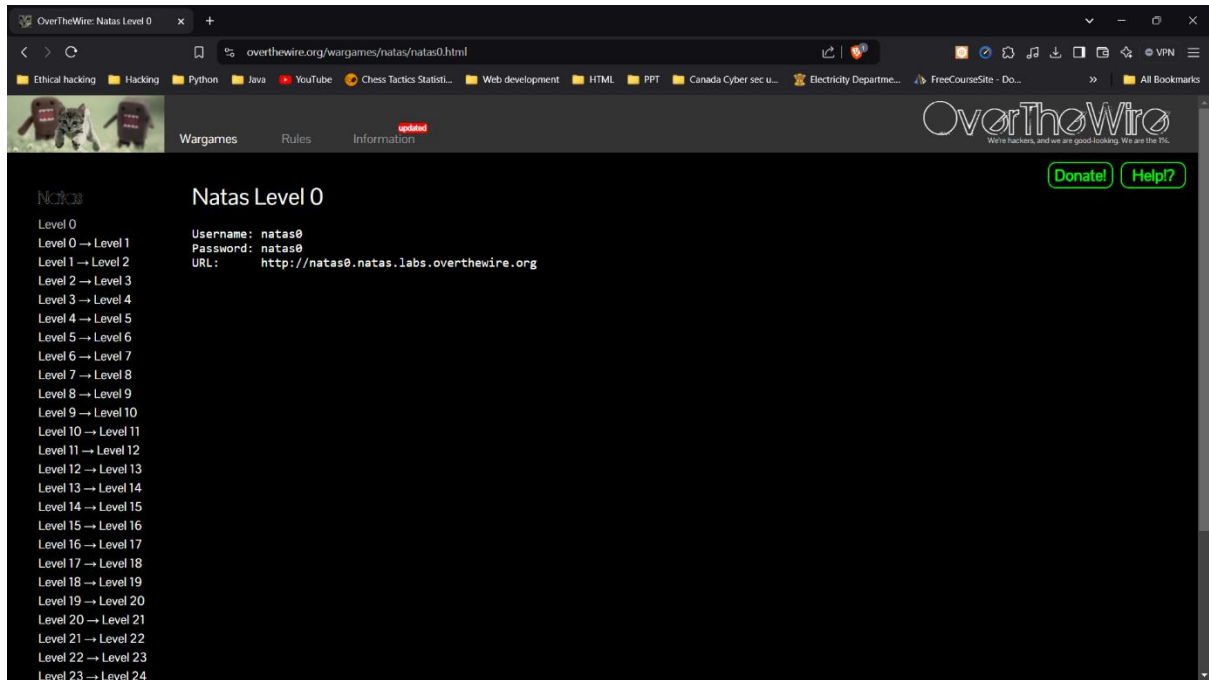


NATAS REPORT (LEVEL 1 – 10)

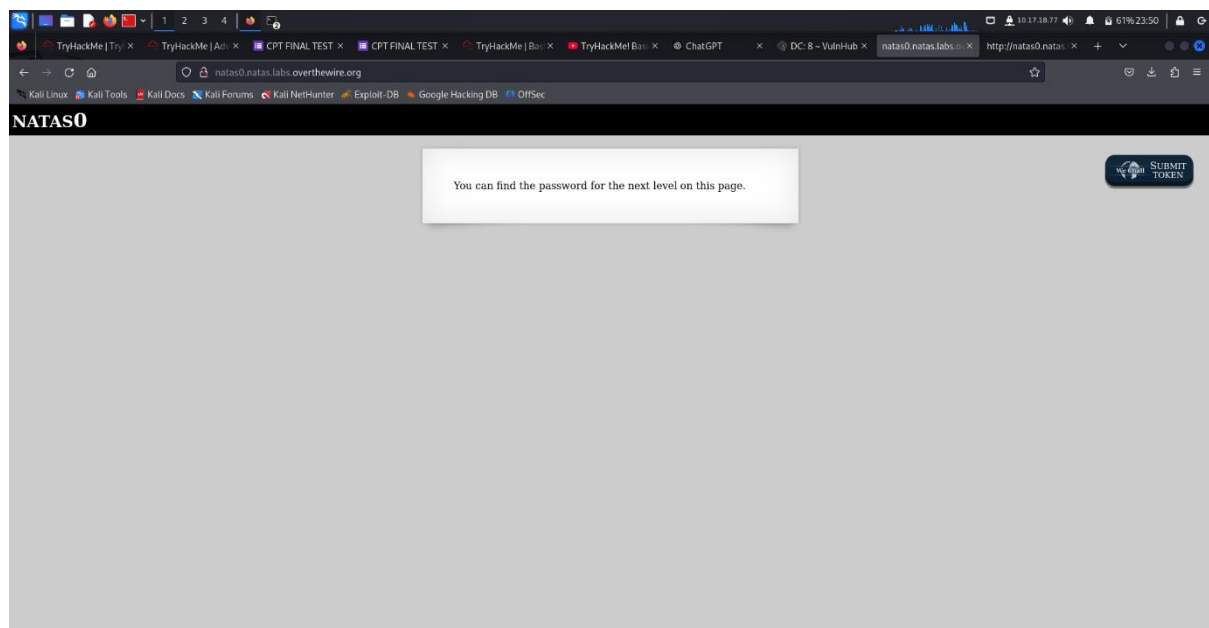
NATAS 0:



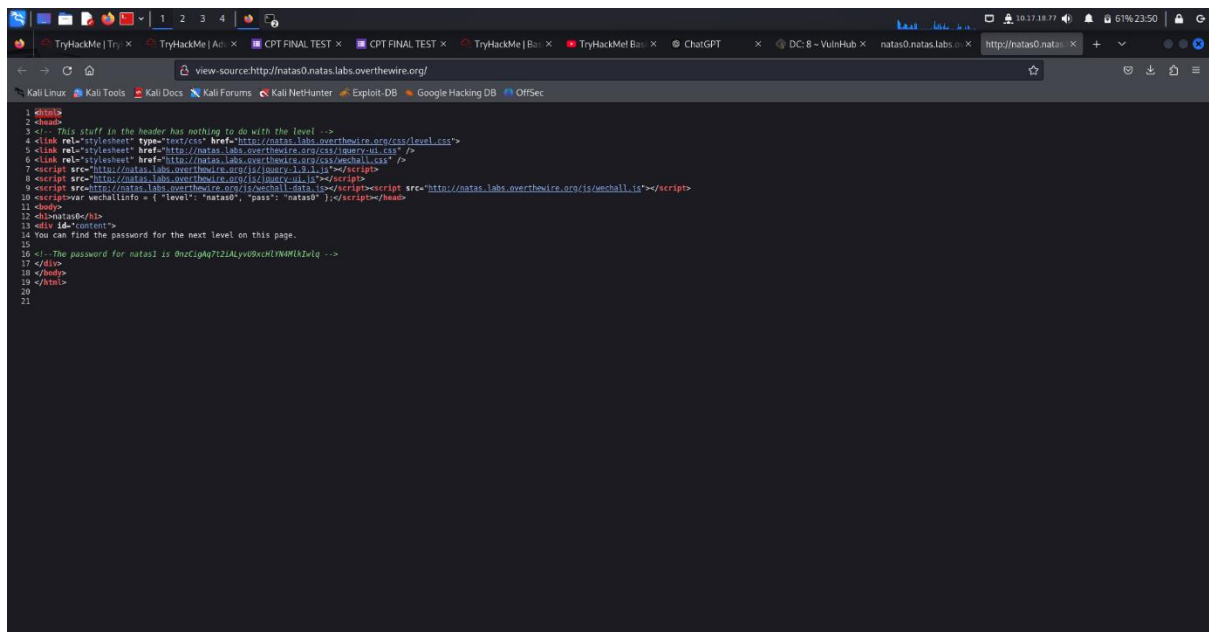
From the above introductory page we can get the user credentials for the user natas0 using it login to the site <http://natas0.natas.labs.overthewire.org>

Username: **natas0**

Password: **natas0**



After logging in we can find this dashboard. Right click here and view the source code



```
1 <html>
2 <head>
3 <!-- This stuff in the header has nothing to do with the level -->
4 <link rel="stylesheet" type="text/css" href="https://natas.labs.overthewire.org/css/level.css">
5 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
6 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jqueryui.css" />
7 <script src="https://natas.labs.overthewire.org/js/jquery.js" /></script>
8 <script src="https://natas.labs.overthewire.org/js/jquery-ui.js" /></script>
9 <script src="https://natas.labs.overthewire.org/js/jquery.js" /></script><script src="http://natas.labs.overthewire.org/js/jquery.js" /></script>
10 <script>var wechallinfo = { "level": "natas0", "pass": "natas0" };</script></head>
11 <body>
12 <div>natas0</div>
13 <div id="content">
14 You can find the password for the next level on this page.
15
16 <!-- The password for natas1 is 0nzCigAq7t2iALyvU9xcHIYN4MlkIwlq -->
17 </div>
18 </body>
19 </html>
20
21
```

Here we can get the password for natas1

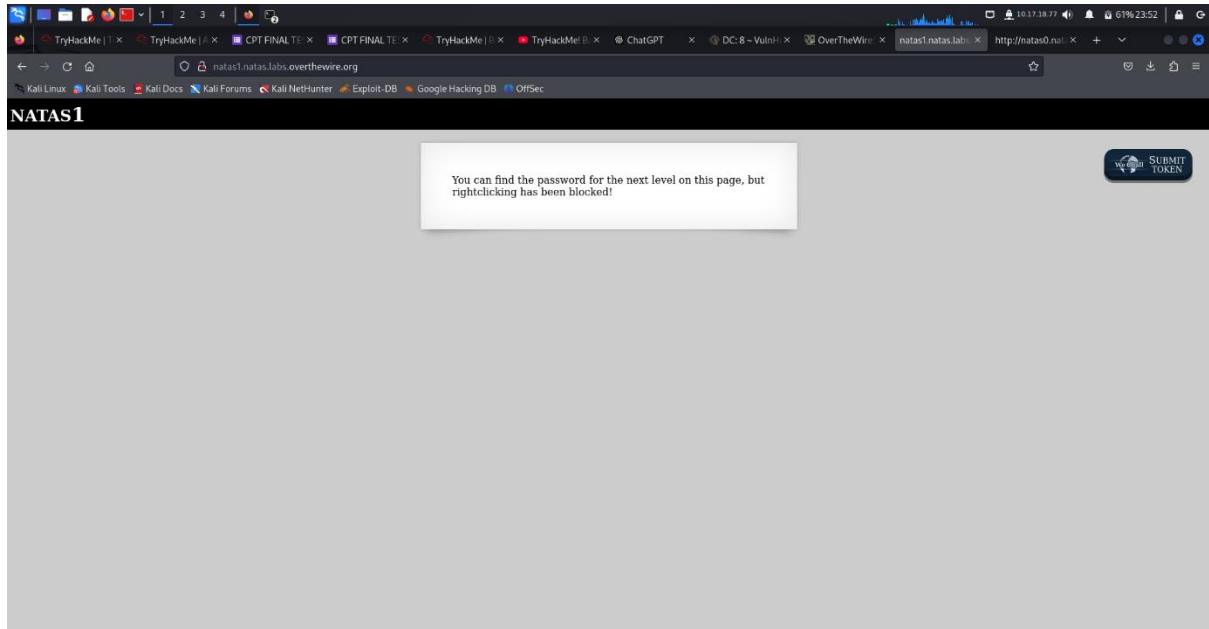
0nzCigAq7t2iALyvU9xcHIYN4MlkIwlq

NATAS 1:

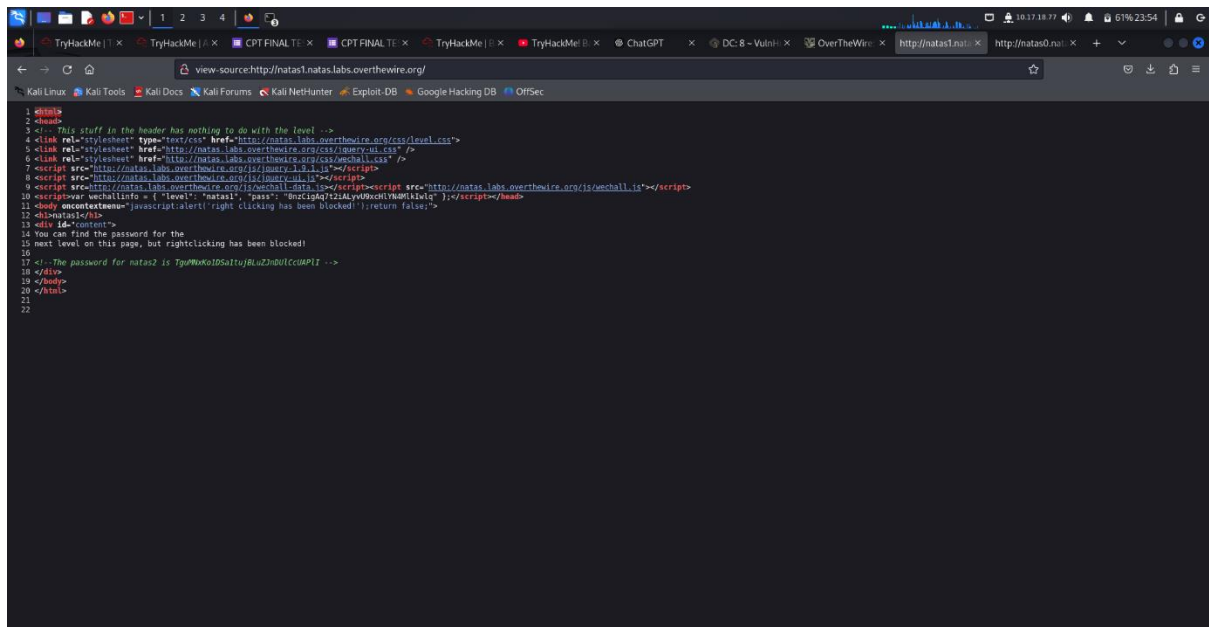
Username: **natas1**

Password: **0nzCigAq7t2iALyvU9xcHIYN4MlkIwlq**

Use this and login in to <http://natas1.natas.labs.overthewire.org>



Here as the right click option is disabled use shortcut Ctrl+U to view the source code and you can find the password for natas2



