

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

Local File Inclusion

30 Points 

Abbreviated LFI

Author

g0uZ, 2 October 2011

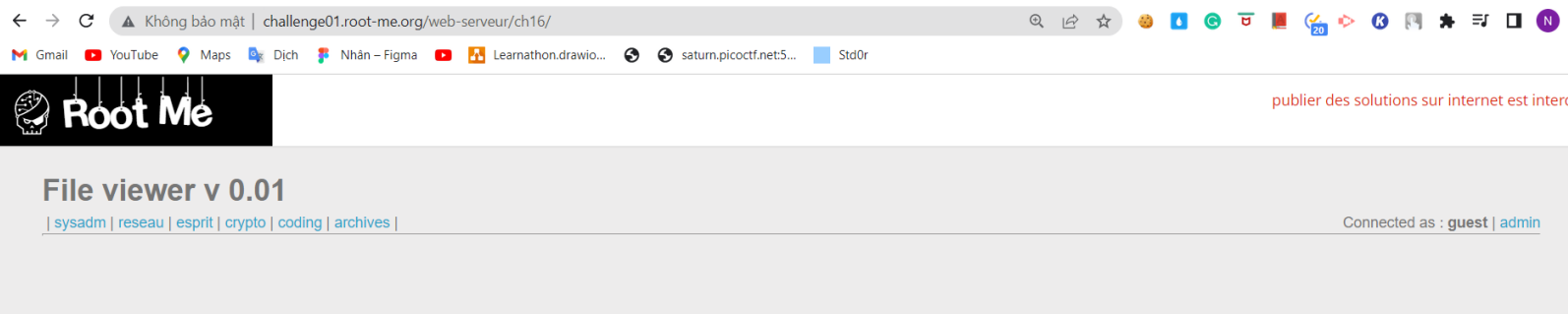
Level 



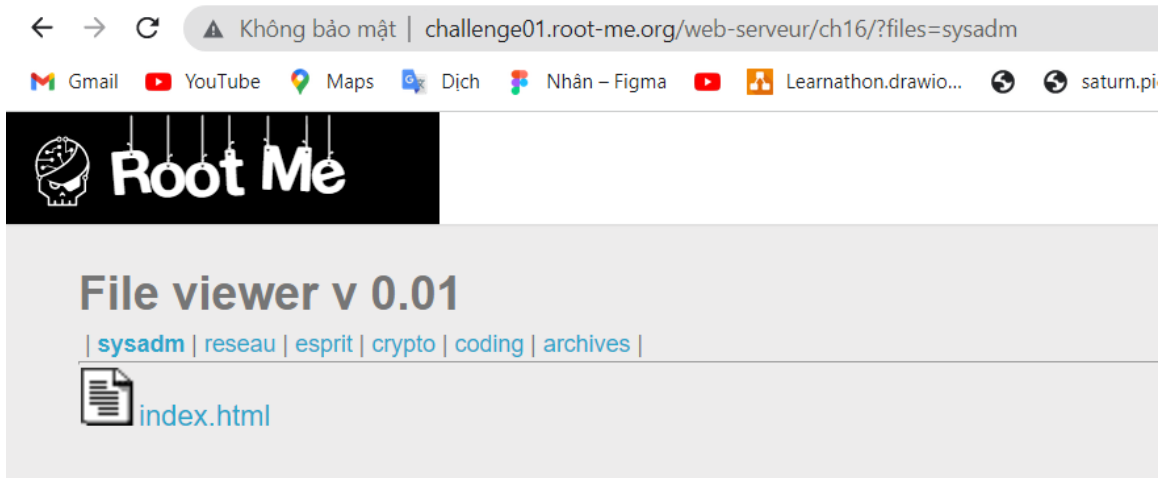
Statement

Get in the admin section.

