Project Report

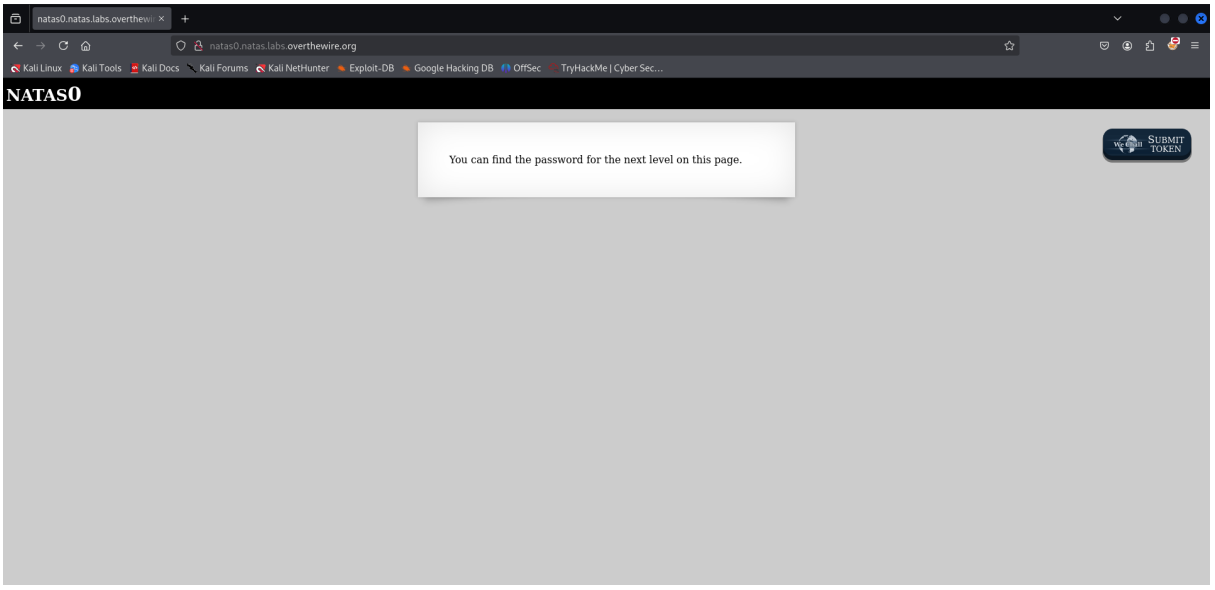
Overthewire Natas

LEVEL 0:

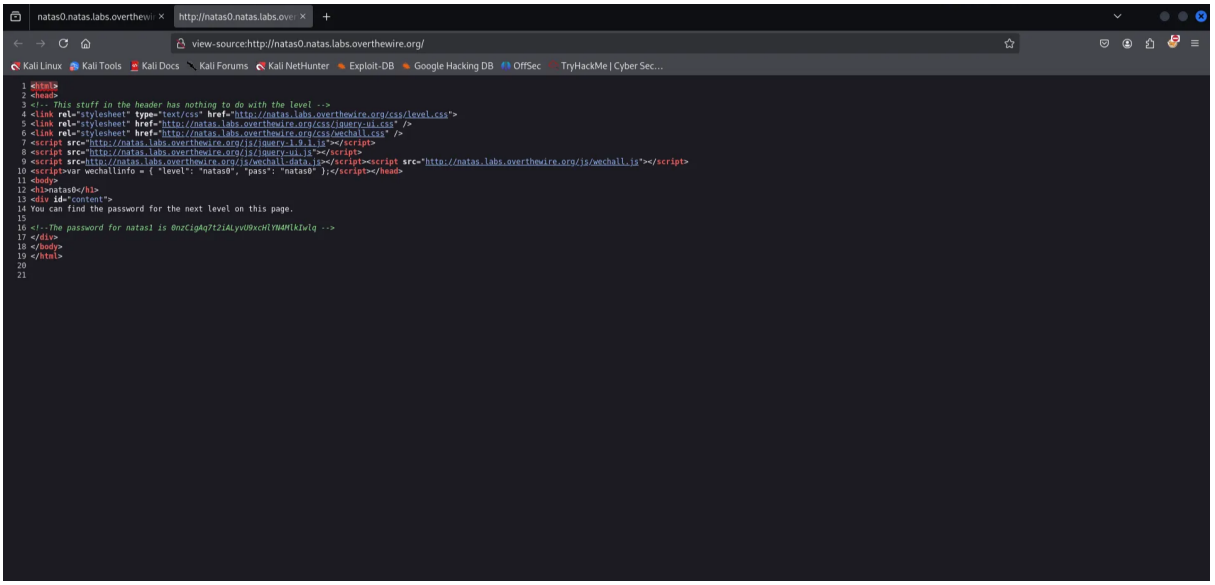
Start here:

Username: natas0
Password: natas0
URL: http://natas0.natas.labs.overthewire.org

- Go to the above url and login using the above mentioned credentials to access the level 0 of Natas.

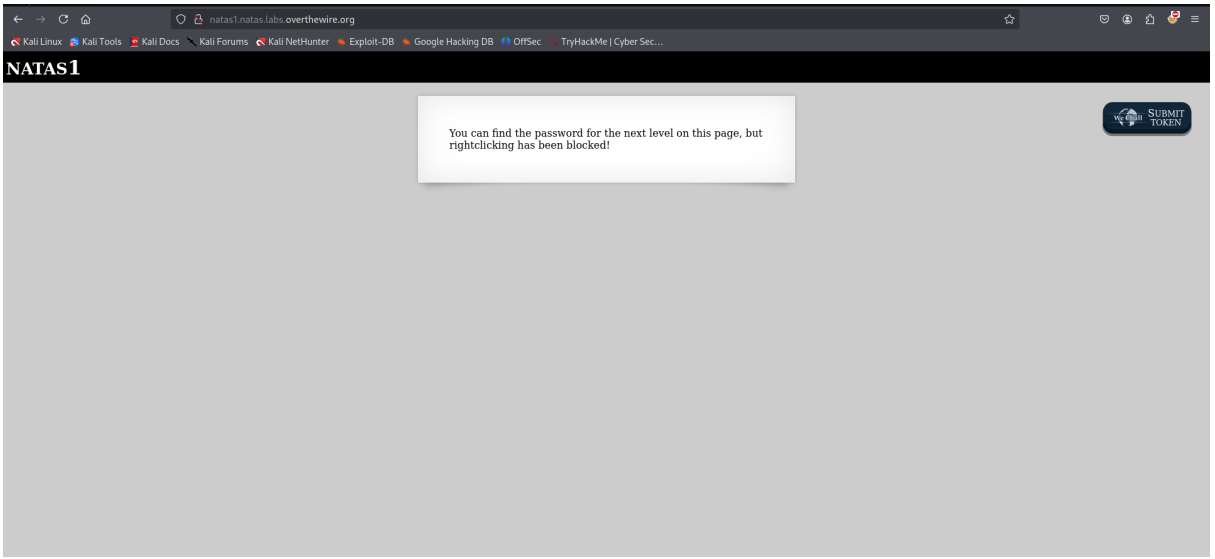


- Now, view the source code of the webpage where the password flag for the next level is in comment.
- Password for level 1 : *0nzCigAq7t2iALyvU9xcHlYN4MlkIwlq*.

