BÀI TẬP CTF

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

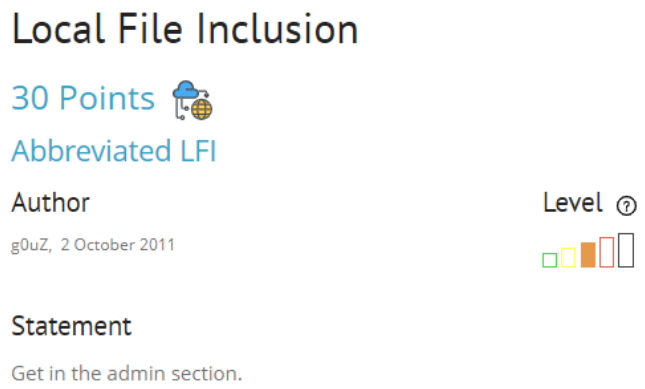
Giảng viên hướng dẫn: *Đỗ Hoàng Hiển*

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

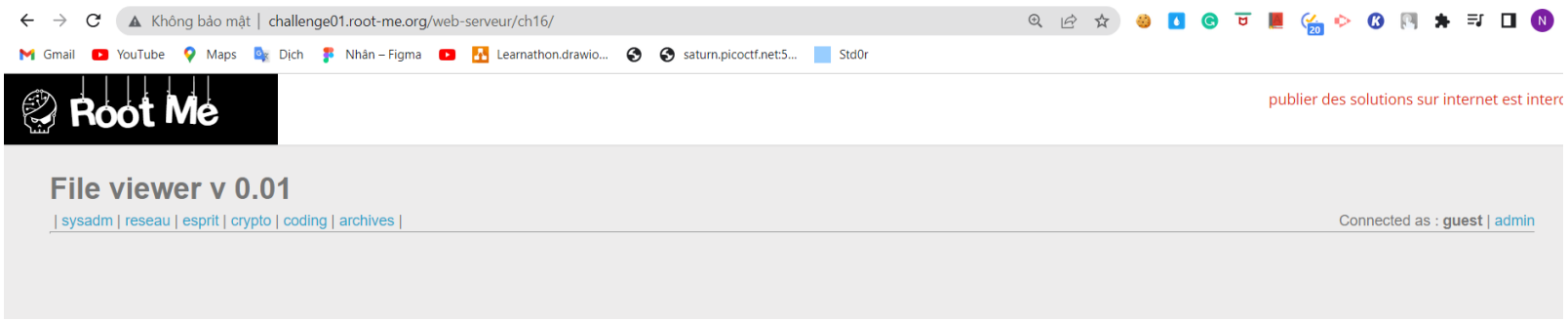
Challenge 1: Local File Inclusion (level medium)

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

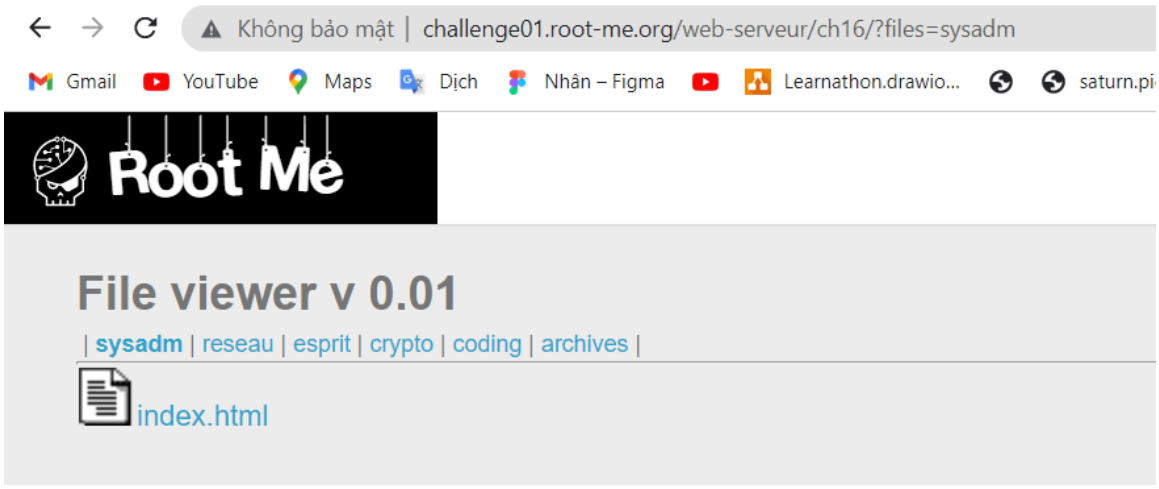
- Thử thách yêu cầu ta lấy section của admin



