BÀI TẬP CTF

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

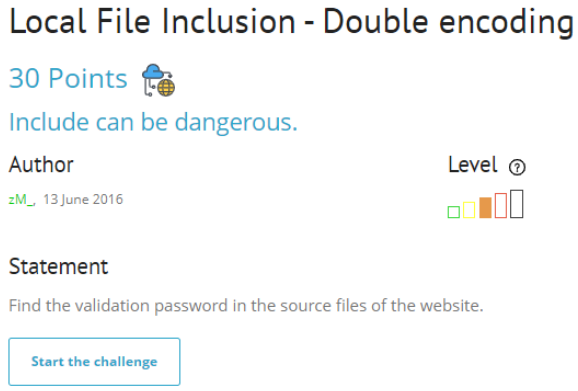
Giảng viên hướng dẫn: *Đỗ Hoàng Hiển*

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

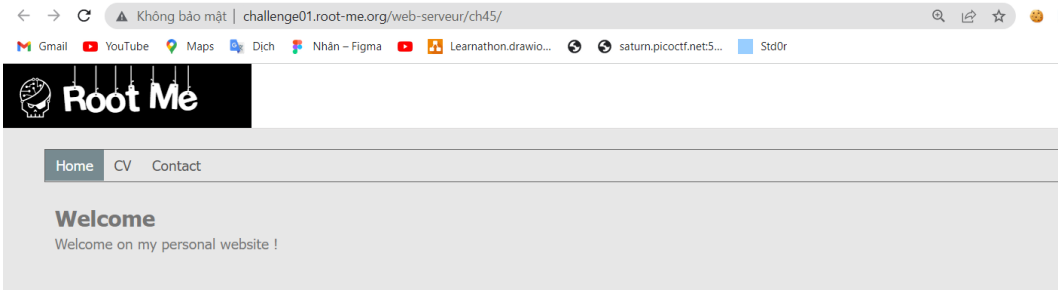
Challenge 2: Local File Inclusion - Double encoding (level medium)

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

- Thử thách yêu cầu ta tìm mật khẩu xác thực trong các tệp nguồn của trang web.

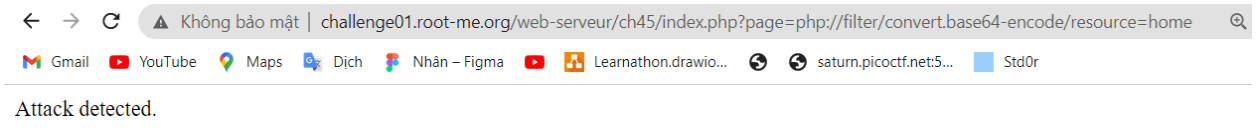


- Truy cập vào thử thác ta nhận được trang web sau



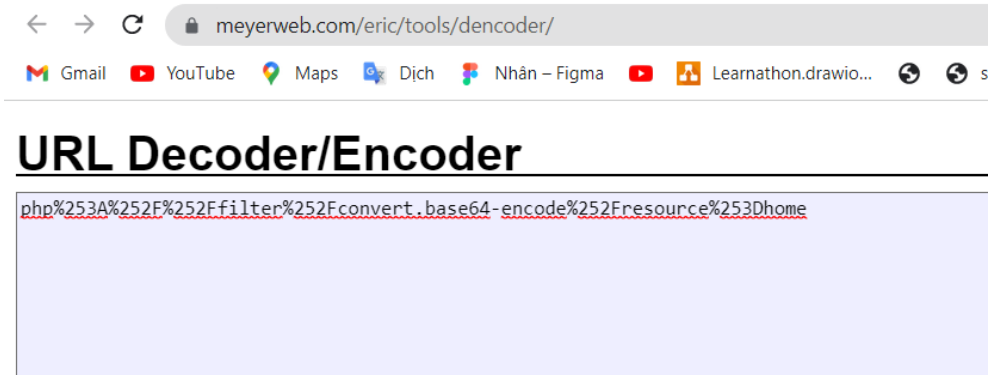
- Gồm 3 tab là home, cv, contact
- Theo như tên challenge ta cần mã hóa gấp đôi đường dẫn để tránh bị phát hiện

- Sử dụng các bộ lọc PHP để tìm các mã nguồn của trang web. Payload đơn giản là: **php://filter/convert.base64-encode/resource=home**
- Với resource có thể gán bằng home, cv hay contact đều được
- Thử truy cập với url http://challenge01.root-me.org/web-serveur/ch45/index.php?page=php://filter/convert.base64-encode/resource=home khi payload chưa được encode.