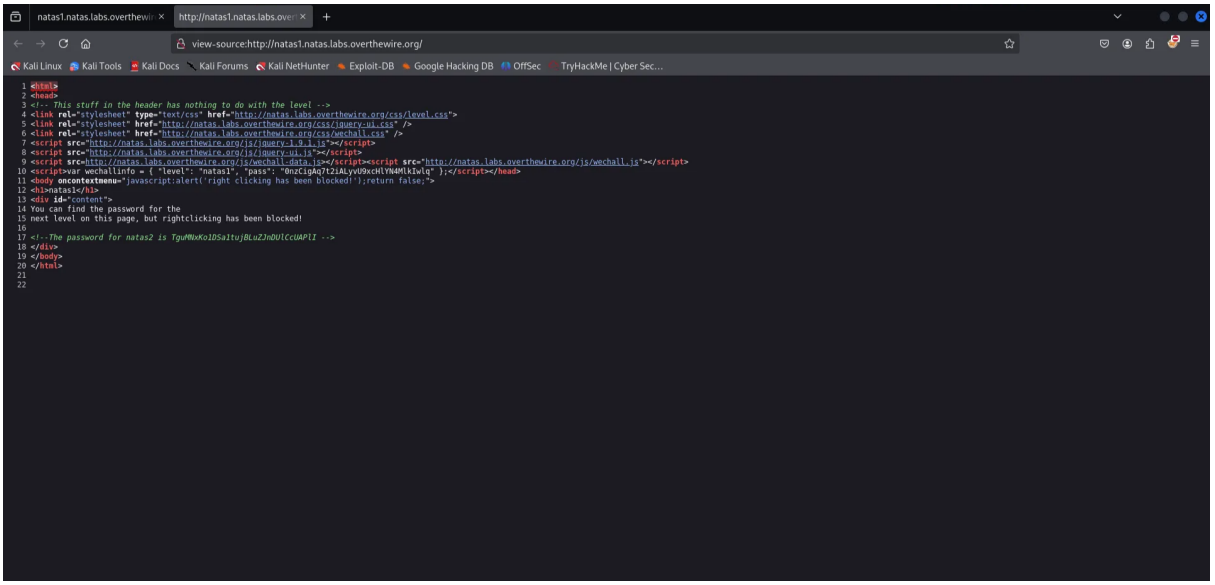


LEVEL 1:

- Now, go to the url http://natas1.natas.labs.overthewire.org and login using "*natas1*" as username and the password found from level 0 to access level 1.



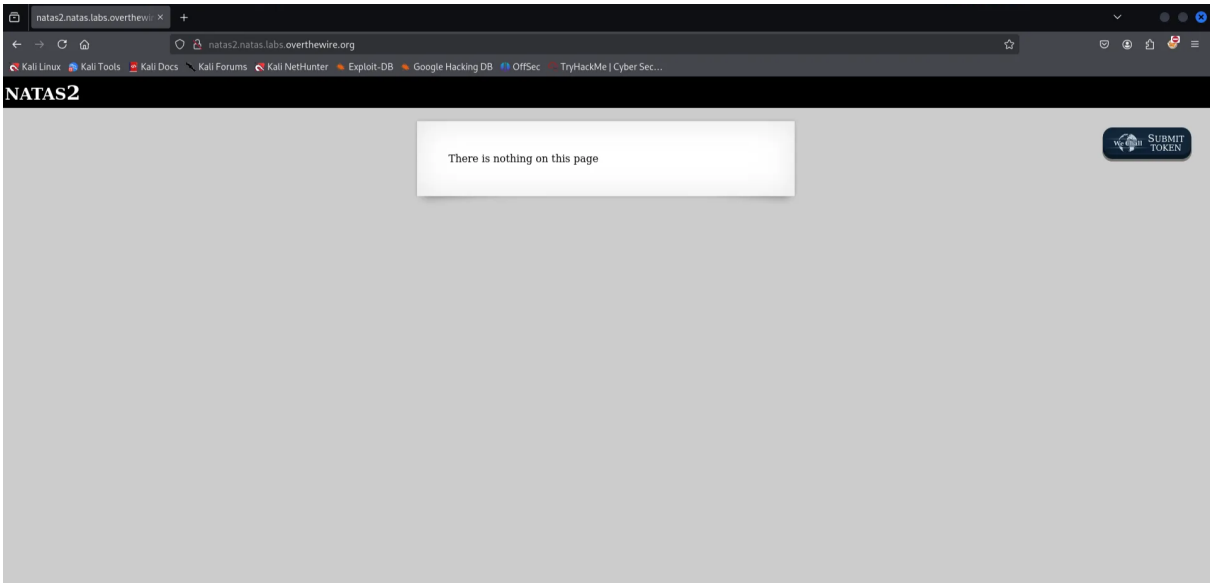
- Here, right click has been disable within the white frame , so view page source outside the white frame.



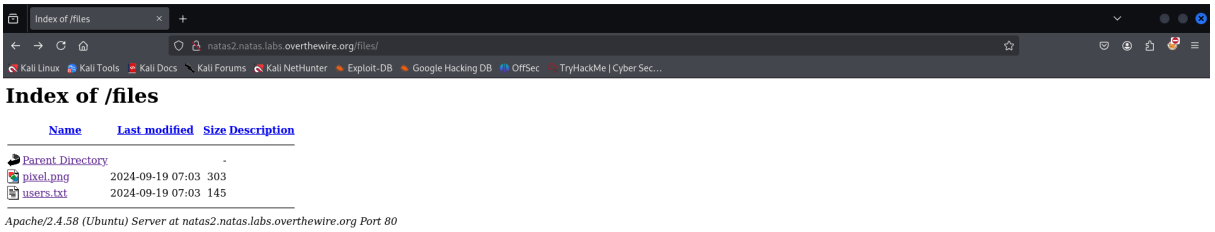
- Now, view the source code of the webpage where the password flag for the next level is in comment.
- Password for level 2 : *TguMNxKo1DSa1tujBLuZJnDUlCcUAPlI*

LEVEL 2:

- Now, go to the url http://natas2.natas.labs.overthewire.org and login using *"natas2"* as username and the password found from level 1 to access level 2.