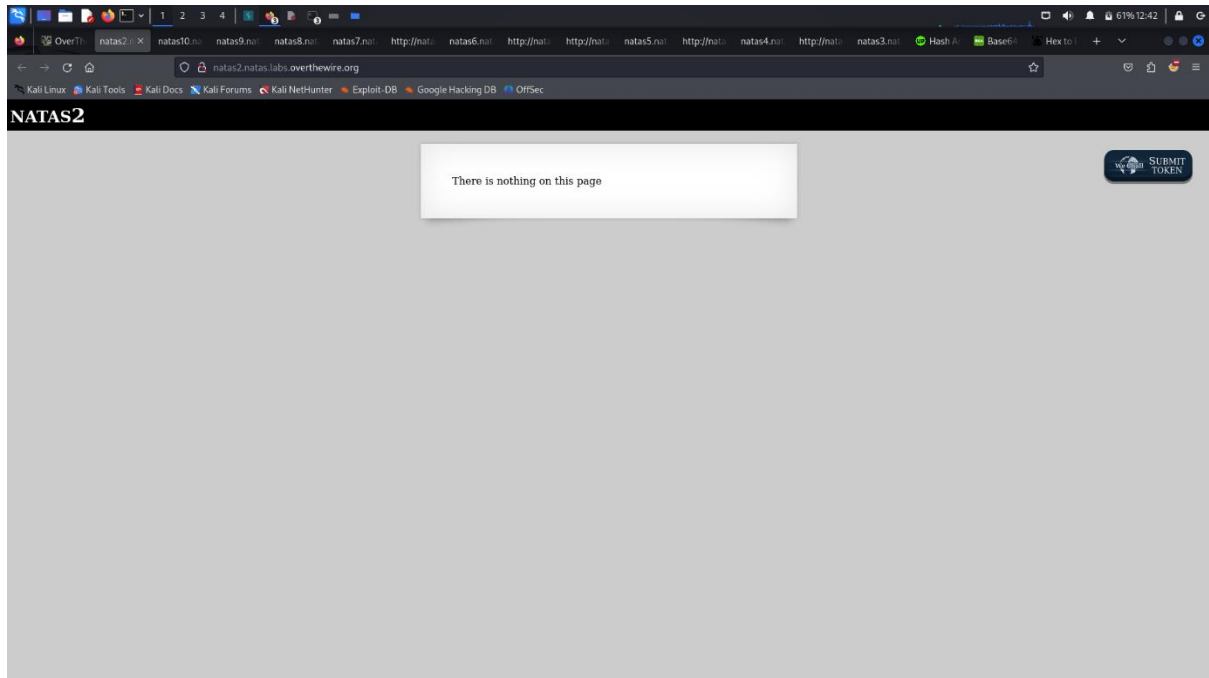
The password for natas2 is **TguMNxKo1DSa1tujBLuZJnDUICcUAPII**

NATAS 2:

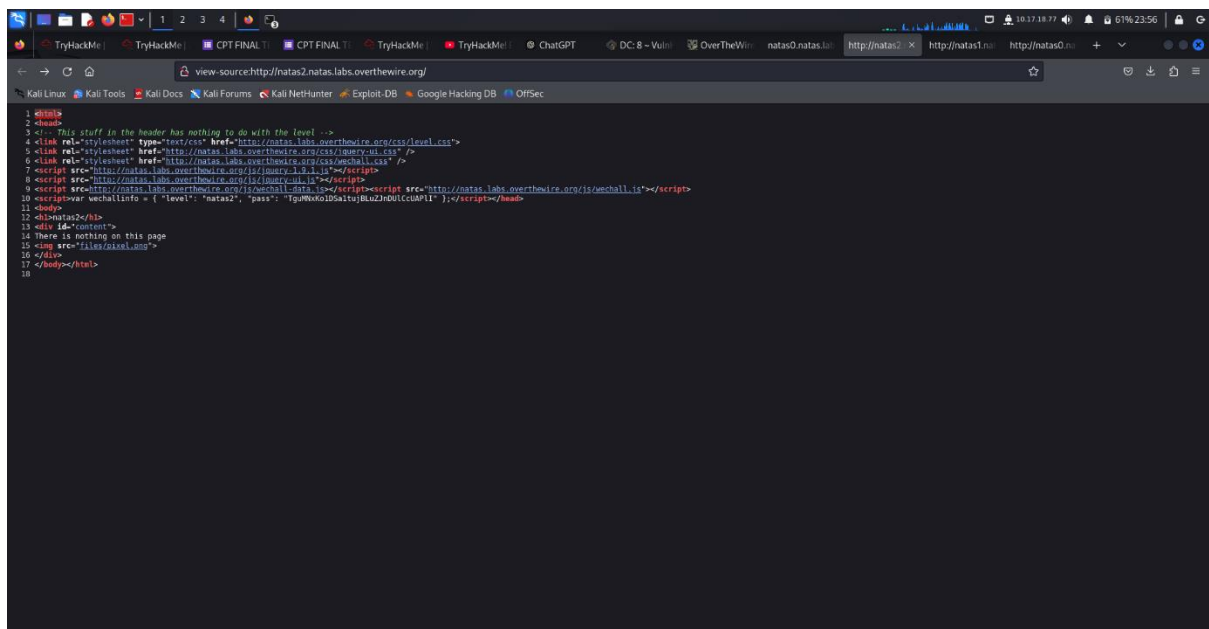
Username: **natas2**

Password: **TguMNxKo1DSa1tujBLuZJnDUICcUAPII**

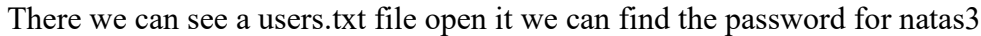
Use this and login to <http://natas2.natas.labs.overthewire.org>



Since there is nothing in this page go and view the source page



Here we can find a folder files so navigate to files

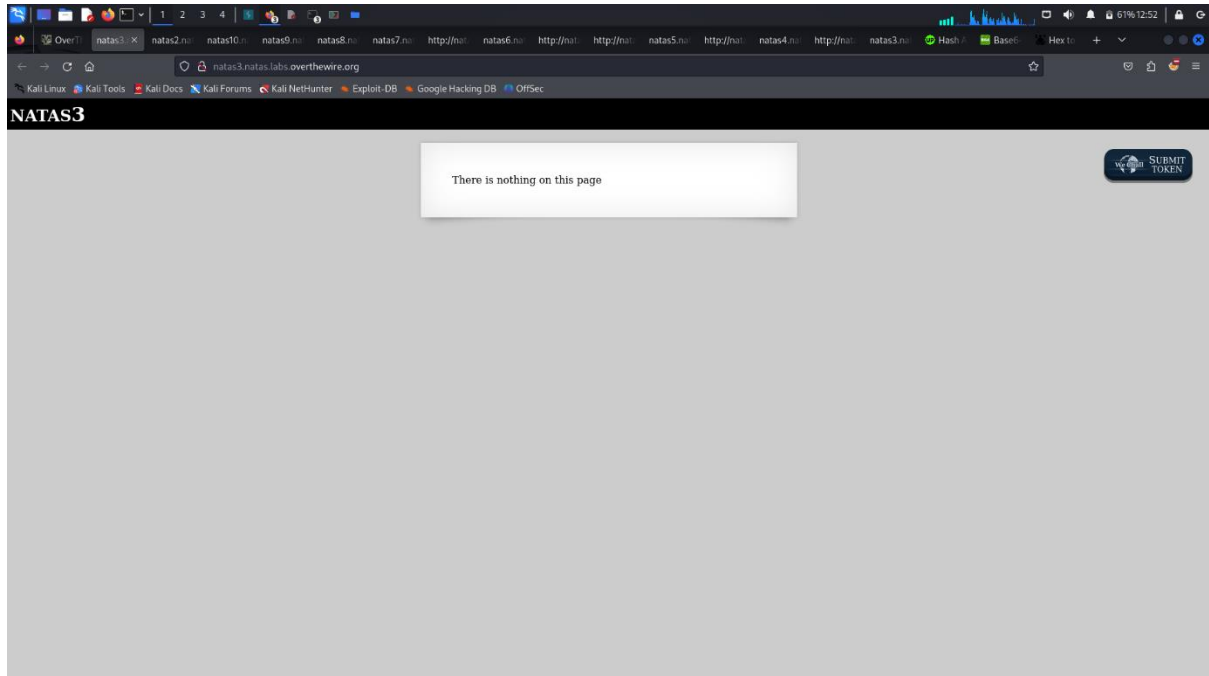


NATAS 3:

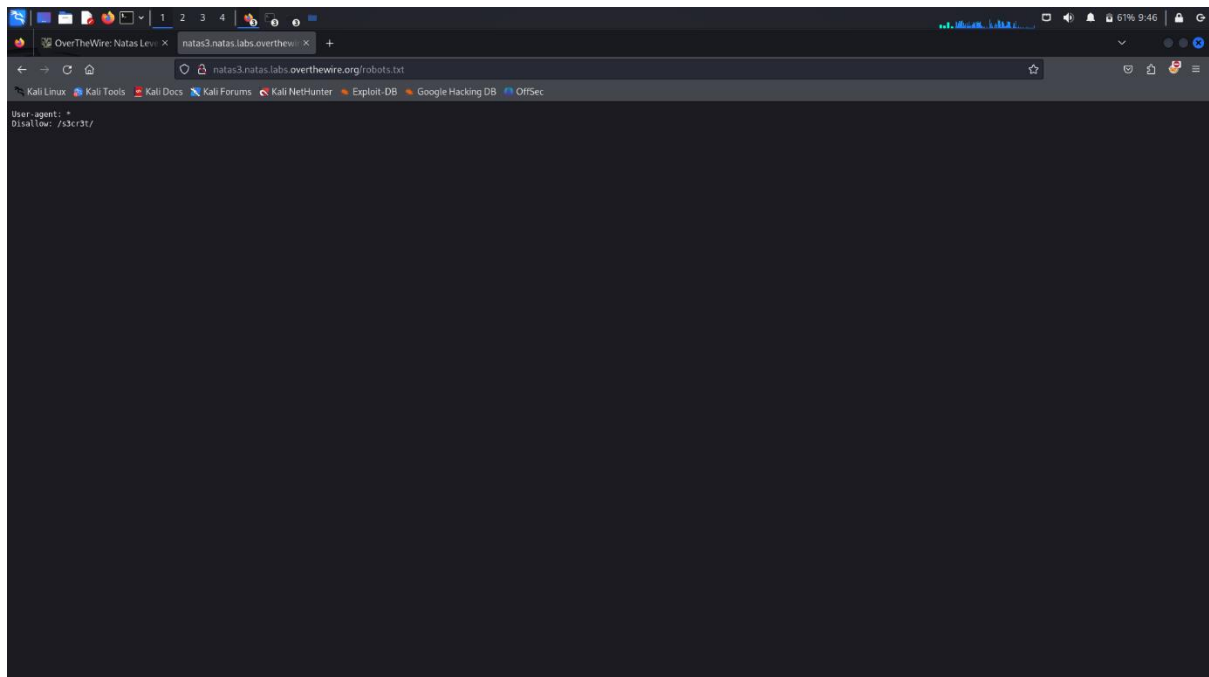
Username: **natas3**

Password: **3gqisGdR0pjm6tpkDKdIWO2hSvchLeYH**

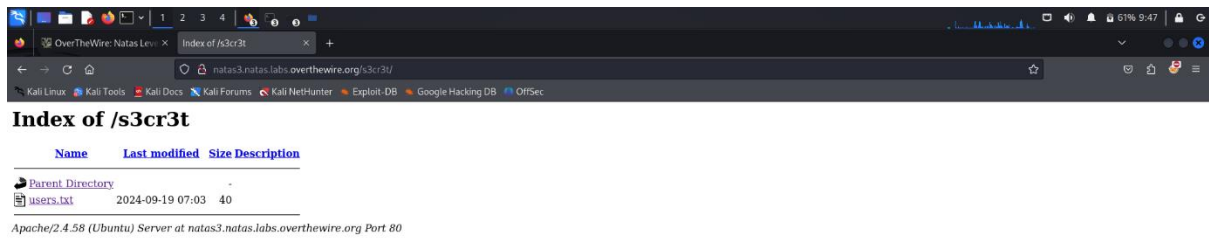
Using this login to <http://natas3.natas.labs.overthewire.org>