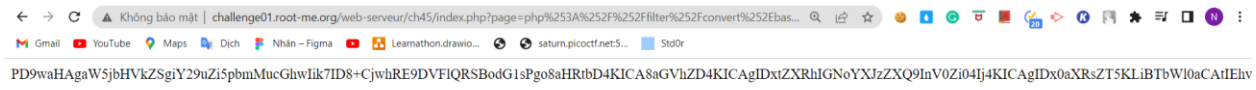


- Kết qua ta thấy dòng attack detected
- Double encode sử dụng tool online (encode url) đoạn payload ta thu được chuỗi

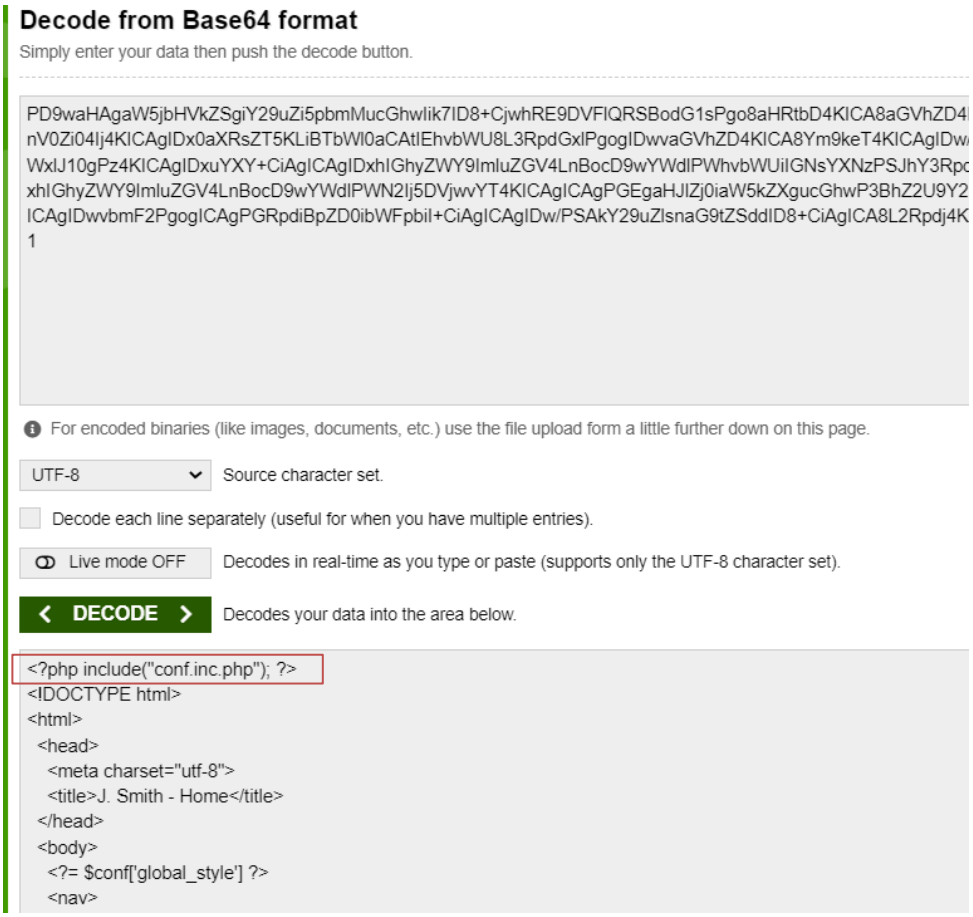
php%253A%252F%252Ffilter%252Fconvert.base64-encode%252Fresource%253Dhome



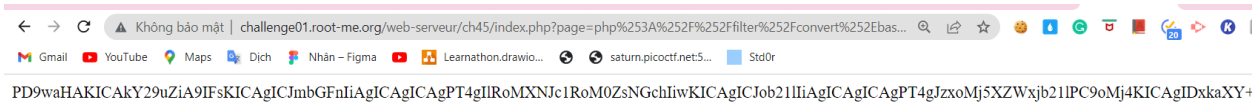
- Truy cập vào url với payload vừa tìm được ta thu được chuỗi base64 bên dưới



