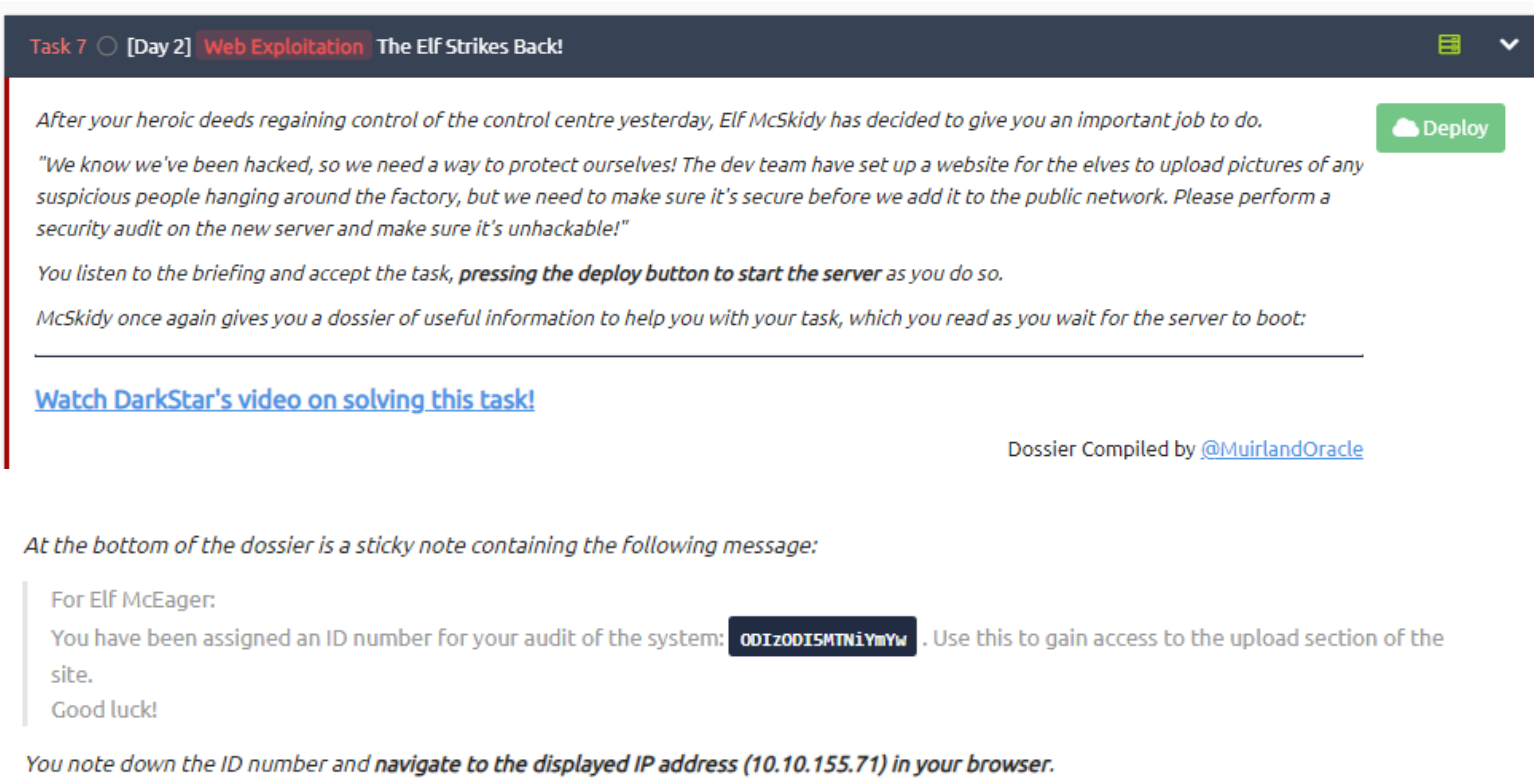
