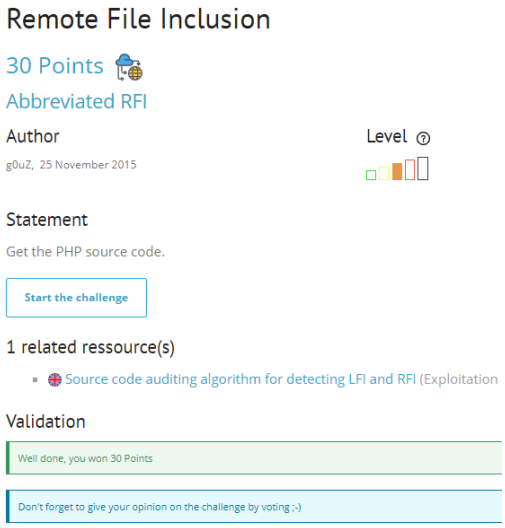
- Ta thấy rằng trong thông báo có dòng **include(): failed opening "1_lang.php".** Từ đó ta suy ra được phần code php có dạng **include($_GET['lang']_lang.php)**
- Tạo đoạn code php để có thể đọc nội dung của file index.php



- Chúng ta không thực sự cần phải sử dụng mã của mình trên một máy chủ khác, sử dụng **data-wrapper** và chuyển payload dạng base64-encoded cho nó.
- Với mã PHP của ta sẽ được encode base64 **PD9waHAgcmVhZGZpbGUoJ2luZGV4LnBocCcpOyA/Pg==**
- Đoạn payload của ta sẽ là **data://text/plain;base64,PD9waHAgcmVhZGZpbGUoJ2luZGV4LnBocCcpOyA/Pg==**
- Đổi giá trị biến lang thành như trên rồi gửi đi
- Vào xem mã nguồn và ta tìm được flag



- Flag tìm được là **R3m0t3_iS_r3aL1y_3v1l**
- Nộp flag vừa tìm được ta vượt qua thử thách thành công



FLAG: R3m0t3_iS_r3aL1y_3v1l