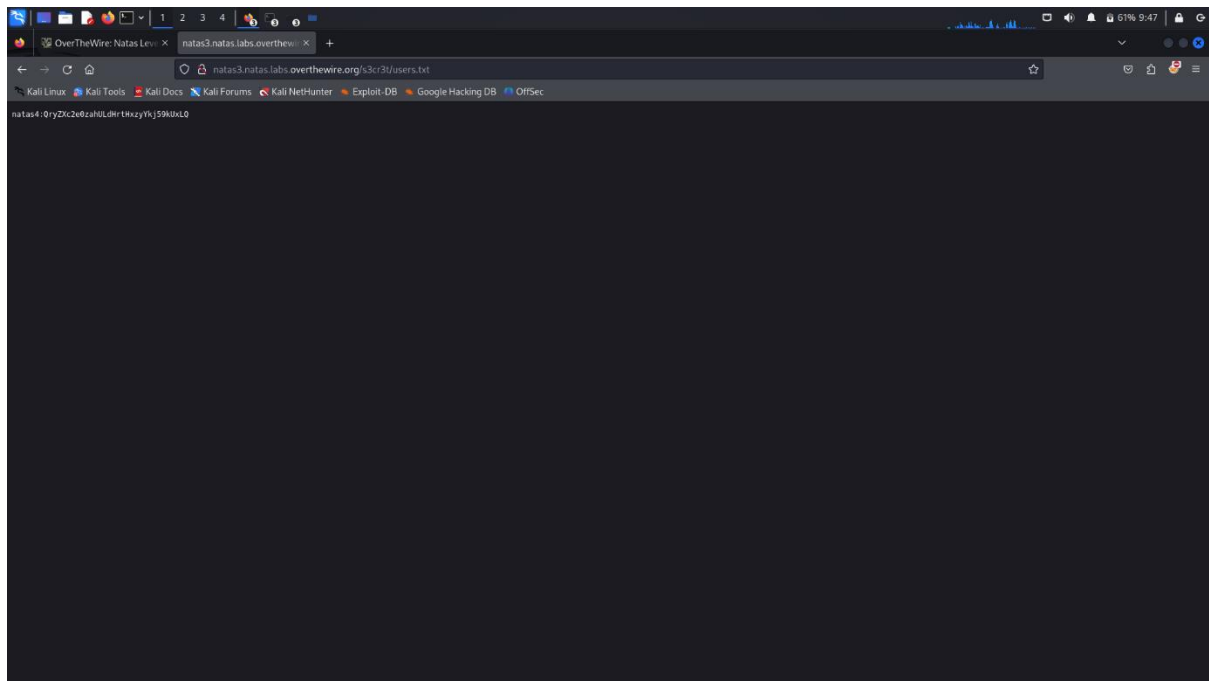
Here there is nothing so we'll look for something in the source page. Since there is nothing useful we can search for robots.txt file



We can see a hidden directory named s3cr3t and opening it we get



We can see a users.txt file and opening it we get password for natas4



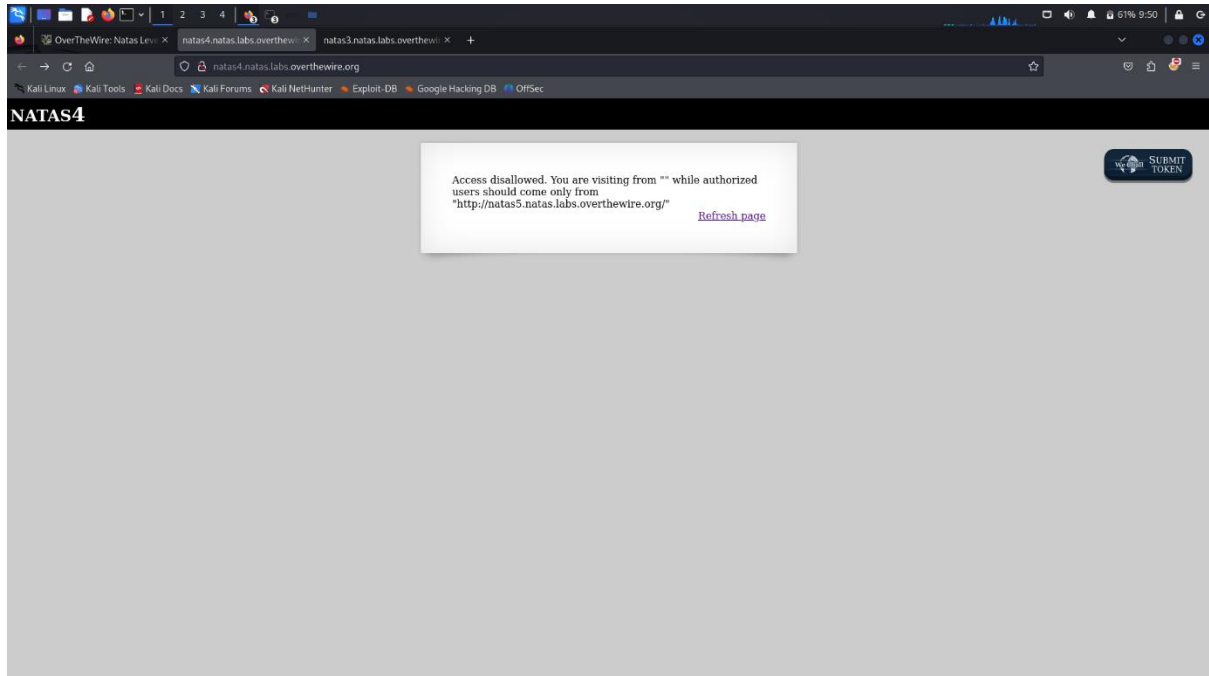
The password for natas4 is **QryZXc2e0zahULdHrtHxzyYkj59kUxLQ**

NATAS 4:

Username: **natas4**

Password: **QryZXc2e0zahULdHrtHxzyYkj59kUxLQ**

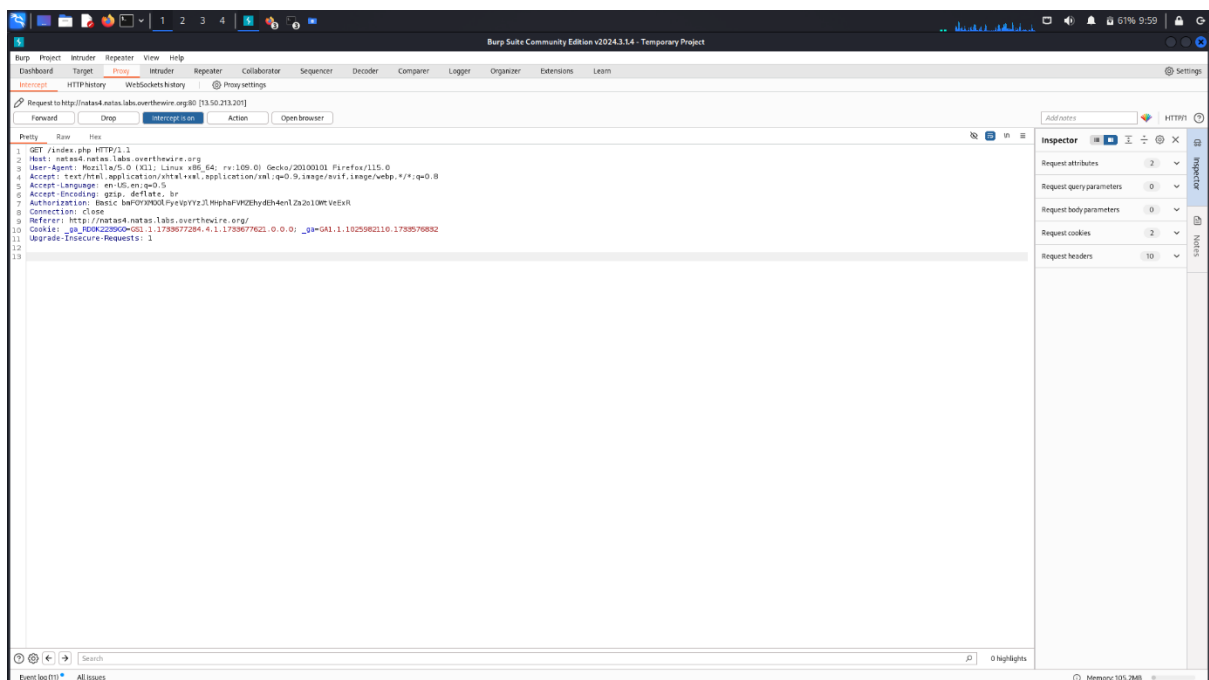
Use this and login to <http://natas4.natas.labs.overthewire.org>



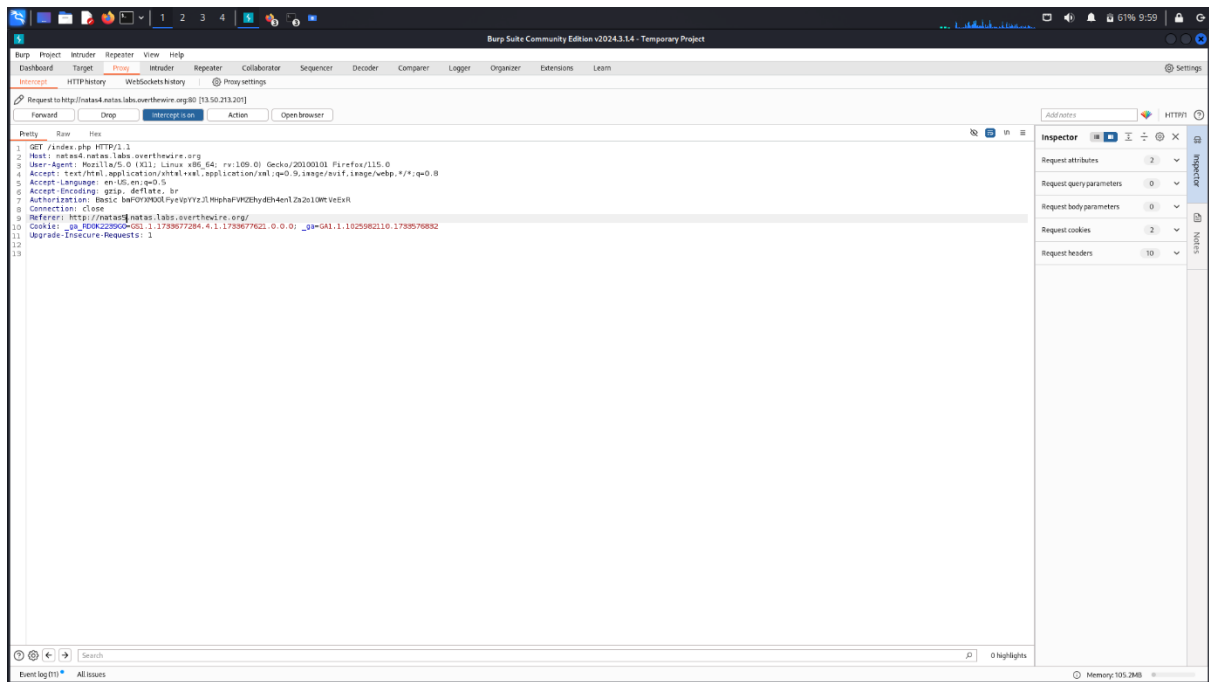
Here access is denied if the user didn't come from this link