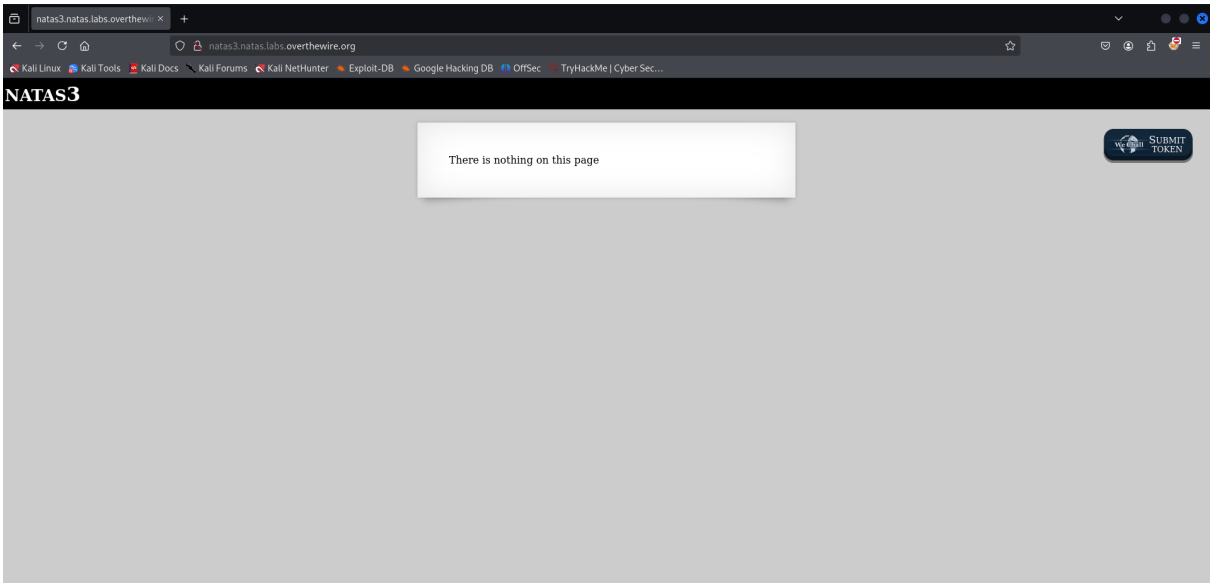
- Now, view the source code of the webpage where we can see there is a tag <img src="files/pixel.png">, this shows that there is a directory named files.
- Now, try traversing to the “/files” directory.



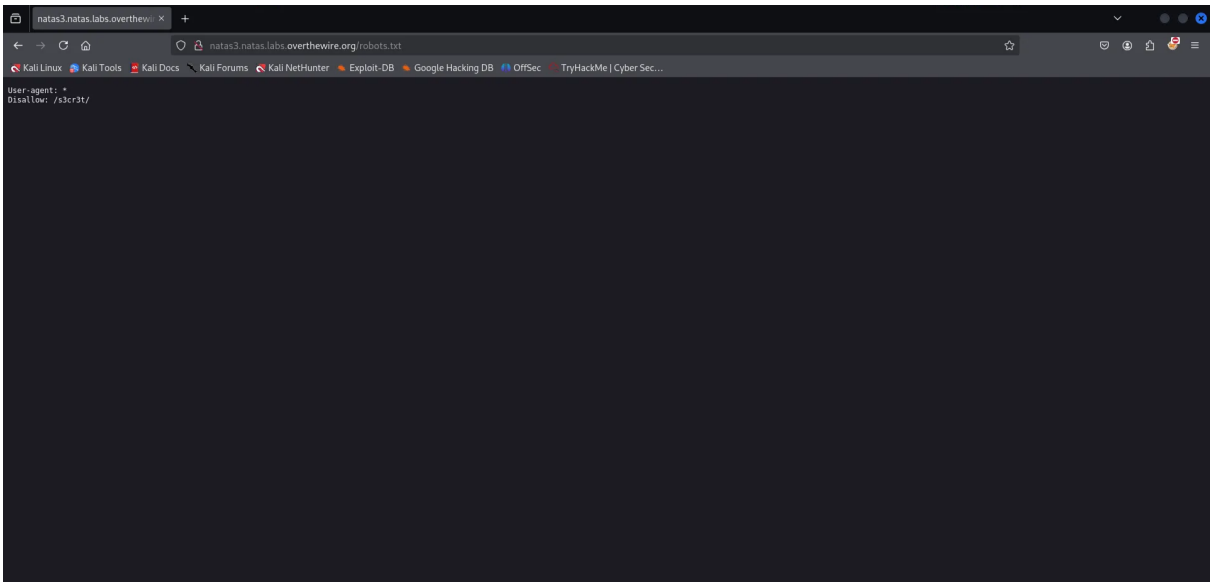
- We can see there is a text file named “users.txt” and contains the password for level 3 in it.
- Password for level 3 : *3gqisGdR0pjm6tpkDKdIWO2hSvchLeYH.*

LEVEL 3:

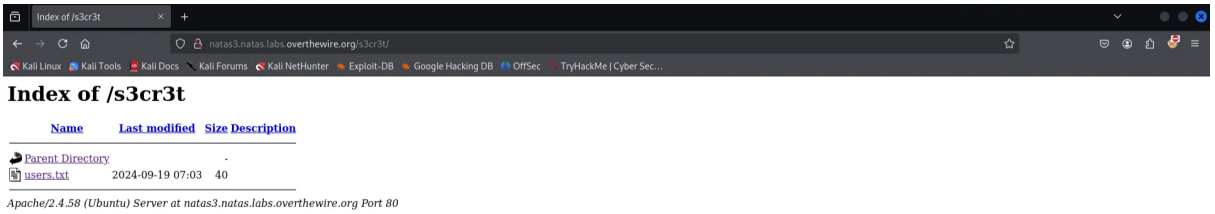
- Now, go to the url http://natas3.natas.labs.overthewire.org and login using “*natas3*” as username and the password found from level 2 to access level 3.



- Now, try traverse to “/robots.txt” to check for hidden directories.
- Now, we can see that there is a hidden directory “/s3cr3t/”.