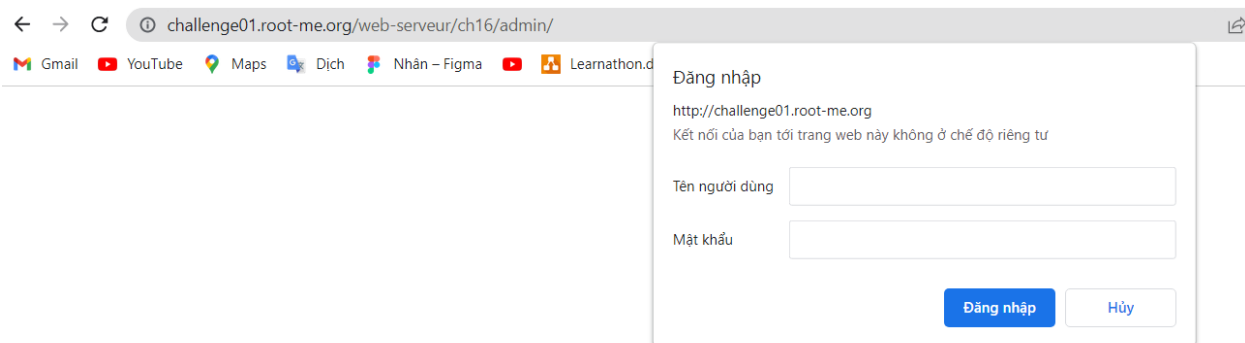
- Truy cập vào challenge ta thấy được trang web như bên dưới



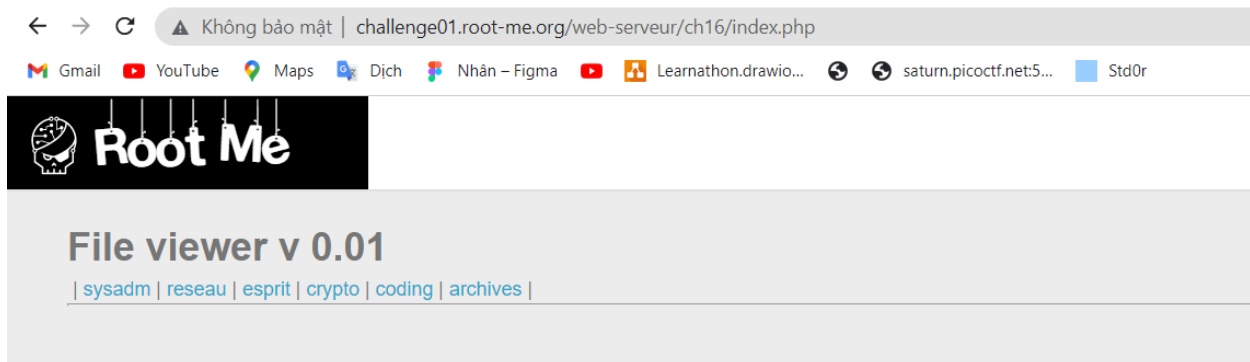
- Gồm các tab là sysadm, reseau, esprit, crypto, coding, archivers, admin
- Ở các tab này chỉ chứa các file. Ví dụ tab sysadm có file index.html