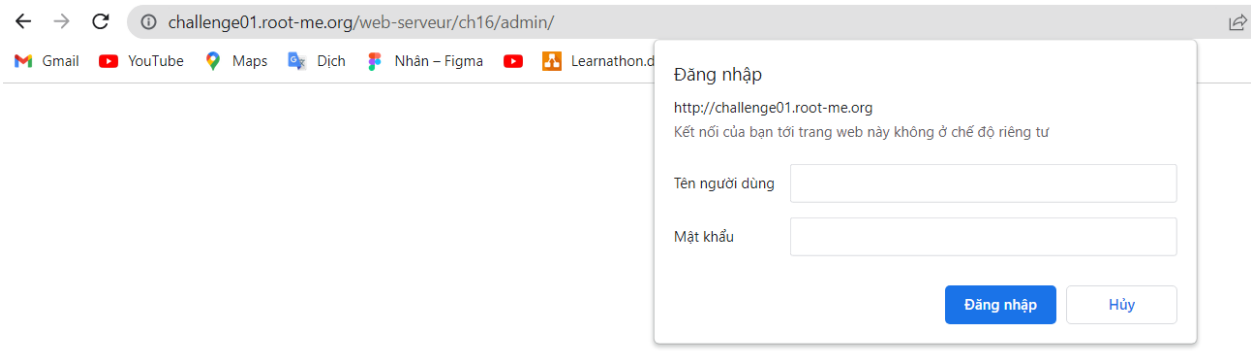
- Truy cập vào challenge ta thấy được trang web như bên dưới



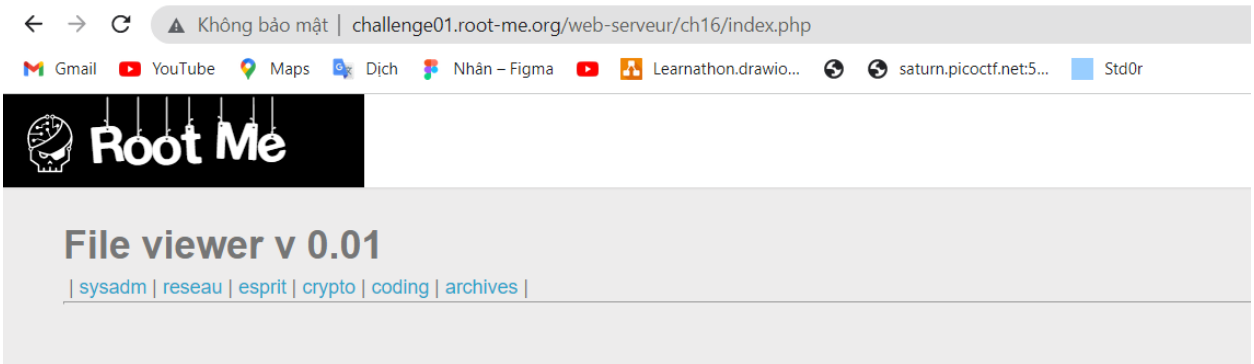
- Gồm các tab là sysadm, reseau, esprit, crypto, coding, archivers, admin
- Ở các tab này chỉ chứa các file. Ví dụ tab sysadm có file index.html



- Riêng ở tab admin thì bắt ta xác thực người dùng



- Thử truy cập vào link http://challenge01.root-me.org/web-serveur/ch16/index.php ta thấy trả về cùng kết quả với trang http://challenge01.root-me.org/web-serveur/ch16/ do đó ta biết được file index.php tồn tại