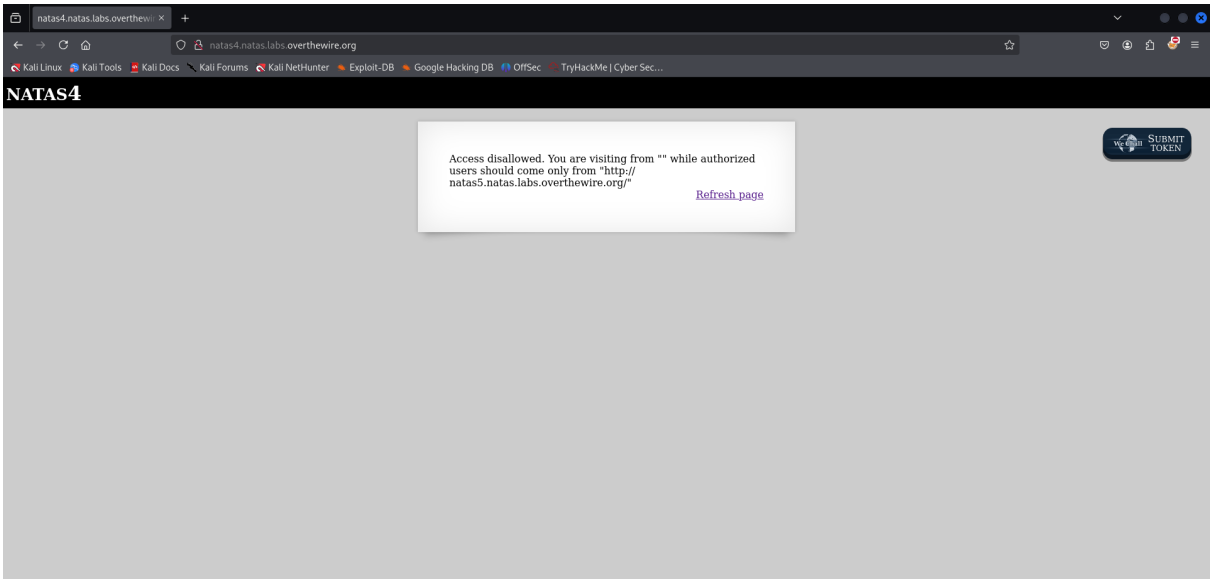


- Here there is a file “users.txt” with the password flag for the next level.
- Password for level 4 : *QryZXc2e0zahULdHrtHxzyYkj59kUxLQ.*



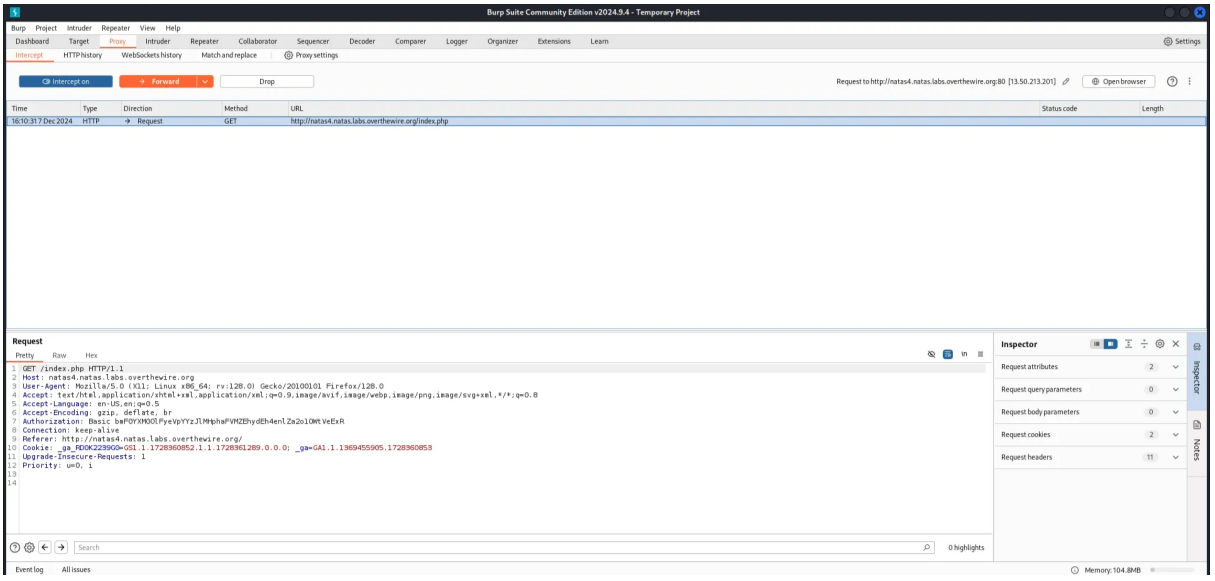
LEVEL 4:

- Now, go to the url http://natas4.natas.labs.overthewire.org and login using *“natas4”* as username and the password found from level 3 to access level 4.

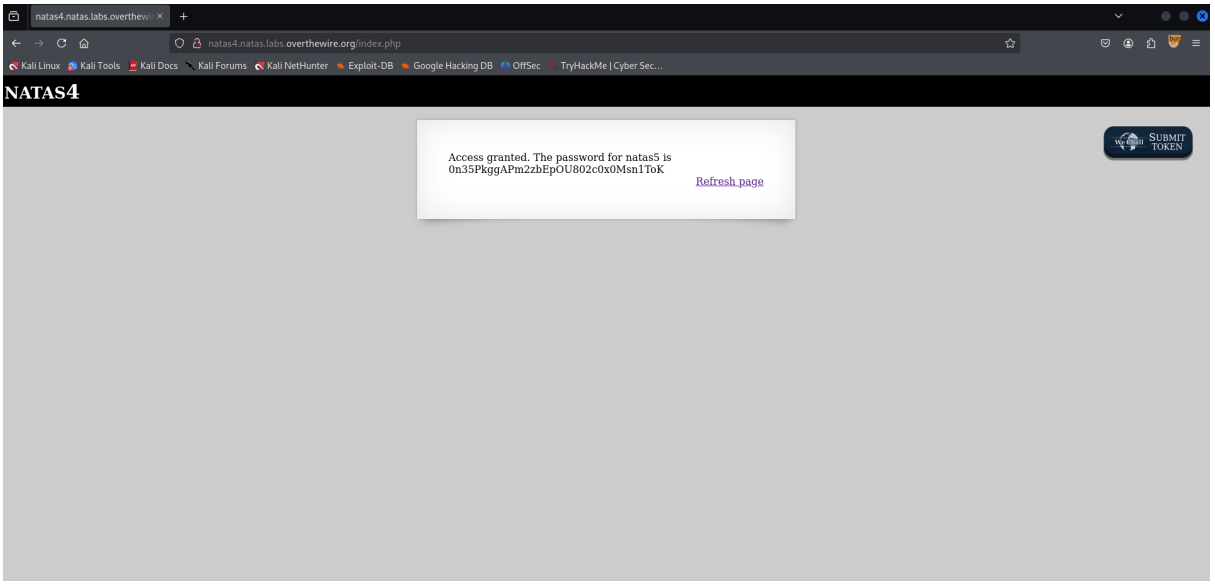


- In this page it says that *“Access disallowed. You are visiting from "" while authorized users should come only from "http://natas5.natas.labs.overthewire.org/""*

- Intercept this request using Burp proxy in Burp suite and click the "*Refresh page*" in the webpage. Now inspect the request captured.