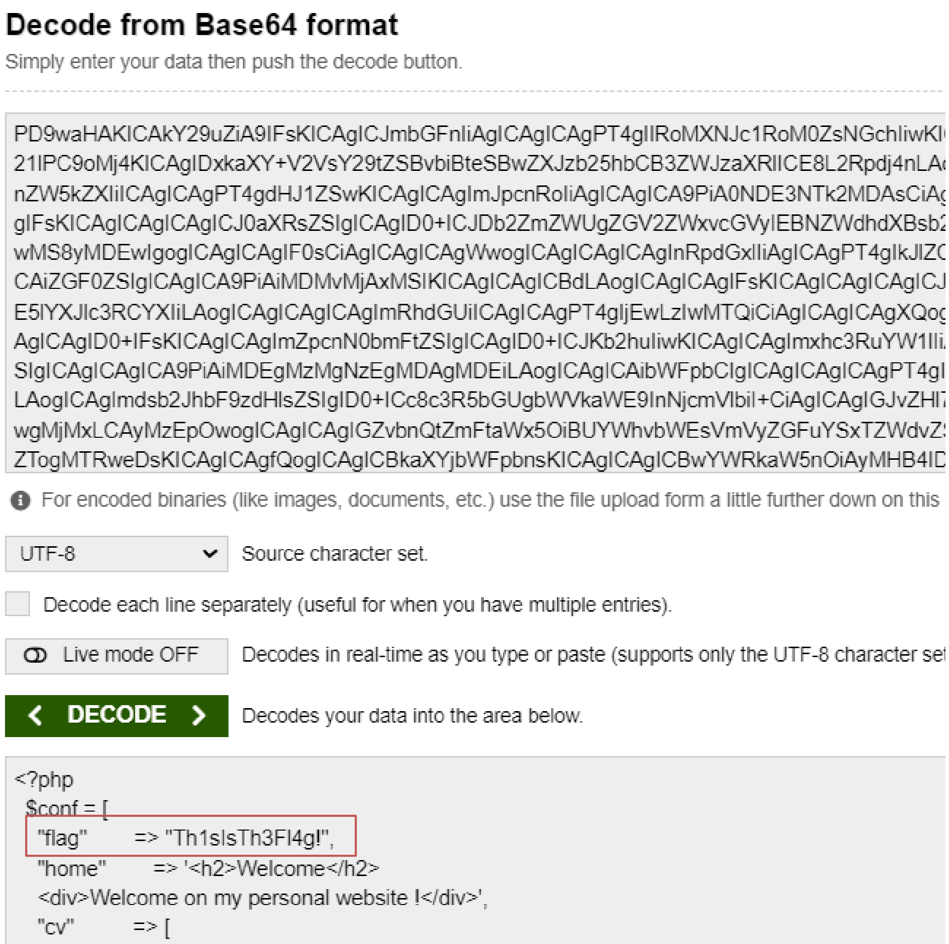
- Decode base64 chuỗi vừa tìm được (sử dụng tool online base64decode)



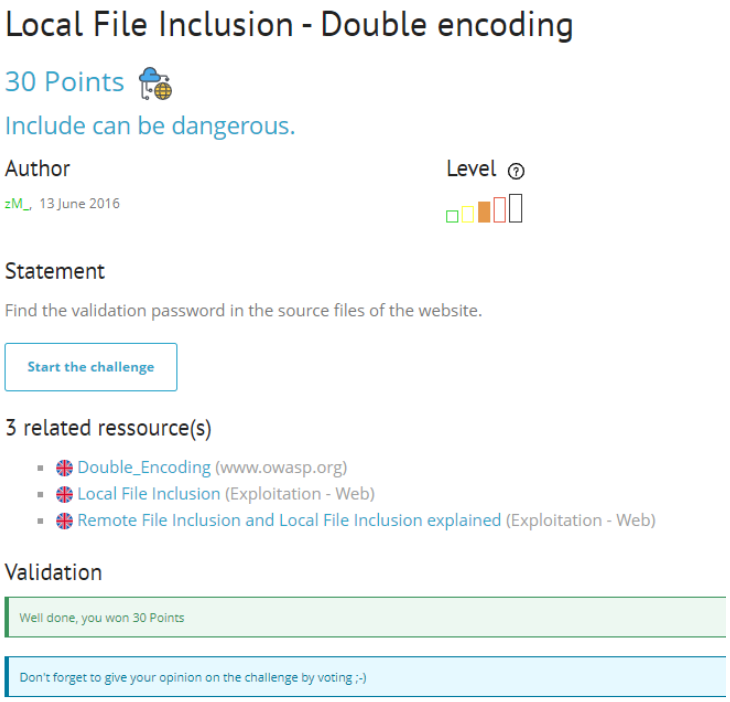
- Ta tìm được mã nguồn của trang chủ là **conf.inc.php**
- Thực hiện lại các bước ở trên với resouce lúc này bằng **conf.icn.php**
- Truy cập vào ta cũng thu được đoạn base64



- Decode đoạn base64 này ta thu được flag



- Nộp flag ta vượt qua thử thách thành công



FLAG: Th1sIsTh3Fl4g!