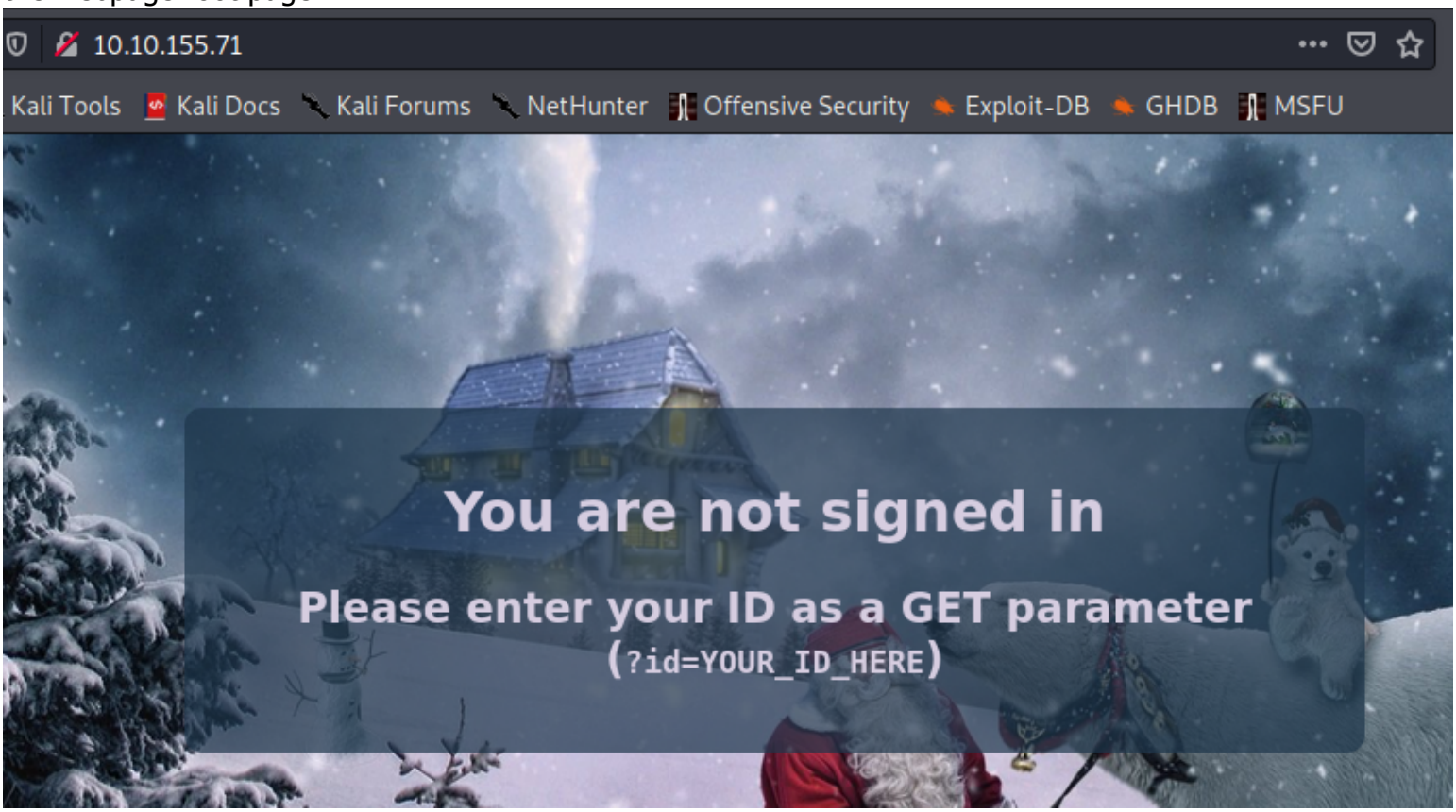
Day 2 - The Elf Strikes Back!