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



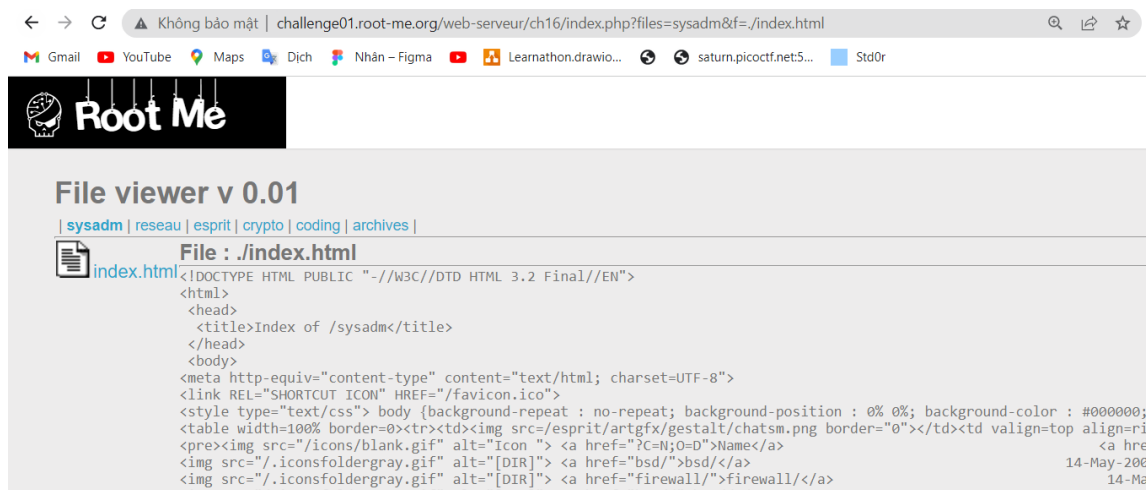
- Thử truy cập vào link <http://challenge01.root-me.org/web-serveur/ch16/index.php> ta thấy trả về cùng kết quả với trang <http://challenge01.root-me.org/web-serveur/ch16/> do đó ta biết được file index.php tồn tại



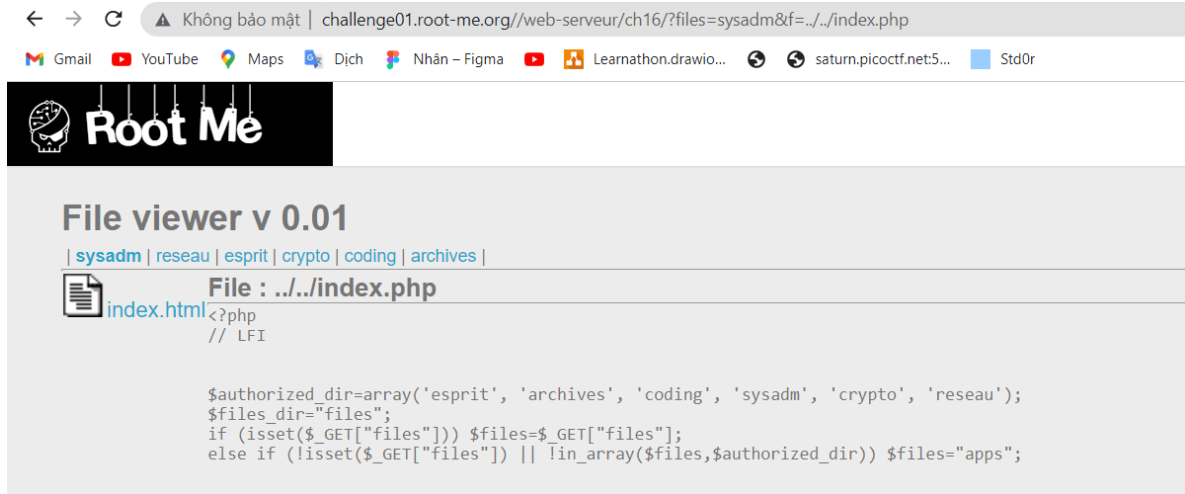
- Thử truy cập vào file index.html ở tab sysadm