<http://natas5.natas.labs.overthewire.org/>

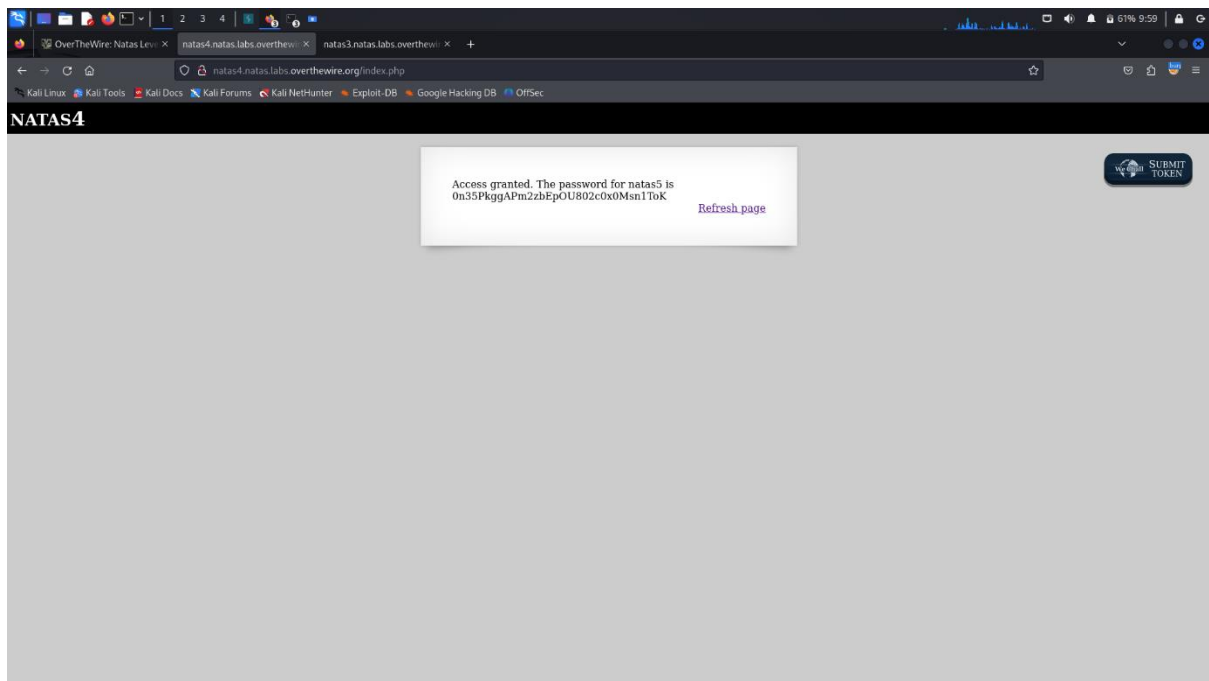
So we can use burpsuite for this to redirect the user to pass through this



Here we can find that the referer is from natas4 so just change it to natas5



After changing just forward it and refresh the page you will find password for natas5



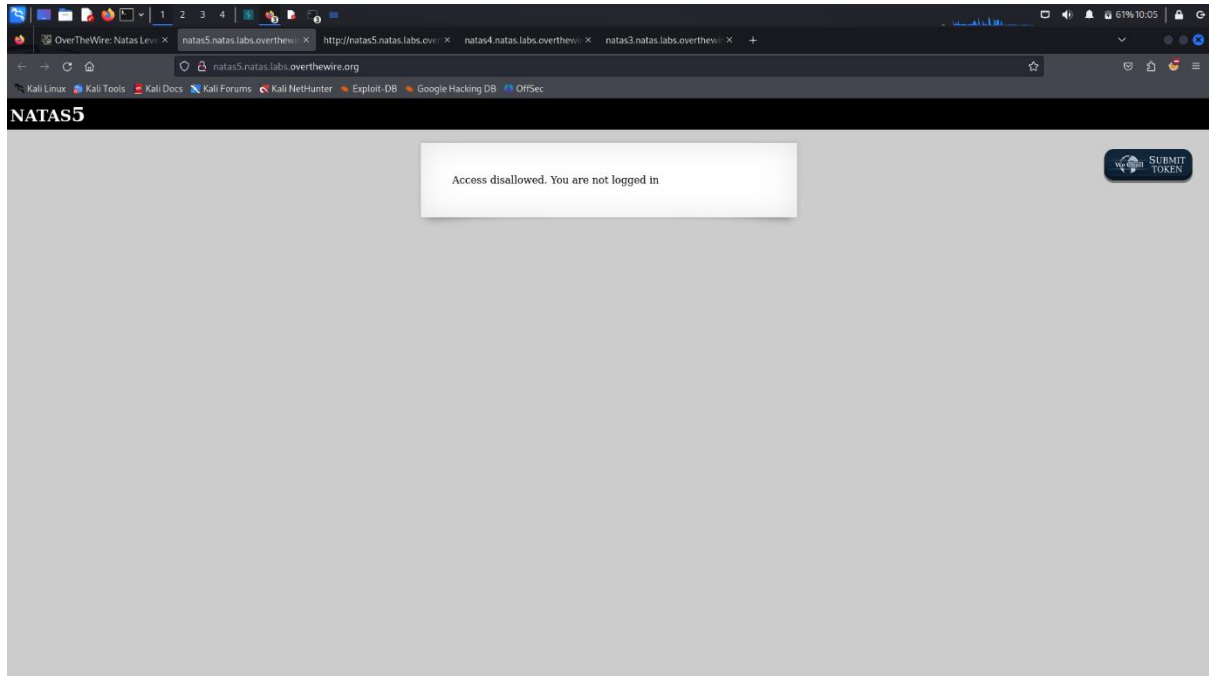
The password for natas5 is 0n35PkggAPm2zbEpOU802c0x0Msn1ToK

NATAS 5:

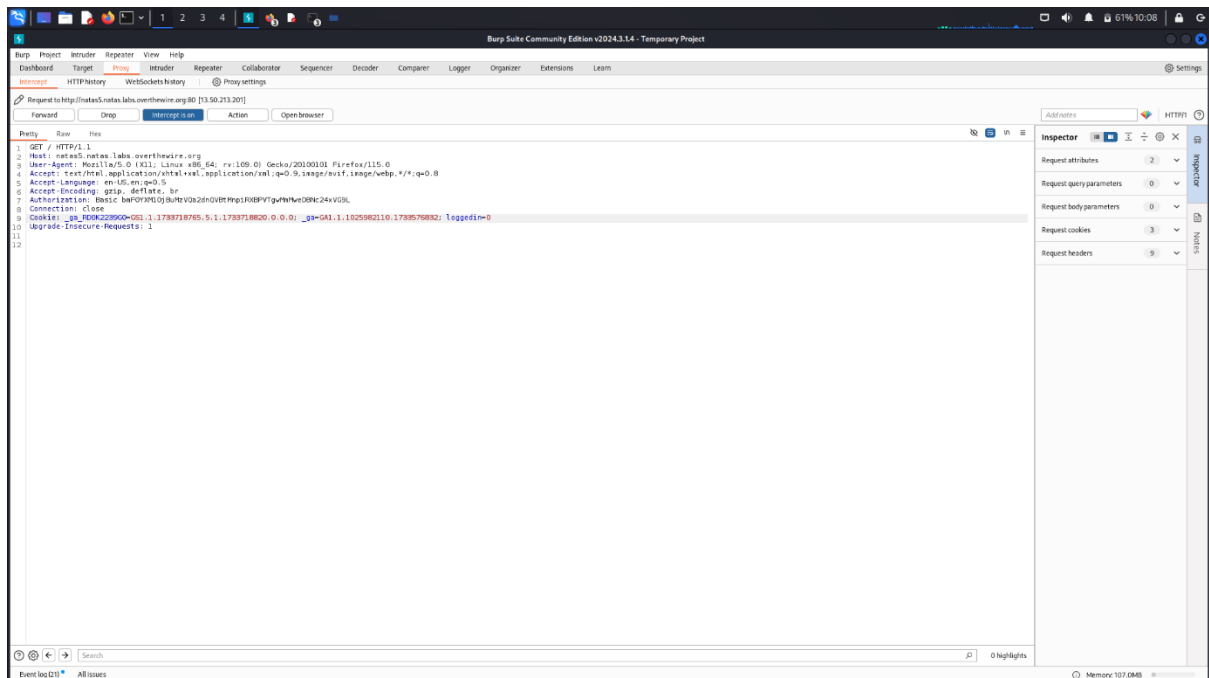
Username: **natas5**

Password: **0n35PkggAPm2zbEpOU802c0x0Msn1ToK**

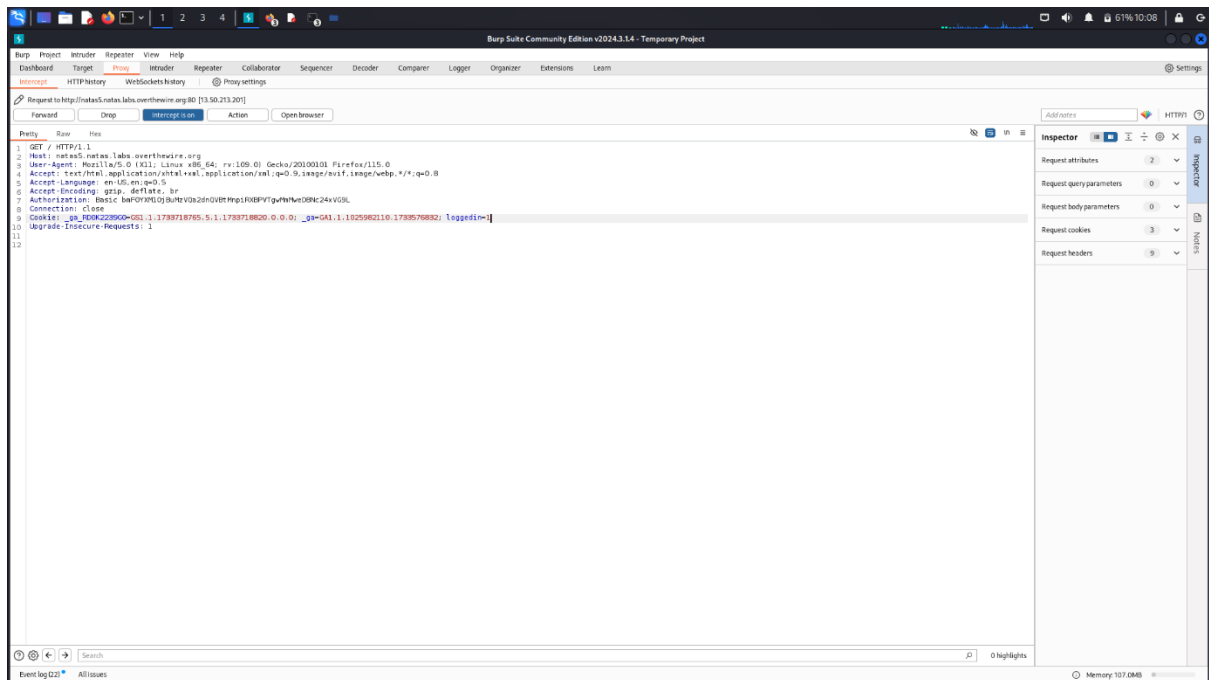
Use this and login to <http://natas5.natas.labs.overthewire.org>



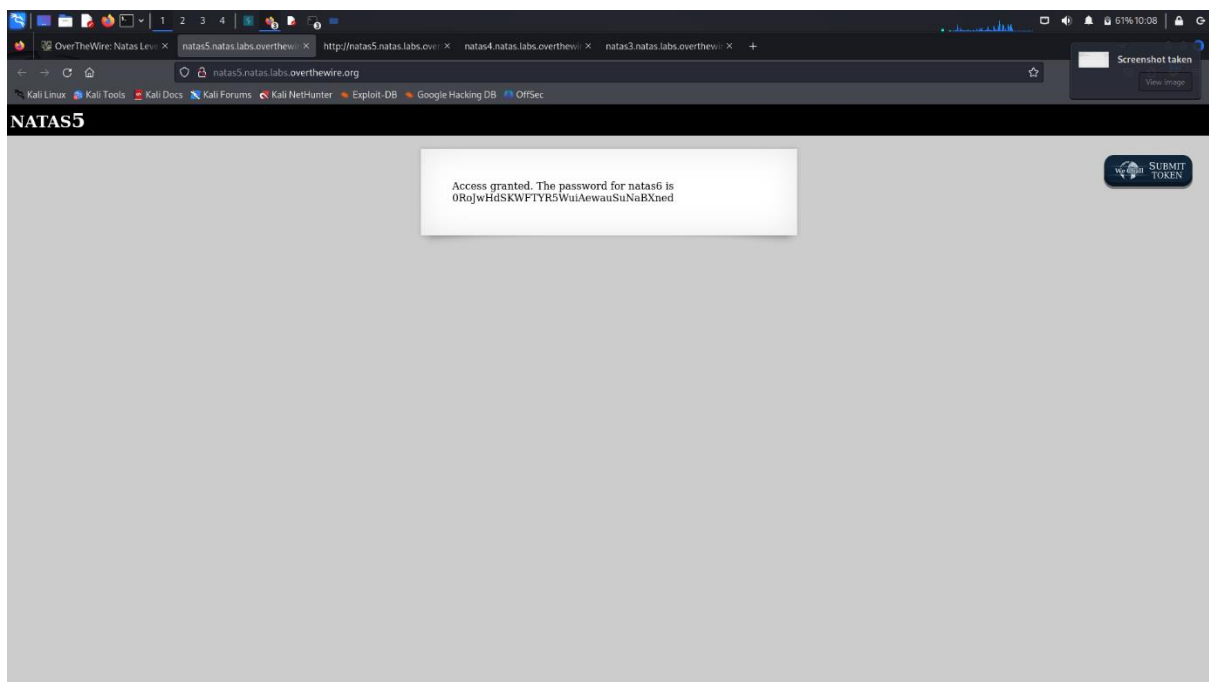
Here also the access is denied for the user so let's use burpsuite to crack it



Here we can see the loggedin value for the user is set to 0. As the access is denied we'll try changing its value to 1



then forward and reload the page the access is granted and the flag for natas6 is found