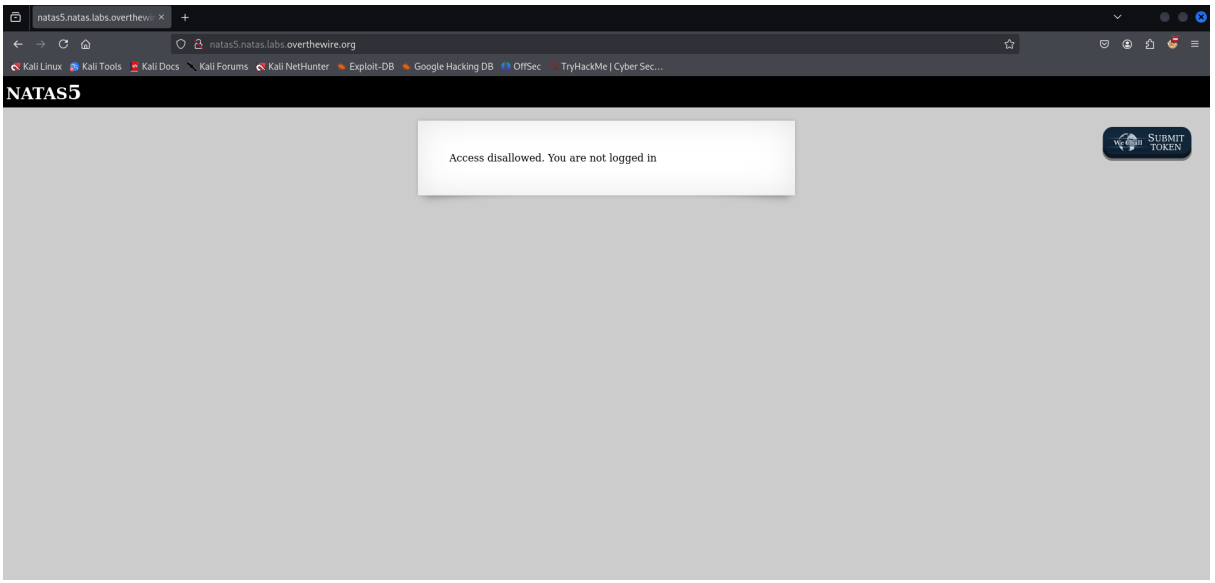


- Now, check for Referer parameter and alter it to *"http://natas5.natas.labs.overthewire.org/"* and forward the request.
- Now the password flag is available in the webpage.
- Password for level 5 : *0n35PkggAPm2zbEpOU802c0x0Msn1ToK*.

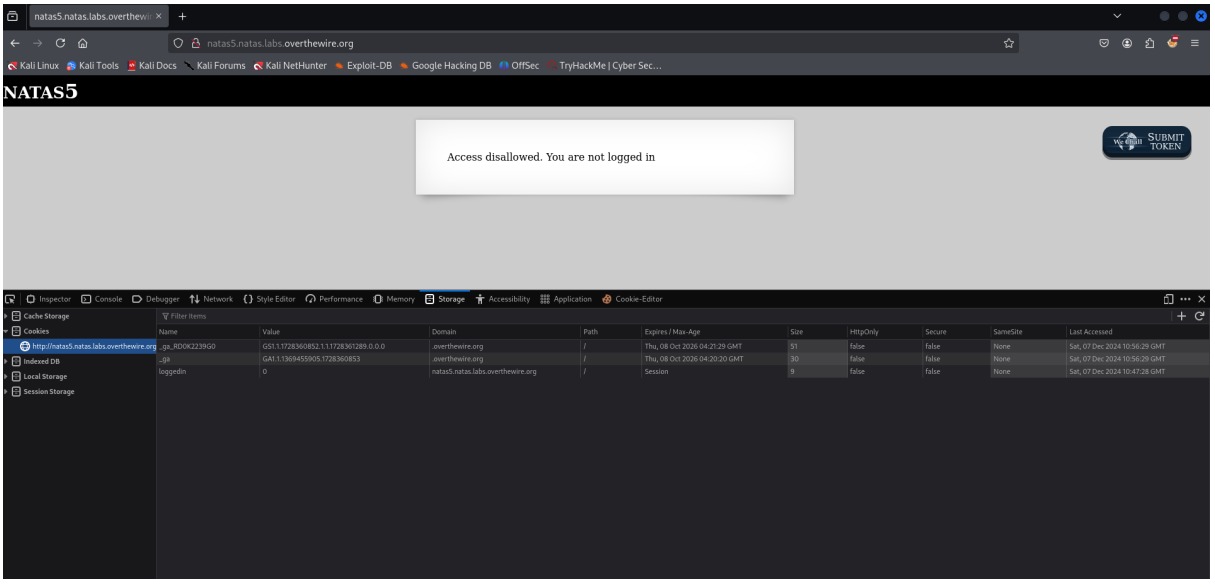


LEVEL 5:

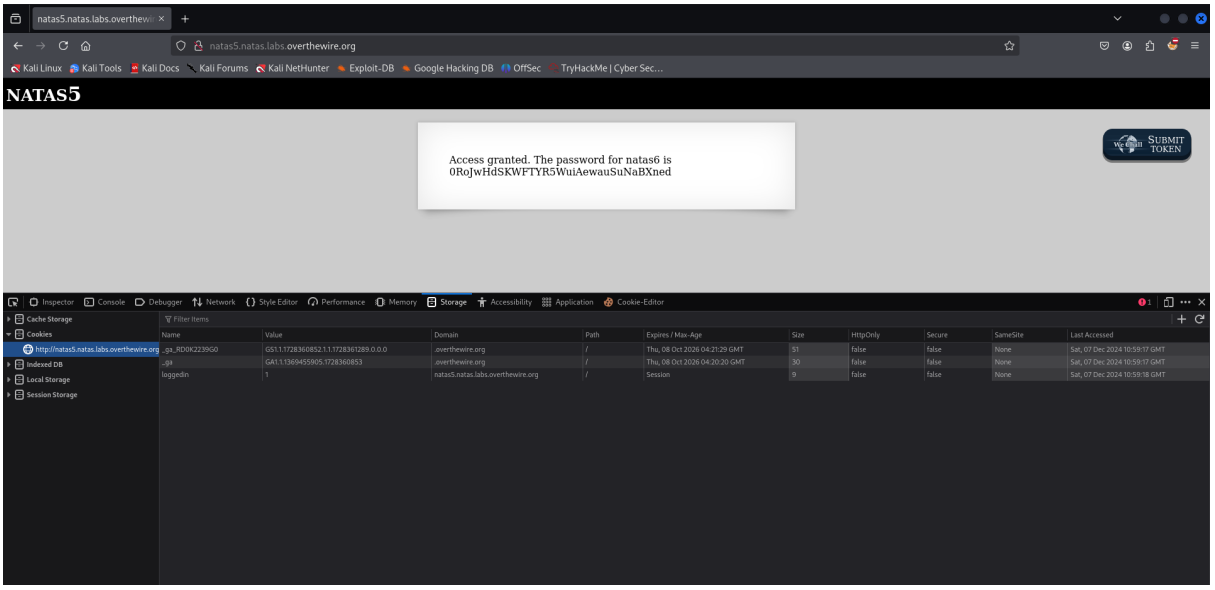
- Now, go to the url http://natas5.natas.labs.overthewire.org and login using “*natas5*” as username and the password found from level 4 to access level 5.



- It says that “*Access disallowed. You are not logged in*”.
- Check for cookies of this page in the browser.
- Now, we can see there is a cookie ‘*loggedin*’ with value 0.