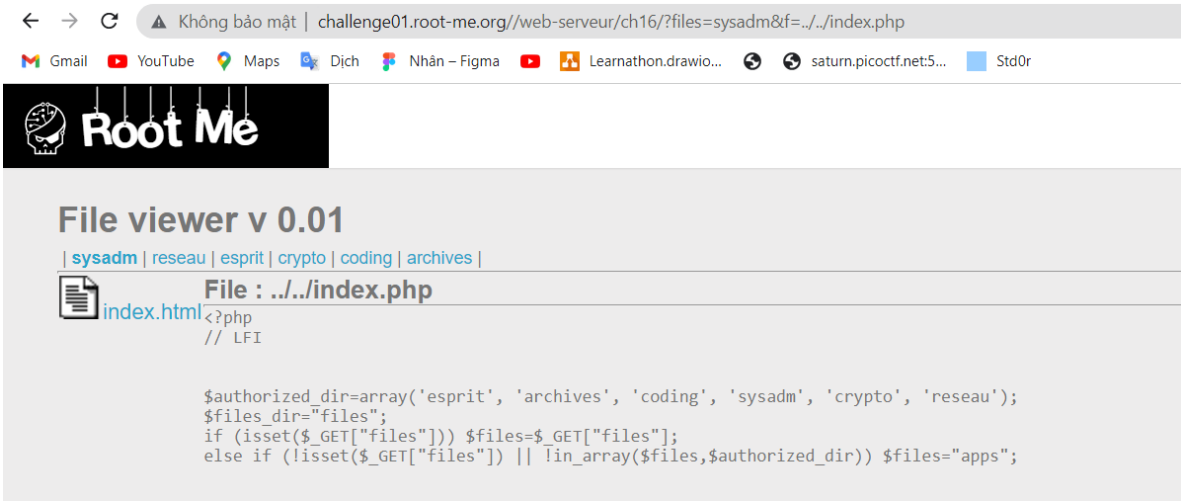


- Thử truy cập vào file index.html ở tab sysadm

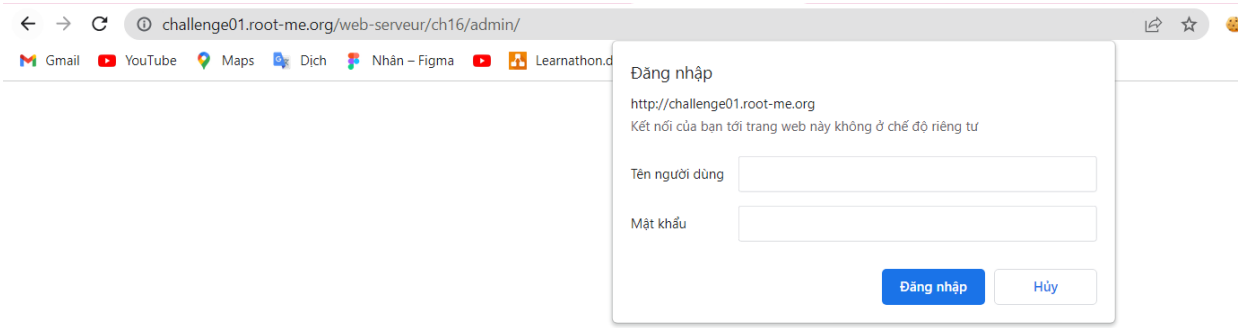

Không bảo mật | challenge01.root-me.org/web-serveur/ch16/index.php?files=sysadm&f=index.html
Gmail YouTube Maps Dịch Nhân – Figma Learnathon.drawio... saturn.picoctf.net:5... Std0r
Root Me
File viewer v 0.01
| sysadm | reseau | esprit | crypto | coding | archives |
index.html
File : index.html
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /sysadm</title>
</head>
<body>
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
<link REL="SHORTCUT ICON" HREF="/favicon.ico">

- Dựa vào url ta biết được biến files để chỉ đến thư mycj sysadm và biến f để mở file index.html
- Thử kiểm tra xem có tồn tại lỗ hổng local file inclusion không bằng cách thêm ./ vào trước index.html trên url