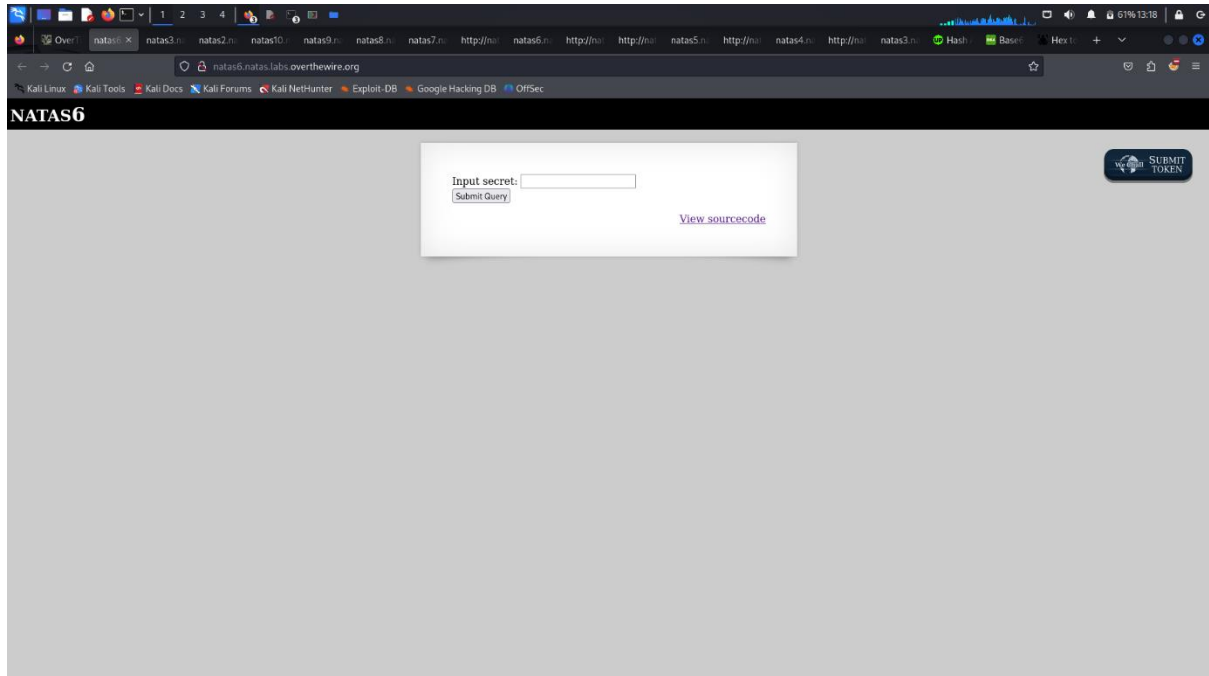
The password for natas2 is **0RoJwHdSKWFTYR5WuiAewauSuNaBXned**

NATAS 6:

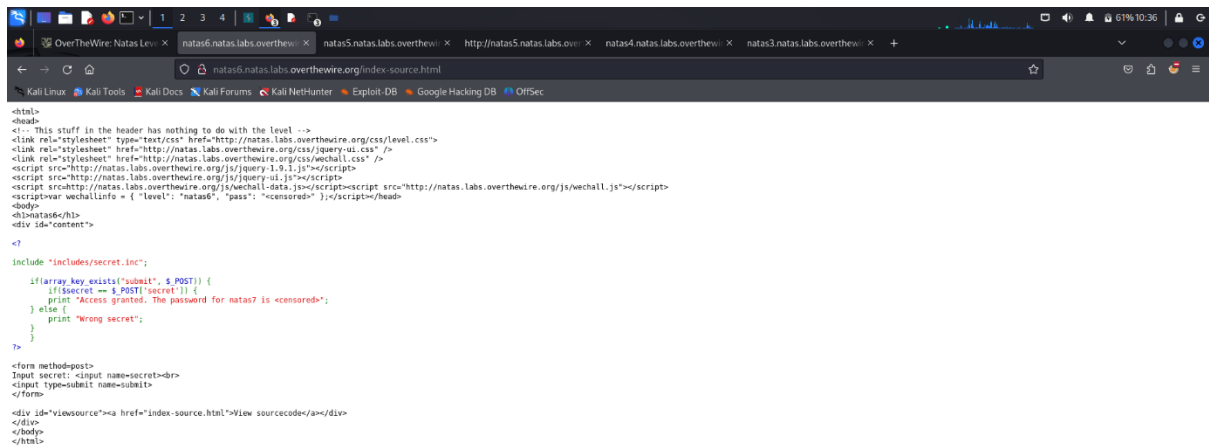
Username: **natas6**

Password: **0RoJwHdSKWFTYR5WuiAewauSuNaBXned**

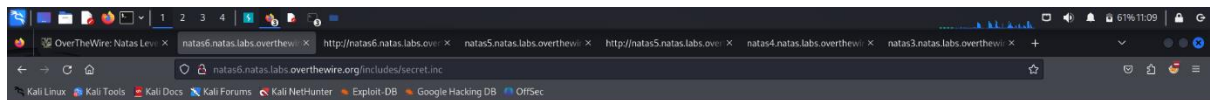
Use this and login to <http://natas6.natas.labs.overthewire.org>



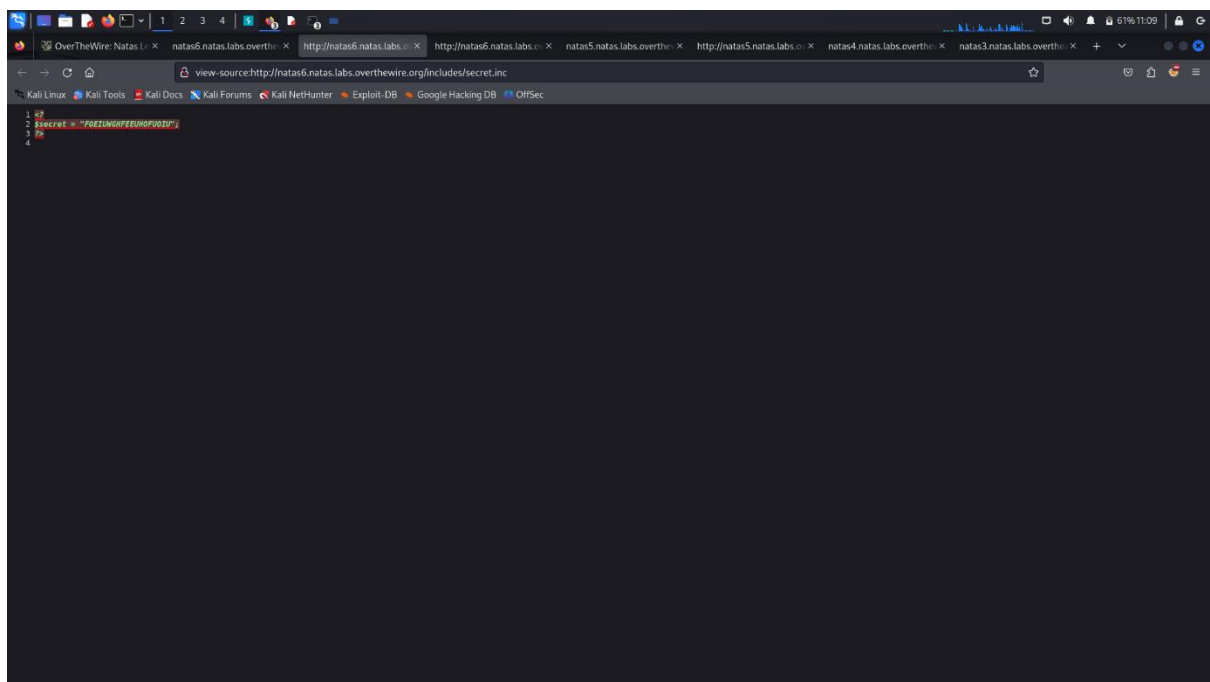
Here we have to enter a secret to find the password so find for any clues in the view sourcecode.



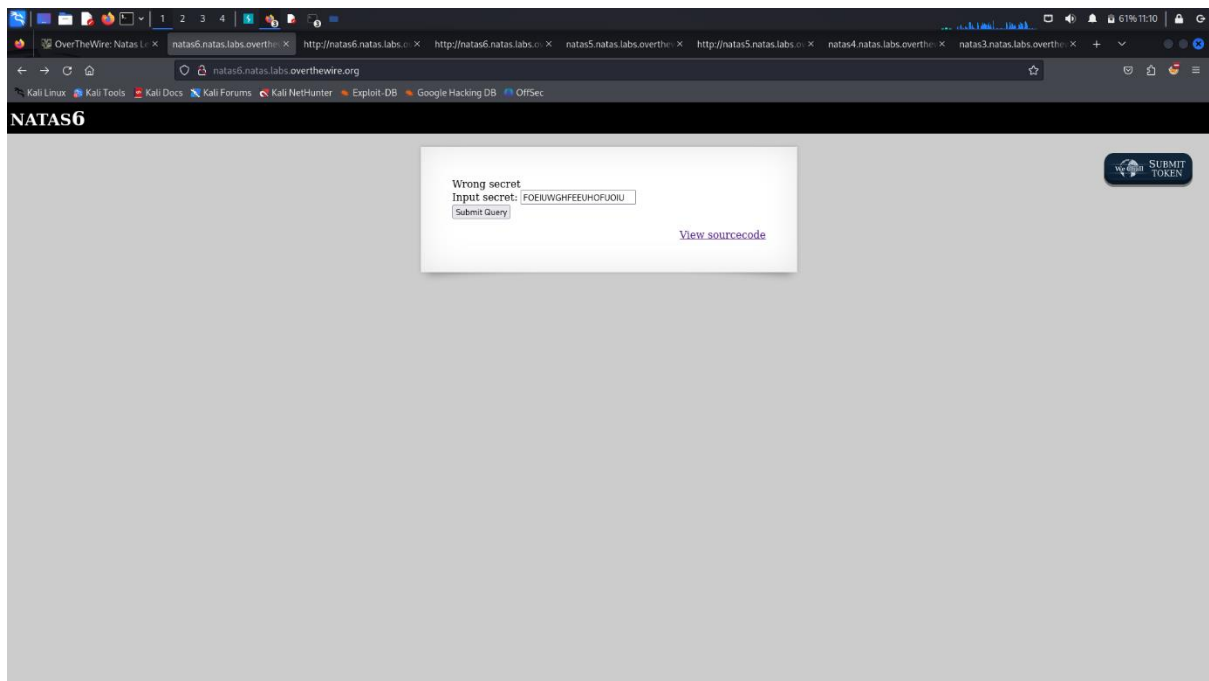
Here we can see that there is a hidden directory `/includes/secret.inc` so open it



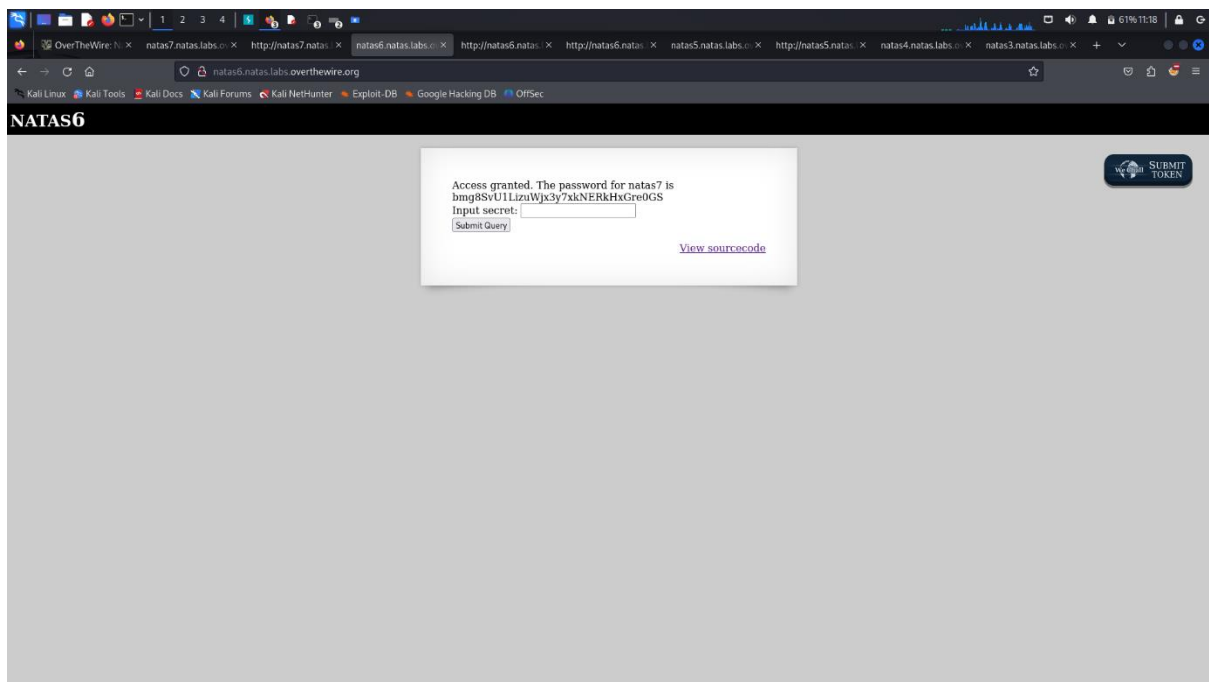
There's nothing useful here so check for something in the source page