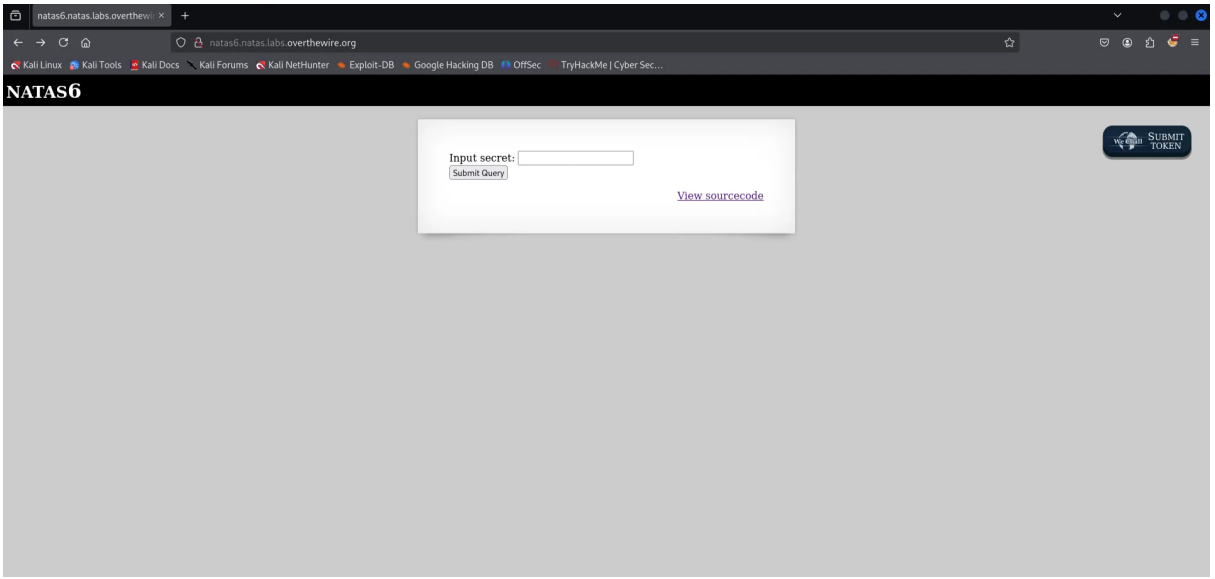
- Change the cookie value to 1 and reload the page.



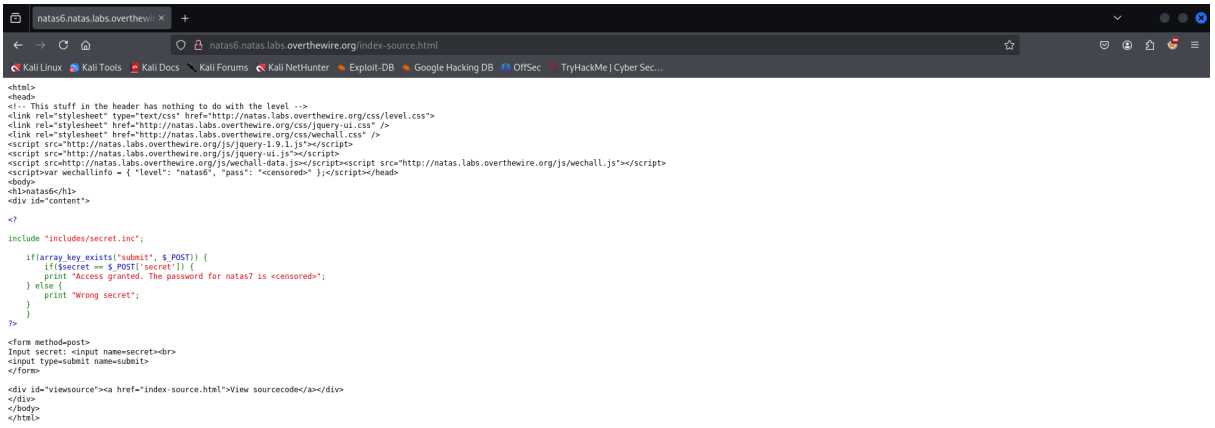
- Now, the password flag is visible.
- Password for level 6 : *0RoJwHdSKWFTYR5WuiAewauSuNaBXned.*

LEVEL 6:

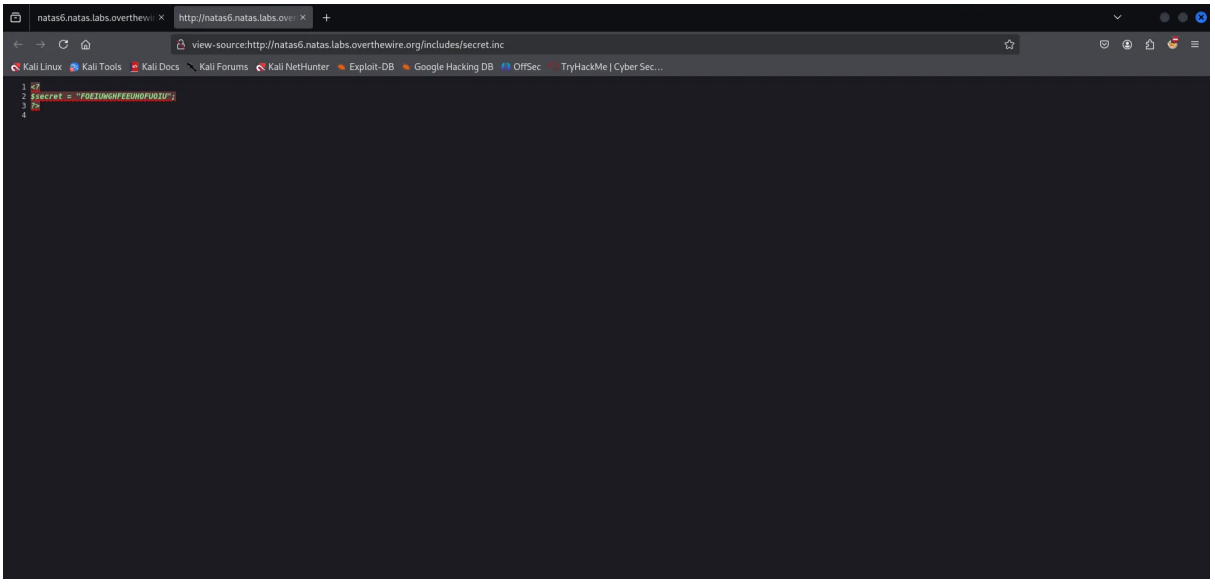
- Now, go to the url http://natas6.natas.labs.overthewire.org and login using *“natas6”* as username and the password found from level 5 to access level 6.