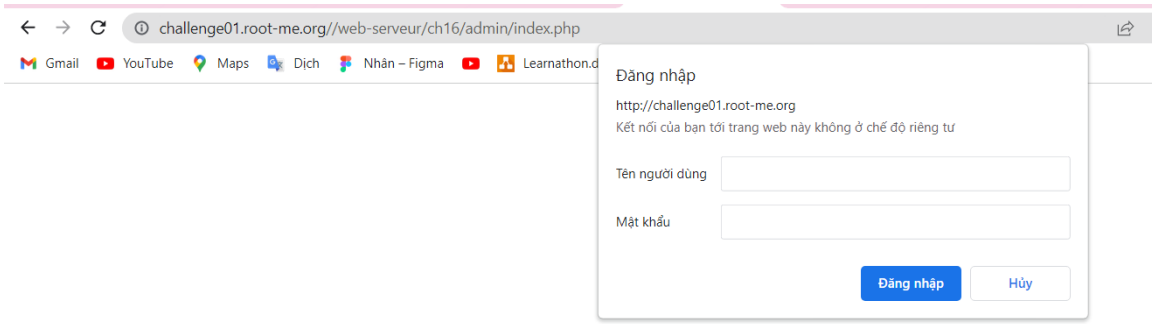
- Ta thấy kết quả trả về giống với trước khi không thêm ./ do đó ở đây có lỗ hổng local file inclusion
- Thực hiện tìm kiếm file **index.php** theo cú pháp files= &f=



- Ta biết được đường dẫn của nó là http://challenge01.root-me.org//web-serveur/ch16/?files=sysadm&f=../../index.php
- Mục tiêu của ta là lấy section của admin, ta truy cập vào trang admin và ta thấy url khi truy cập vào admin là http://challenge01.root-me.org//web-serveur/ch16/admin/

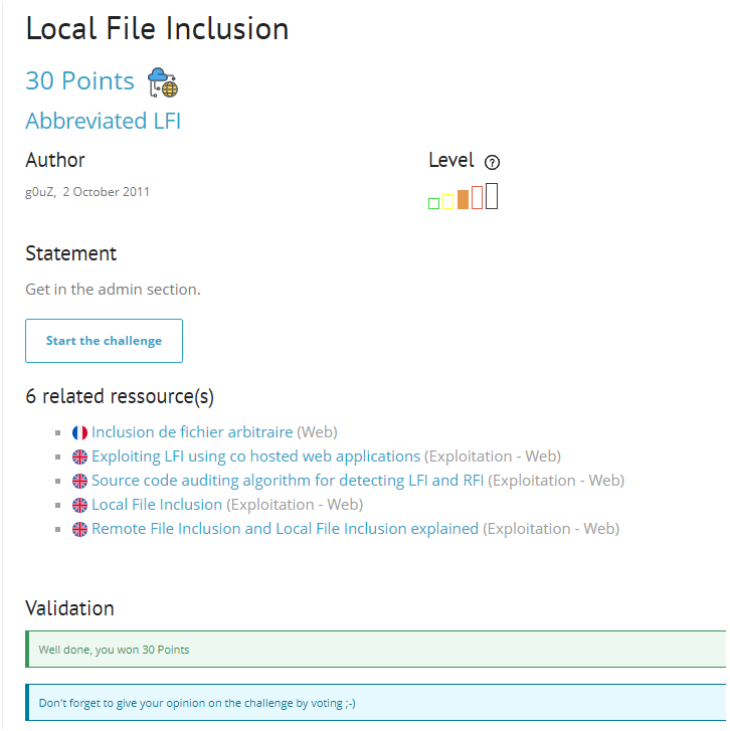


- Truy cập với url sau http://challenge01.root-me.org//web-serveur/ch16/admin/index.php ta thấy cùng một kết quả trả về



- Do đó ta biết file **admin/index.php** tồn tại
- Tìm kiếm và ta biết được file này nằm tại http://challenge01.root-me.org/web-serveur/ch16/?files=sysadm&f=../../admin/index.php

- Ở đây ta tìm được section của admin là OpbNJ60xYpvAQU8
- Nộp kết quả này ta vượt qua thử thách thành công



FLAG: OpbNJ60xYpvAQU8