Scenario



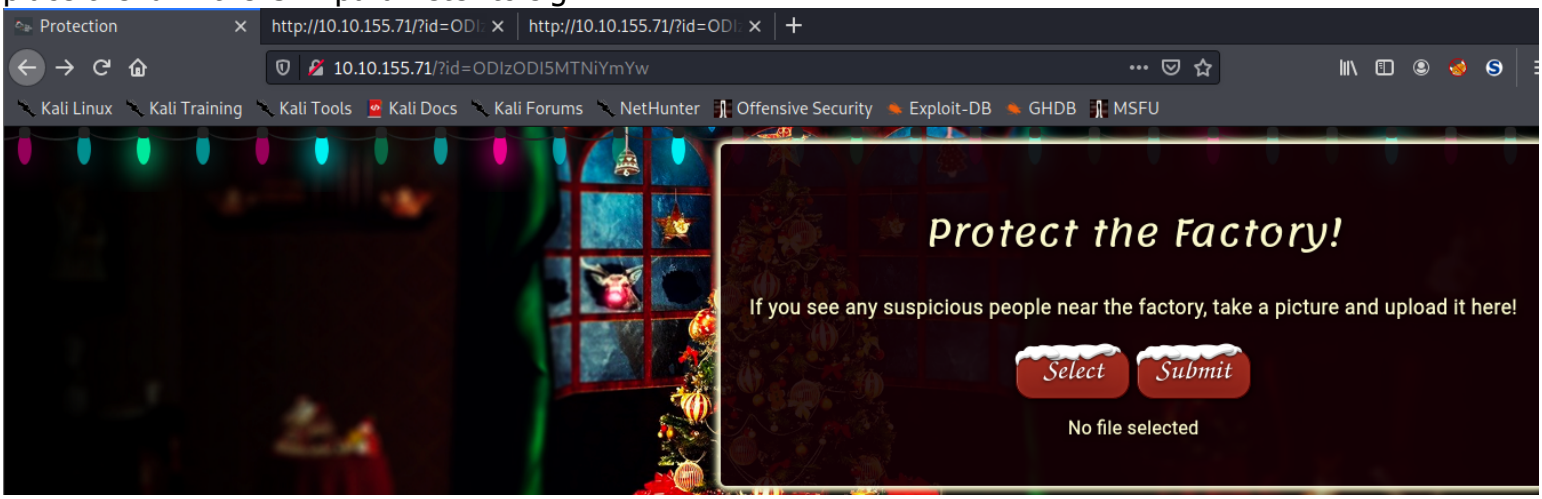
the webpage root page



the id

he system: ODIzODI5MTNiYmYw . Use

place the id in the GET parameter to sign in

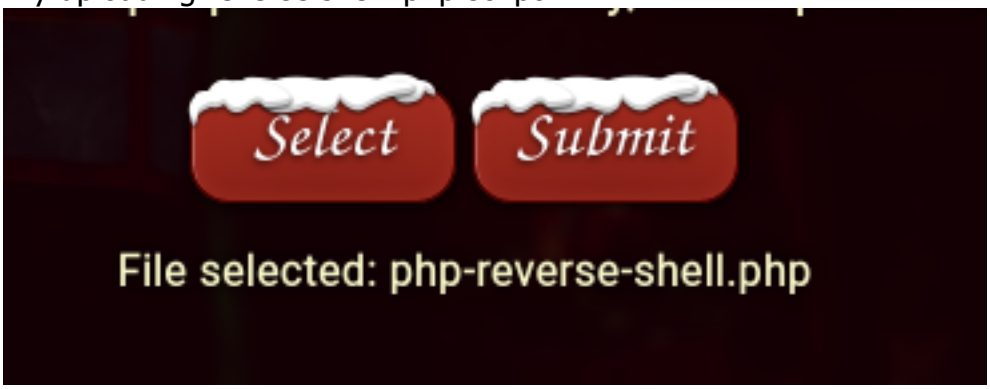


Question: What string of text needs added to the URL to get access to the upload page?
-?id=ODIzODI5MTNiYmYw