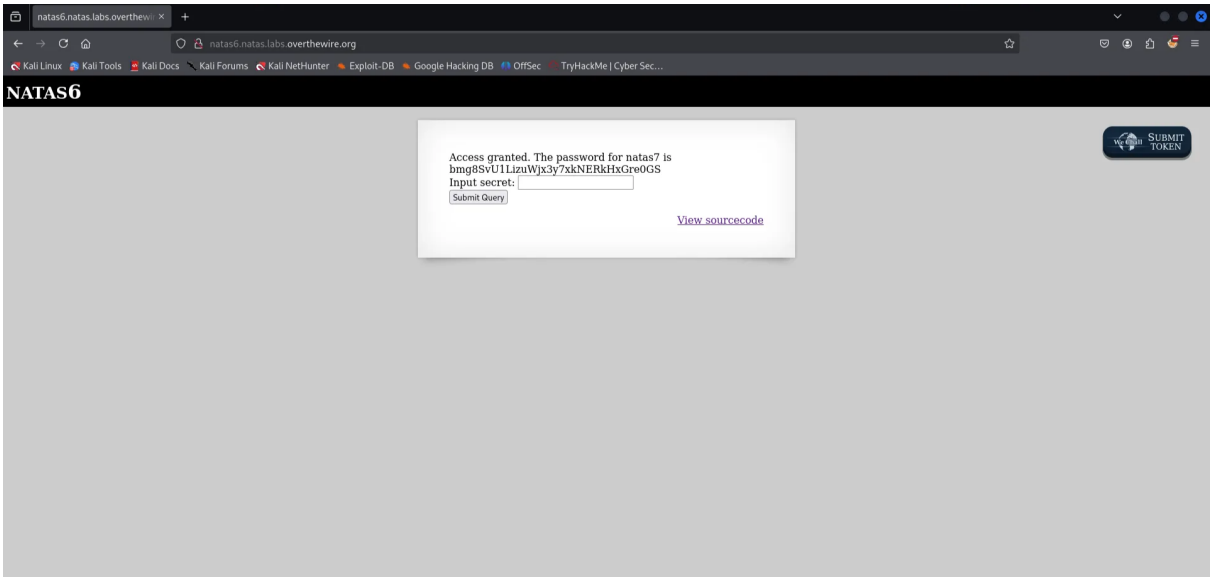
- Now, view the sourcecode of the page using the hyperlink in the page.



- We can see that the secret is located in "*includes/secret.inc*", traverse to the directory.
- Now, we can see a empty webpage with no clue. So view page source to identify any hint.



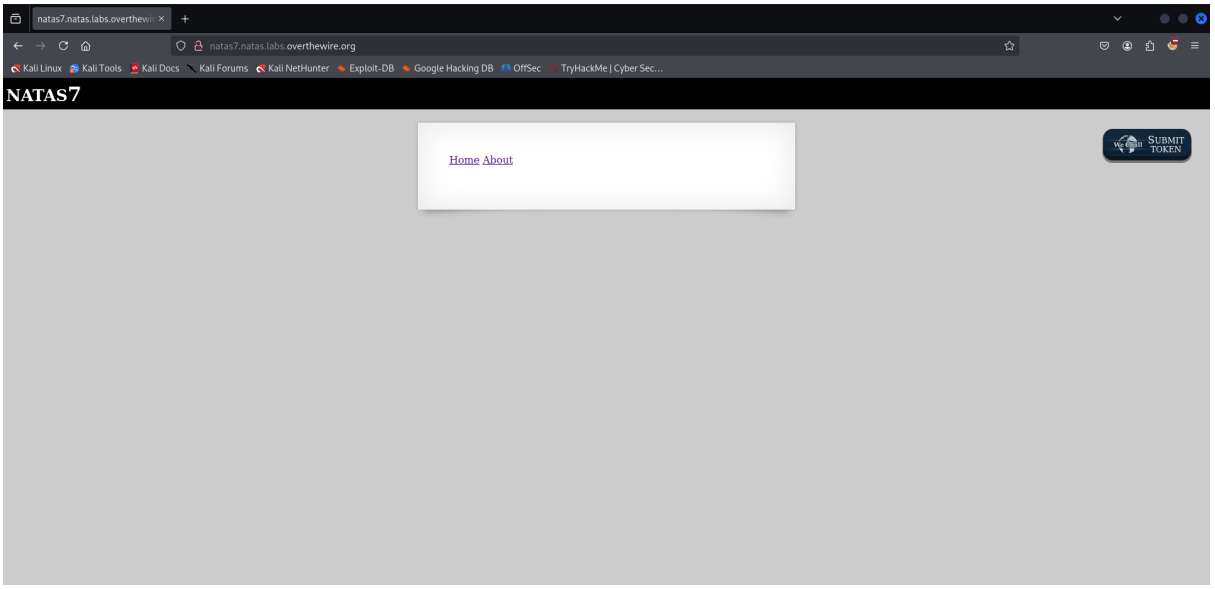
- Now we got the secret "FOEIUWGHFEEUHOFUOIU", try this as input in the first page.



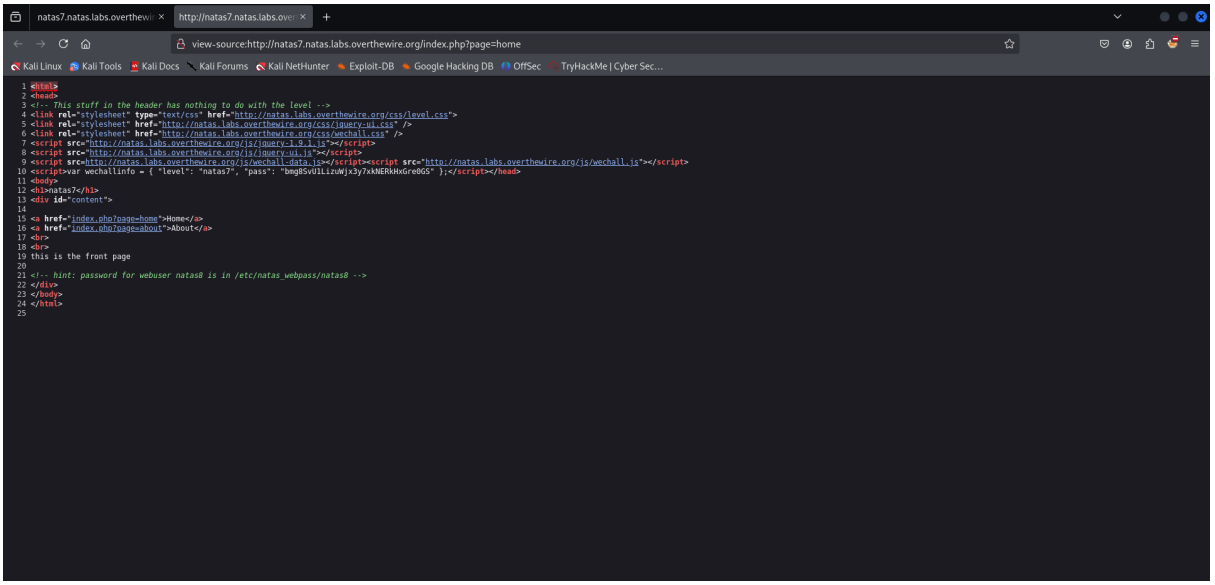
- Now the password flag is found, password for level 7 : *bmg8SvU1LizuWjx3y7xkNERkHxGre0GS*.