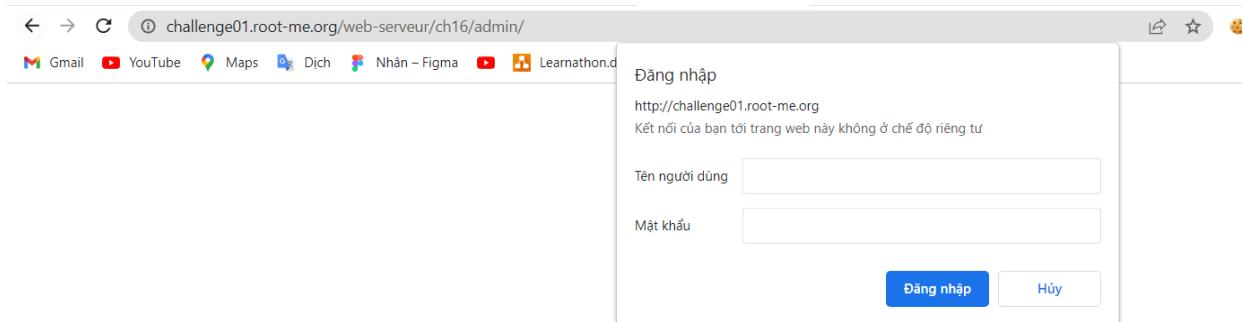
- Dựa vào url ta biết được biến files để chỉ đến thư mục sysadm và biến f để mở file index.html
- Thử kiểm tra xem có tồn tại lỗ hổng local file inclusion không bằng cách thêm ./ vào trước index.html trên url



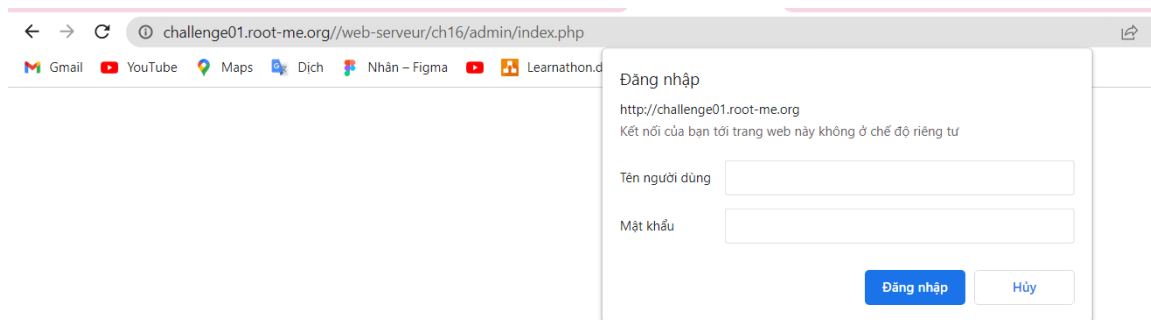
- Ta thấy kết quả trả về giống với trước khi không thêm ./ do đó ở đây có lỗ hổng local file inclusion
- Thực hiện tìm kiếm file **index.php** theo cú pháp files= &f=



- 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>

```

foreach ($matches as $m) {
    $data[$m[1]] = $m[3] ? $m[3] : $m[4];
    unset($needed_parts[$m[1]]);
}

return $needed_parts ? false : $data;
}

function auth($realm){
    header('HTTP/1.1 401 Unauthorized');
    header('WWW-Authenticate: Digest realm="'.$realm.'",qop="auth",nonce="'.uniqid().'",opaque="'.md5($realm).'"');
    die($realm);
}

$realm = 'PHP Restricted area';
$users = array('admin' => 'OpbNJ60xYpvAQU8');

```

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

Local File Inclusion

30 Points 🌐

Abbreviated LFI

Author

g0uZ, 2 October 2011

Level ①

🟢🟡🟠🔴

Statement

Get in the admin section.

[Start the challenge](#)

6 related ressource(s)

- 🇫🇷 Inclusion de fichier arbitraire (Web)
- 🇺🇸 Exploiting LFI using co hosted web applications (Exploitation - Web)
- 🇺🇸 Source code auditing algorithm for detecting LFI and RFI (Exploitation - Web)
- 🇺🇸 Local File Inclusion (Exploitation - Web)
- 🇺🇸 Remote File Inclusion and Local File Inclusion explained (Exploitation - Web)

Validation

Well done, you won 30 Points

Don't forget to give your opinion on the challenge by voting :)

FLAG: OpbNJ60xYpvAQU8