Pentesting
Herr Münch

Thomas Dauner
23.11.2022

Writeup: M and Ms Container

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

run dirb on 172.17.0.2

found /flag

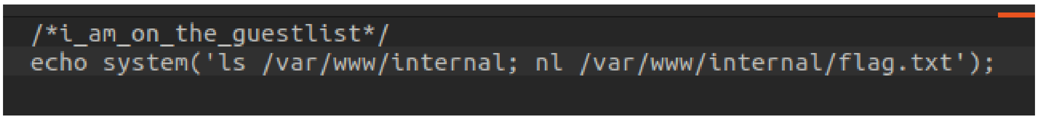
when access flag found

flag: flag_s0_many_c0lors

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

I found the “callmemaybe.php”. This php files take a “number” parameter. The “number” parameter is used in a php command to open a file. If the file contains a text with “/*i_am_on_the_guestlist*/” the file gets executed as php code (which we can use to do remote code execution on the webservers host system and extract the flags).

I created a file called “execute.php” with /*i_am_on_the_guestlist*/ in it and a php command which executes a command on the system shell and prints it output.



```
/*i_am_on_the_guestlist*/
echo system('ls /var/www/internal; nl /var/www/internal/flag.txt');
```

Figure 1: Example of my "execute.php" file

Then I hosted a local webserver on my system and passed the URL of the file on my webserver to the "number" parameter of the “callmemaybe.php”. On this way I got remote code execution. I executed "ls /" through the “execute.php” on the “callmemaybe.php” on the webserver. Then I found the file of the flag. I read the flag with nl FILENAME.

Flag: flag_th0s3_ar3_my_m-and-ms

- 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?

I did it like in the second task but accessed the flag in the /var/www/public directory.

Flag: flag_1nt3ernal_fl4g_m-and-ms