Here we can find the secret message copy that and enter it in the text box in the dashboard



Press the submit query button and we can find the password for natas7



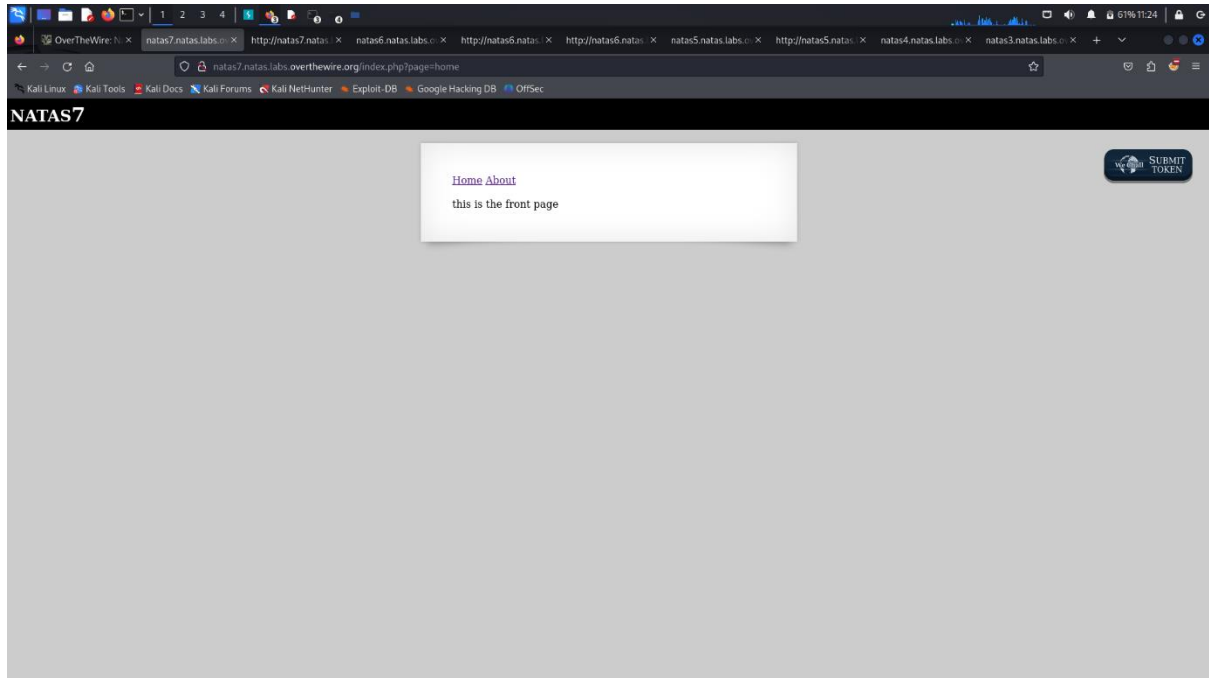
The password for natas7 is **bmg8SvU1LizuWjx3y7xkNERkHxGre0GS**

NATAS 7:

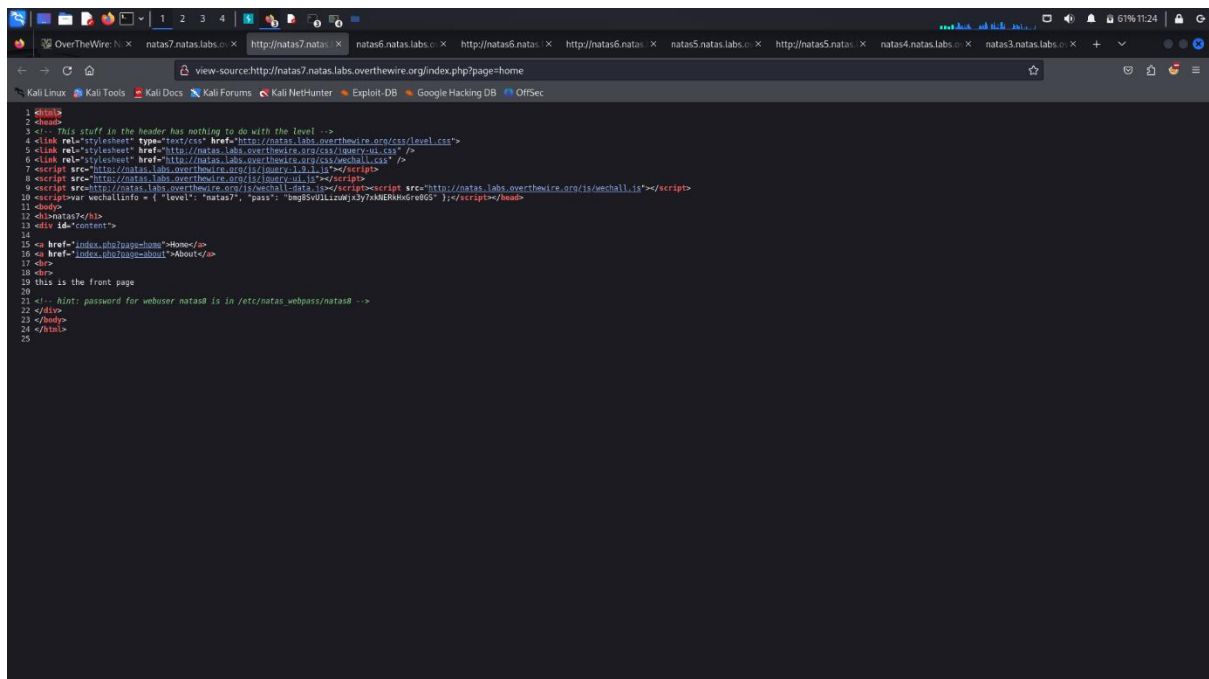
Username: **natas7**

Password: **bmg8SvU1LizuWjx3y7xkNERkHxGre0GS**

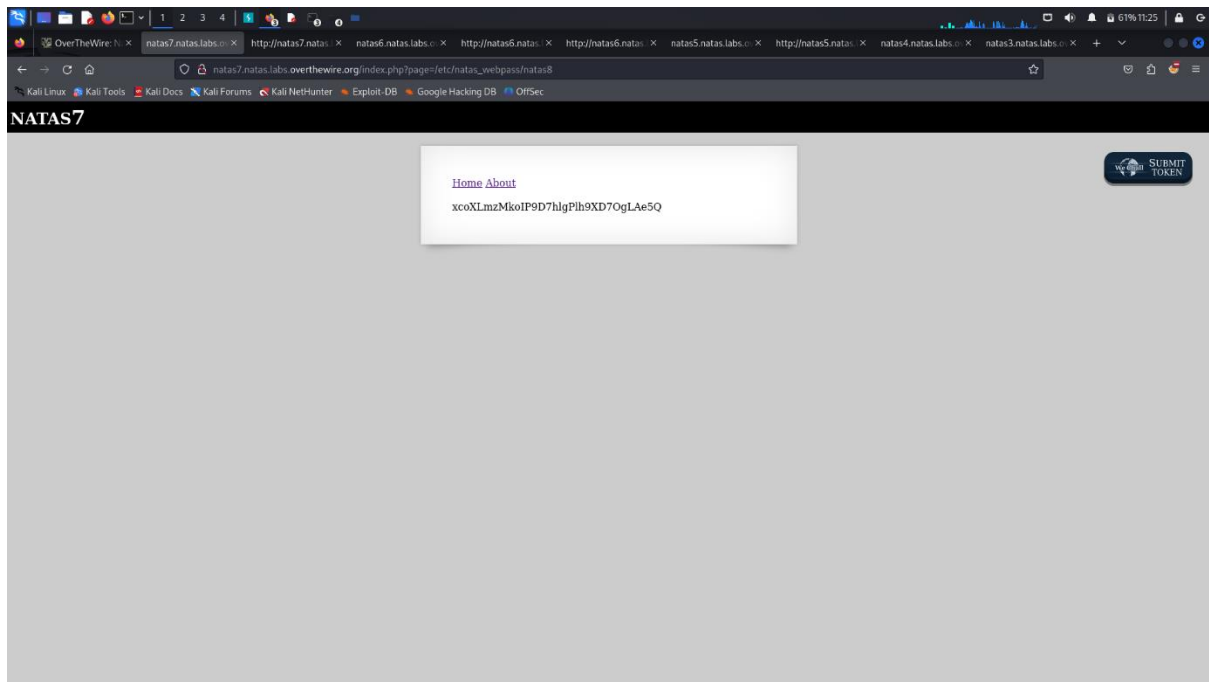
Use this and login to <http://natas7.natas.labs.overthewire.org>



Here there are only 2 pages home and about so view the source page to find something useful.



By seeing it we got clue for natas8 password which is in the directory `/etc/natas_webpass/natas8` so navigating to it we can find the password.



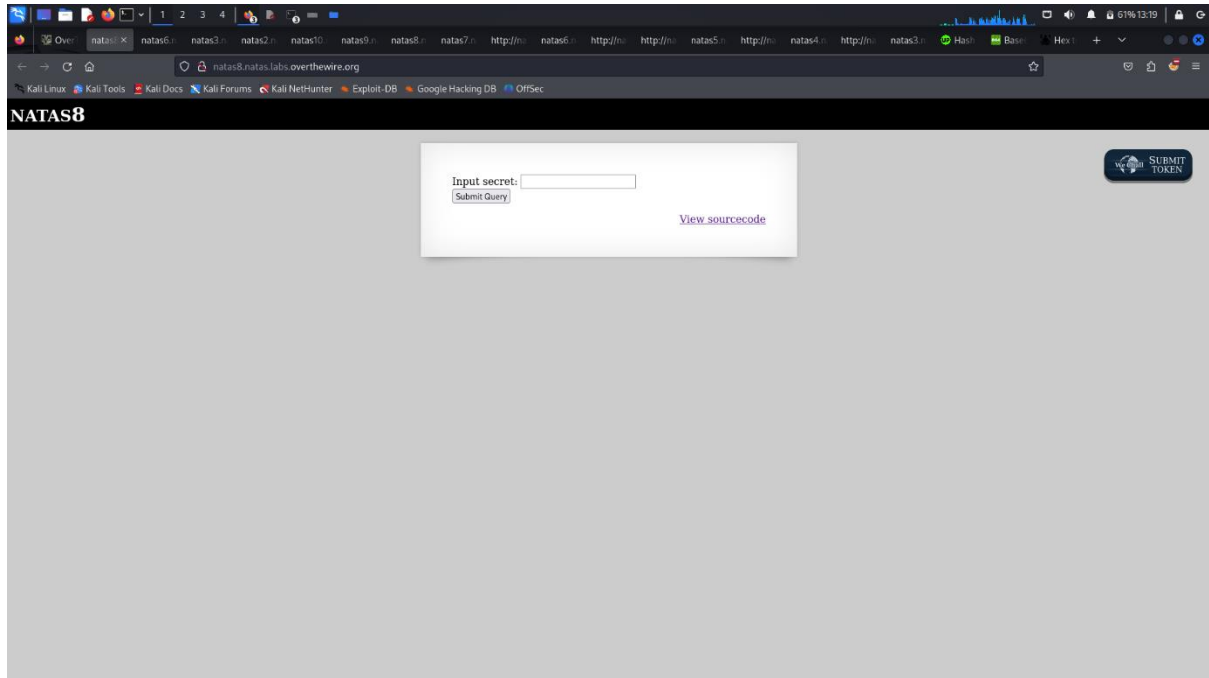
The password for natas8 is **xcoXLmzMkoIP9D7hlgPlh9XD7OgLae5Q**

NATAS 8:

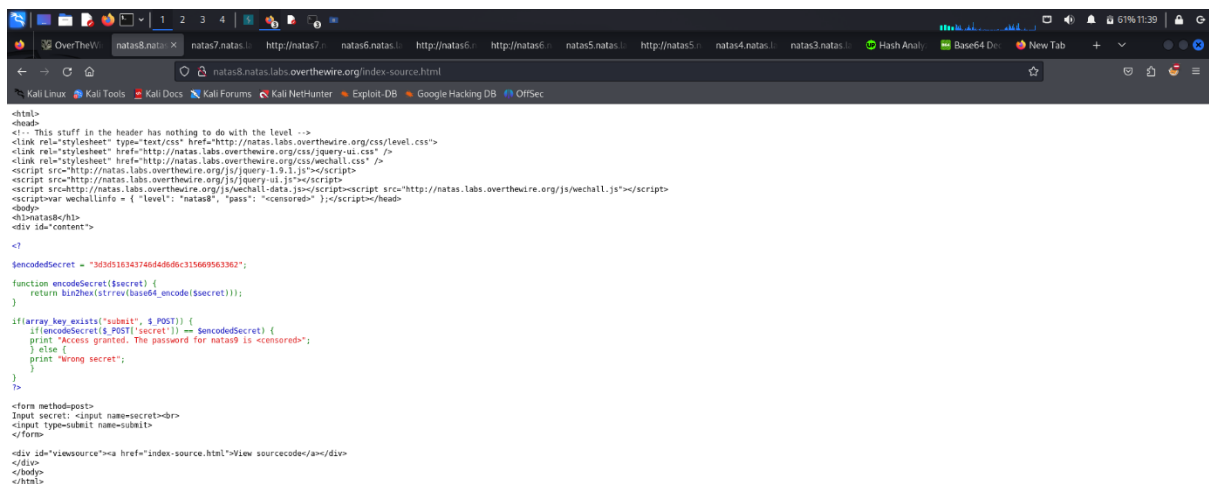
Username: **natas8**

Password: **xcoXLmzMkoIP9D7hlgPlh9XD7OgLAe5Q**

Use this and login to <http://natas8.natas.labs.overthewire.org>



Open the view sourcecode we can find a secret message hidden



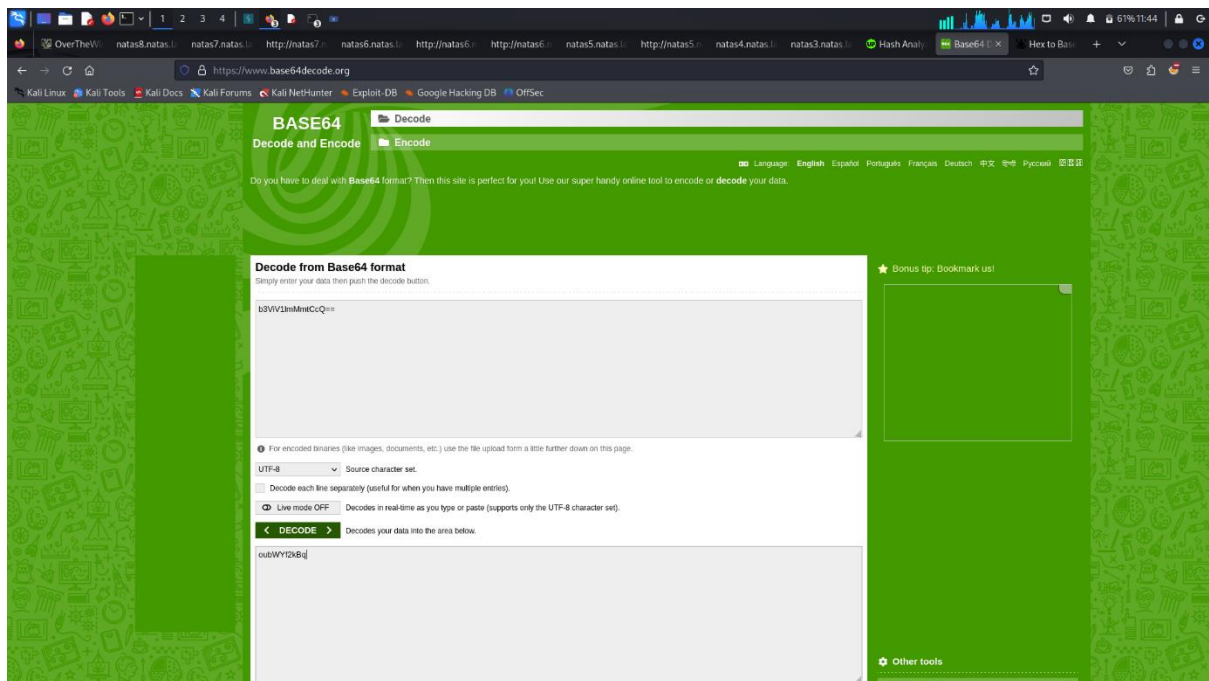
```
$encodedSecret = "3d3d516343746d4d6d6c315669563362";
```

```
function encodeSecret($secret) {  
    return bin2hex(strrev(base64_encode($secret)));  
}
```

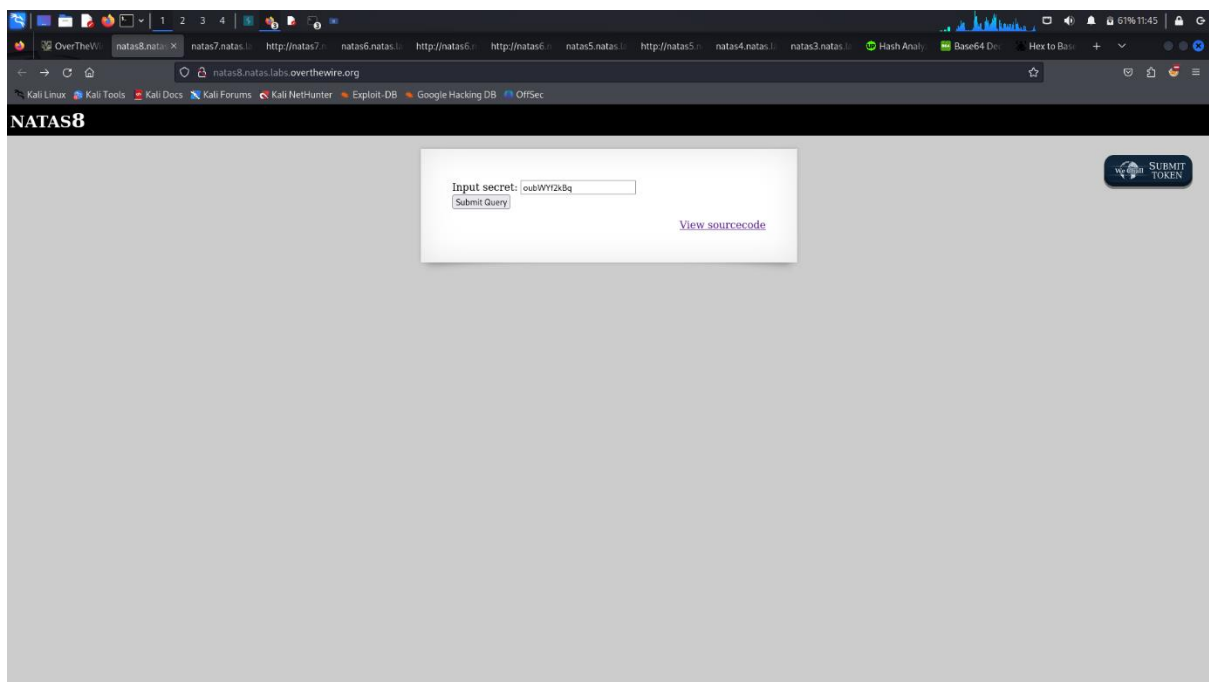
[illegible]

A screenshot of a web browser displaying the 'Base64 Decode and Encode' website. The browser's address bar shows the URL 'https://www.base64decode.org'. The website has a green background with a pattern of small icons. At the top, there are tabs for 'Decode' and 'Encode'. Below this, a message states: 'Do you have to deal with Base64 format? Then this site is perfect for you! Use our super handy online tool to encode or decode your data.' The main section is titled 'Decode from Base64 format' and includes instructions: 'Simply enter your data then push the decode button.' A text input field contains the string 'PT1RYON06U1bDPFwVzYg=='. Below the input field, there are options for 'UTF-8' character set, a checkbox for 'Decode each line separately', and a radio button for 'Live mode OFF'. A green button labeled '< DECODE >' is visible. The output area shows the decoded string '==QcCrmMnt1VV3b'. A 'Bonus tip: Bookmark us!' message is also present.

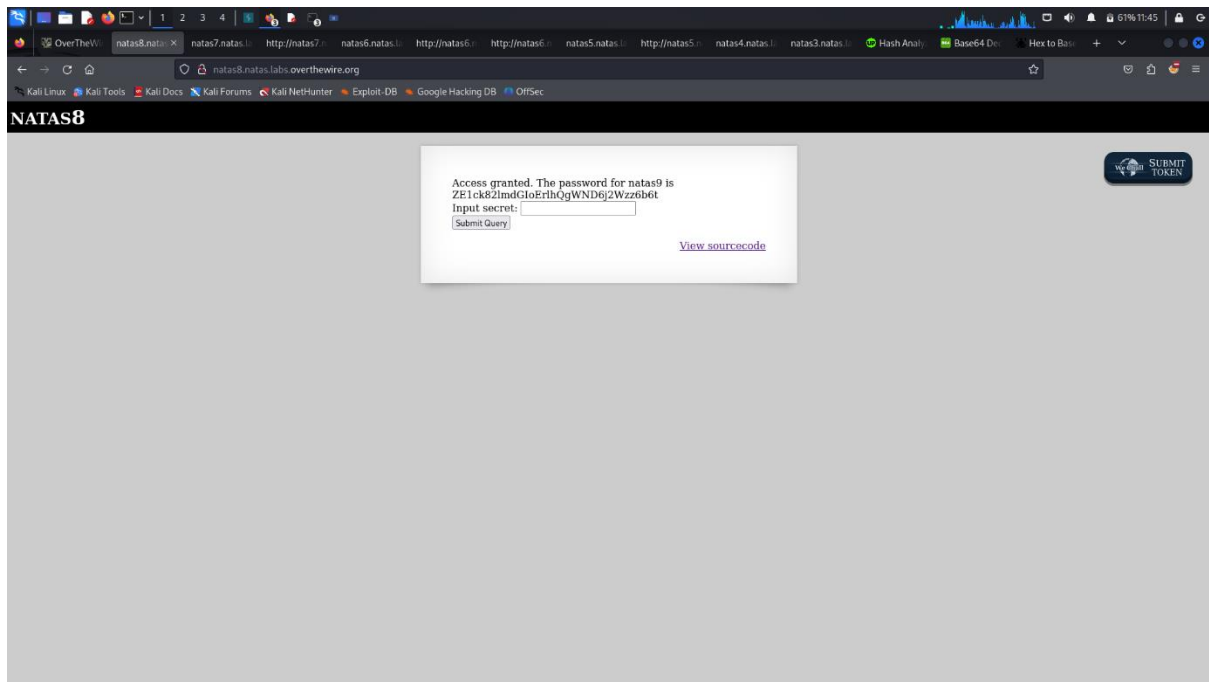
Now we need to decode it again to get the secret message



Now we got the secret message **oubWYf2kBq** paste it on the input



Press submit query to get the password for natas9 user



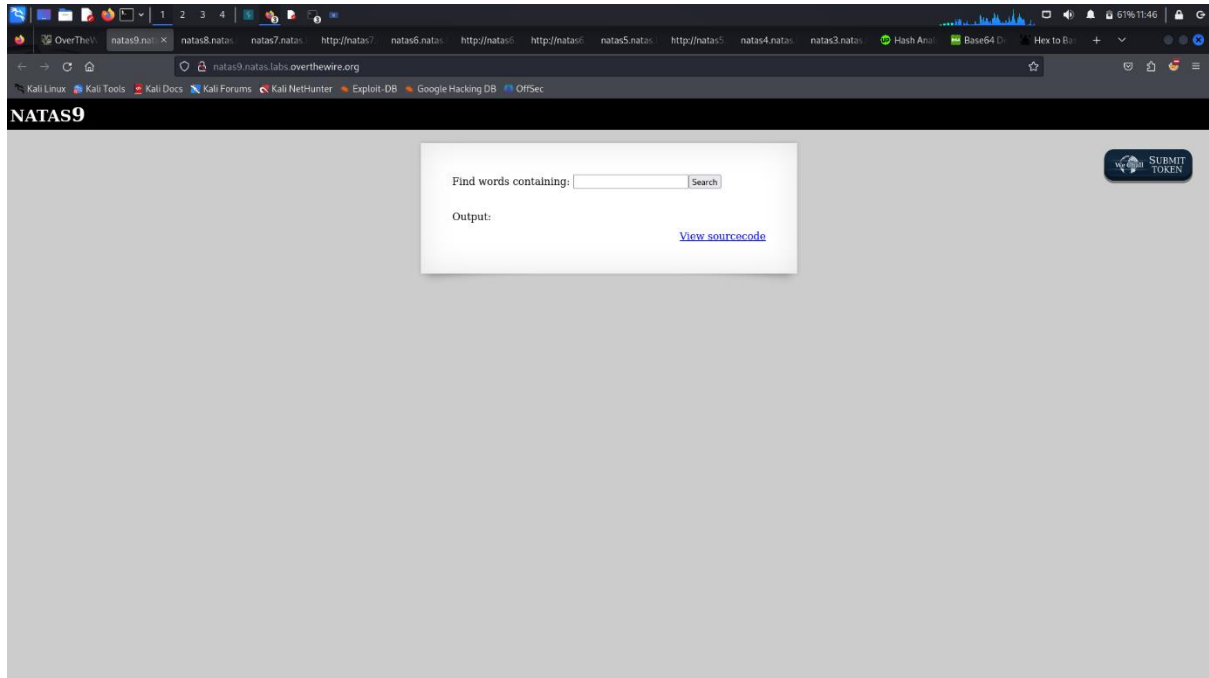
The password for natas9 is **ZE1ck82lmdGIoErIhQgWND6j2Wzz6b6t**

NATAS 9:

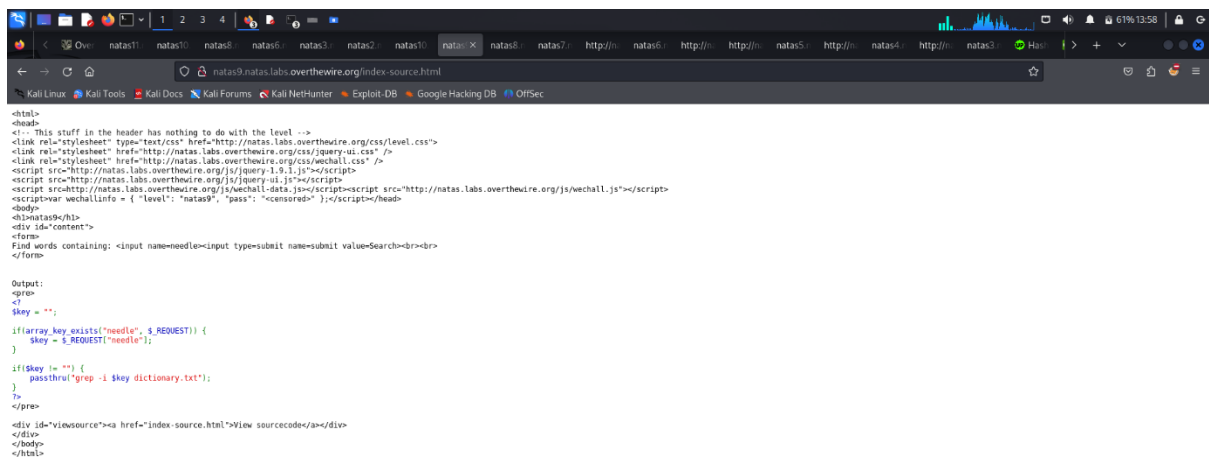
Username: **natas9**

Password: **ZE1ck82lmdGIoErlhQgWND6j2Wzz6b6t**

Use this and login to <http://natas9.natas.labs.overthewire.org>



View the sourcecode

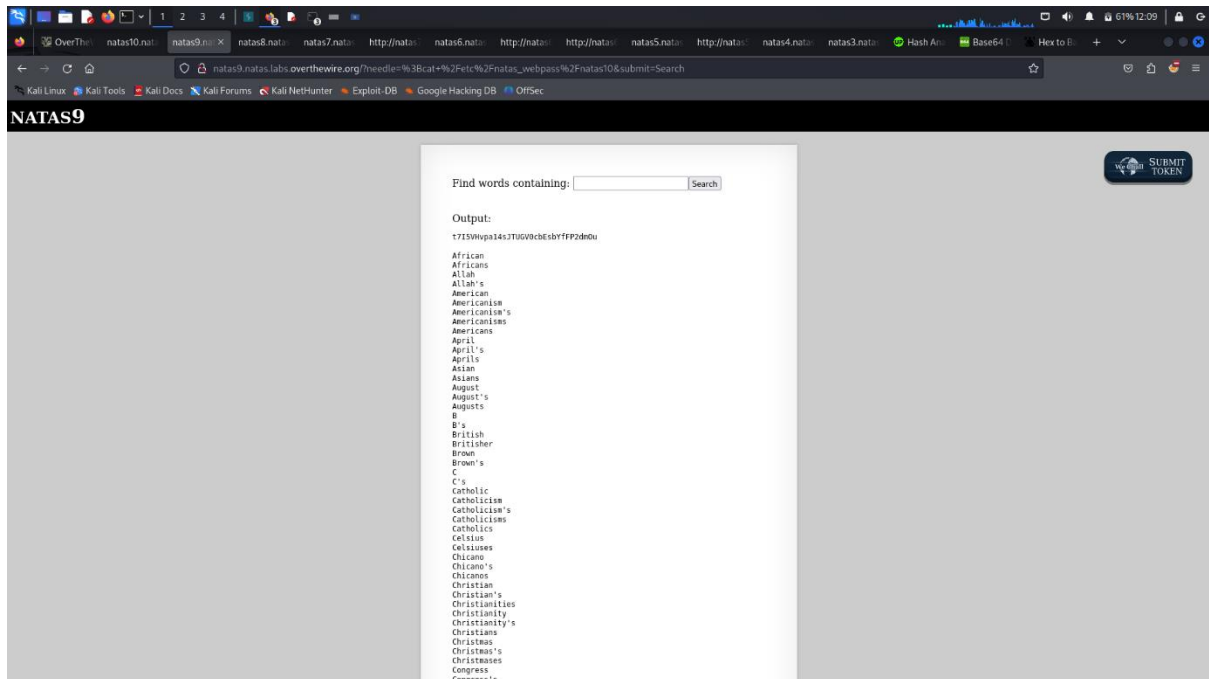


If we enter any word it gets input using funct passthru() and sends it as \$key.

So we can try executing several commands using (;)

We can try this -- **;cat /etc/natas_webpass/natas10**

Here (;) is used to separate multiple commands, cat is used to display all the content in that file



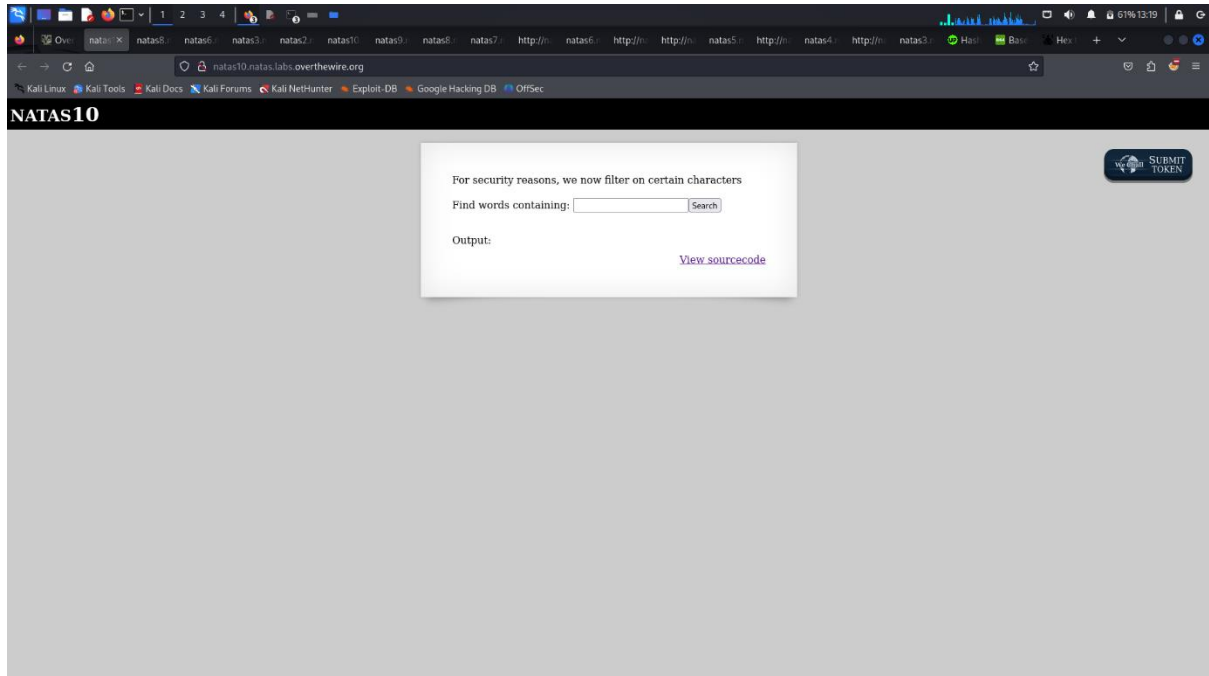
The password for natas10 is **t7I5VHypa14sJTUGV0cbEsbYfFP2dmOu**

NATAS 10:

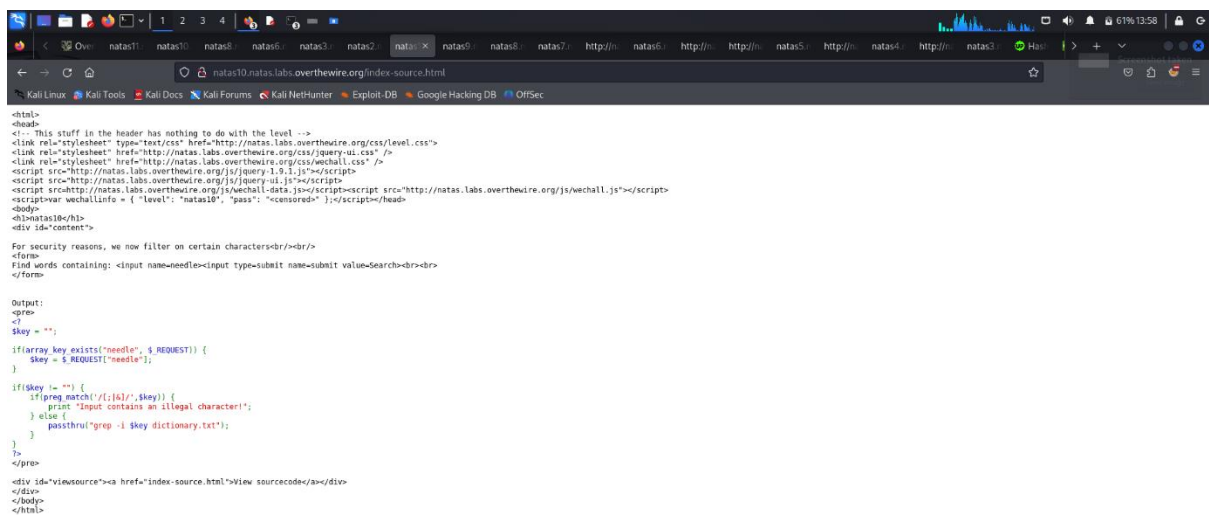
Username: **natas10**

Password: **t7I5VHvpa14sJTUGV0cbEsbYfFP2dmOu**

Use this and login to <http://natas10.natas.labs.overthewire.org>

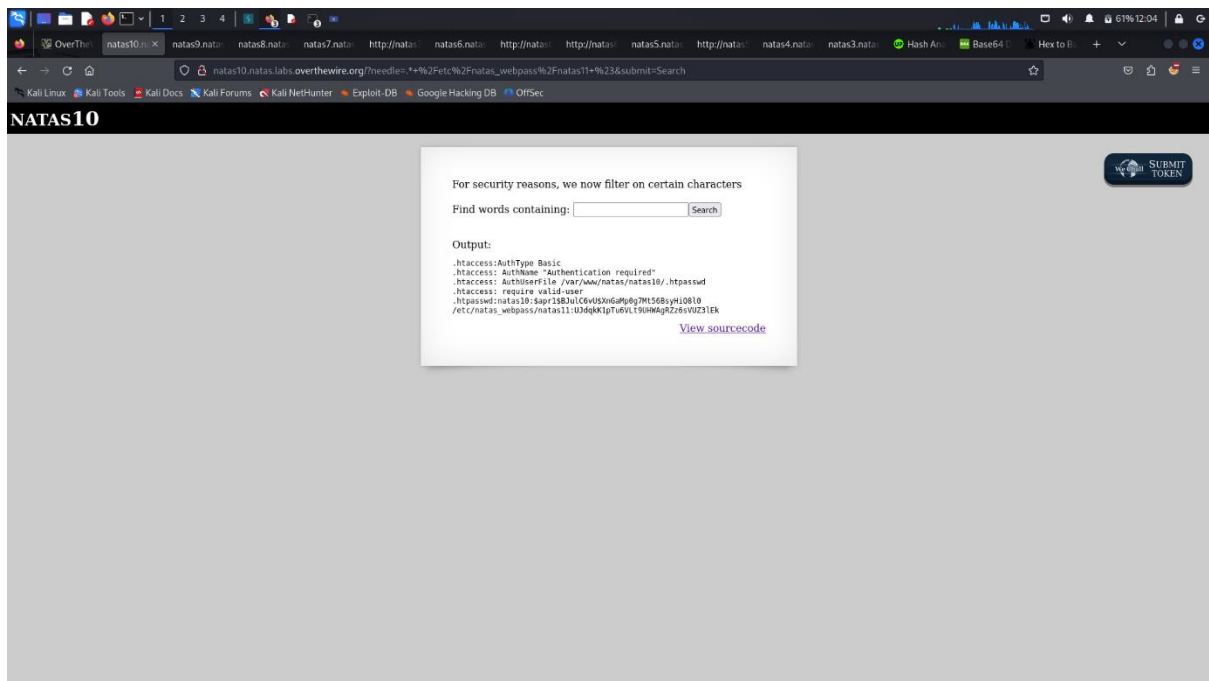


On viewing the sourcecode we can find that If we enter any word it gets input using funct `passthru()` and sends it as `$key` and we are restricted to use few characters such as `/` and `;` and `&`



To override this filter we can use `(.*)` and `(#)`

We can try using this command --- `.* /etc/natas_webpass/natas11 #`



The password for natas11 is **UJdqkK1pTu6VLt9UHWAgRZz6sVUZ3IEk**

- Submitted by **Dheepan G**