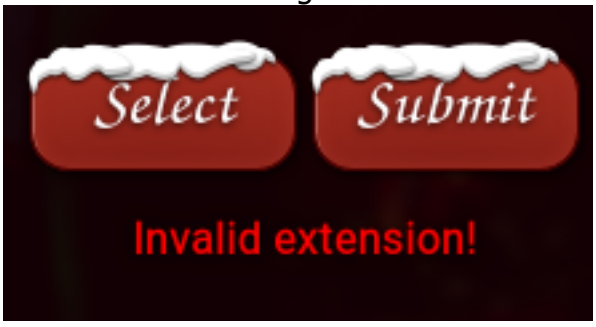
Question: What type of file is accepted by the site?
-image

edit the reverse shell php script to my ip

Try uploading reverse shell .php script



it shows error message



check the source code & found the extension that accepted only

```
<input type=file id="chooseFile" accept=".jpeg,.jpg,.png">
```

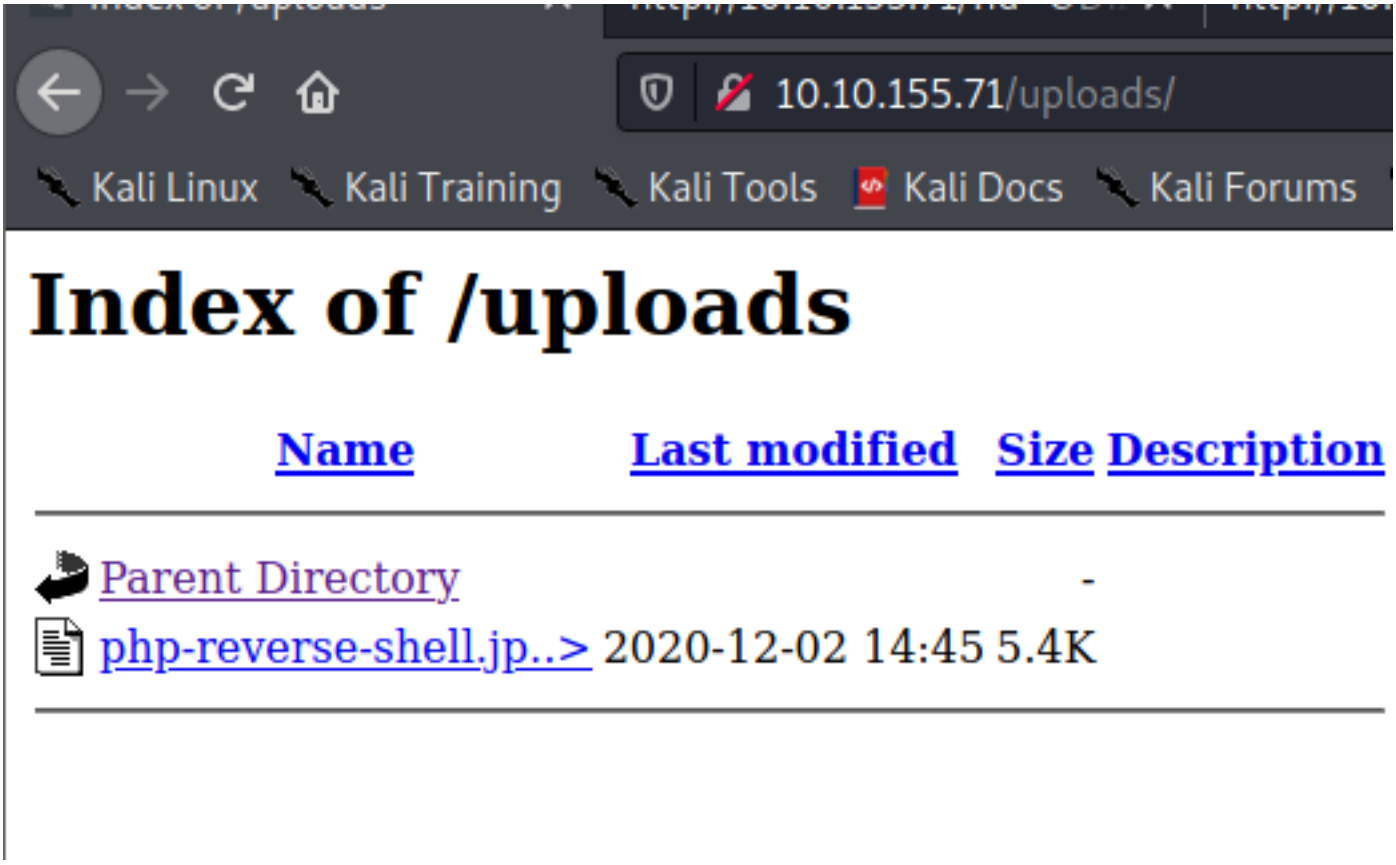
edit the filename including .jpeg in front of .php

```
┌──(nobodyatall㉿0×DEADBEEF)-[~]
└─$ mv php-reverse-shell.php php-reverse-shell.jpeg.php
```

select the reverse shell script & upload it

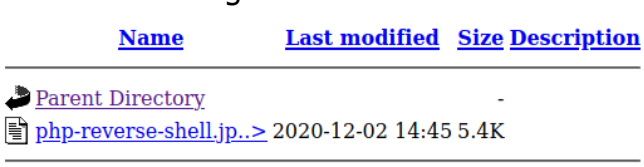
& we've bypass the filter

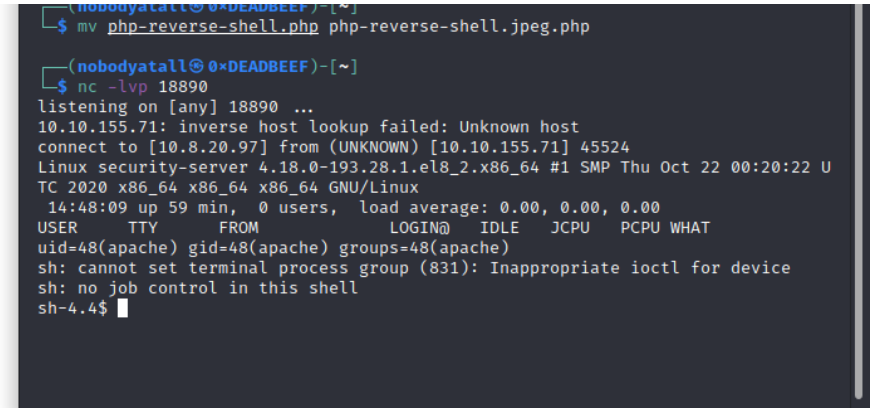
check the availability of /uploads directory as this might be the correct directory they store the reverse shell script
//& we've found our php script & the /upload directory was available



Question: In which directory are the uploaded files stored?
-/uploads/

execute it & we got our initial shell





Question: What is the flag in `/var/www/flag.txt`?

```
sh-4.4$ cat /var/www/flag.txt
cat /var/www/flag.txt
Gateway Timeout

The gateway did not receive a timely response from the upstream server or appl
You've reached the end of the Advent of Cyber, Day 2 -- hopefully you're enjoyi
ng yourself so far, and are learning lots!
This is all from me, so I'm going to take the chance to thank the awesome @Varg
naar for his invaluable design lessons, without which the theming of the past t
wo websites simply would not be the same.


Have a flag -- you deserve it!
THM{MGU3Y2UyMGUwNjExYTY4NTAxOWJhMzhh}


Good luck on your mission (and maybe I'll see y'all again on Christmas Eve)!
 --Muiri (@MuirlandOracle)
```