LEVEL 7:

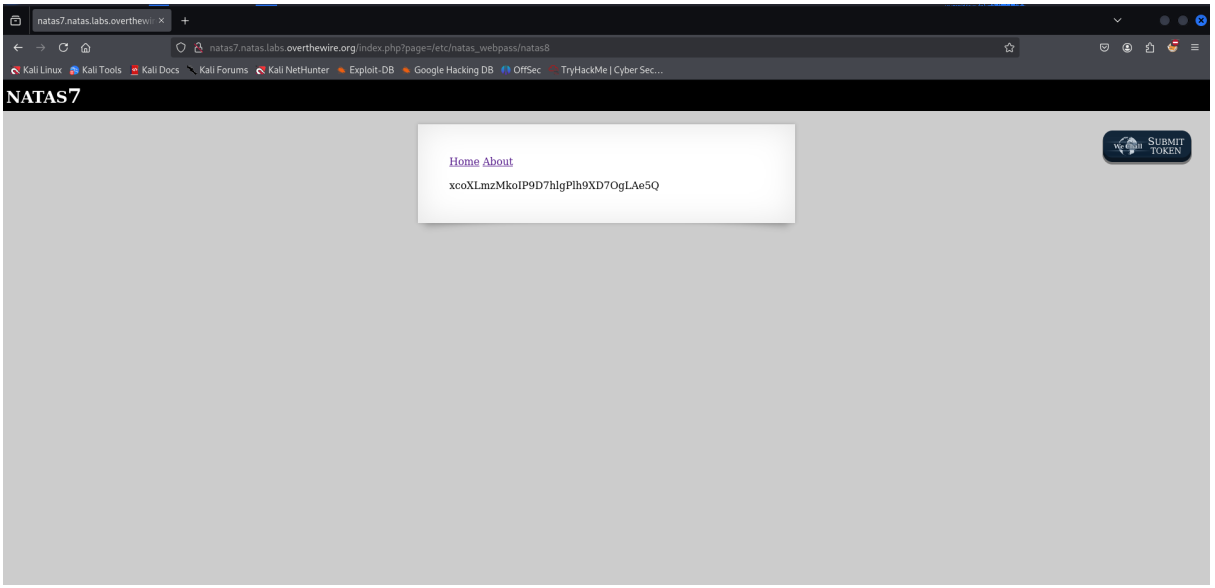
- Now, go to the url http://natas7.natas.labs.overthewire.org and login using "*natas7*" as username and the password found from level 6 to access level 7.



- In page source we find a hint for the flag, it say that flag can be found in "*/etc/natas_webpass/natas8*".



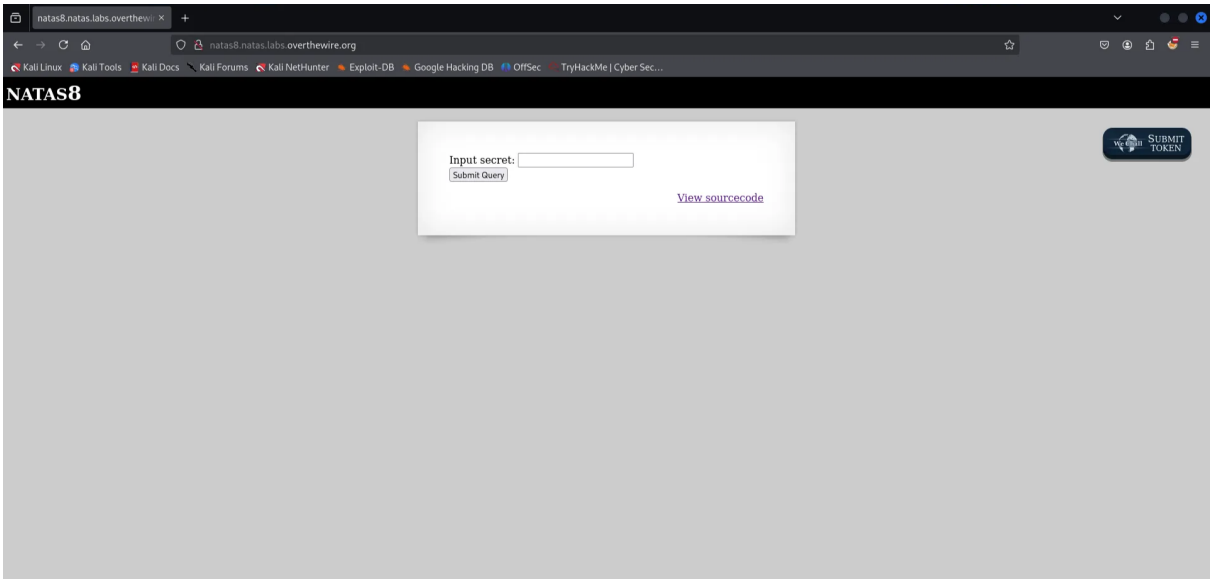
- In the URL of the homepage, it gets a parameter “?page=home”. Now try replacing “home” with *“/etc/natas_webpass/natas8”.*



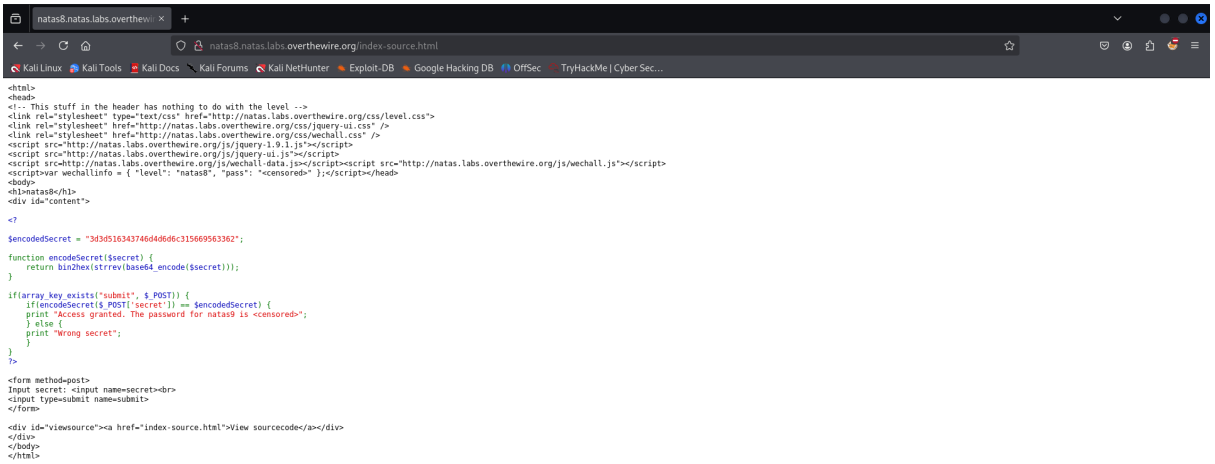
- Now the password flag for level 8 is found.
- Password for level 8 : *xcoXLmzMkoIP9D7hlgPlh9XD7OgLAe5Q.*

LEVEL 8:

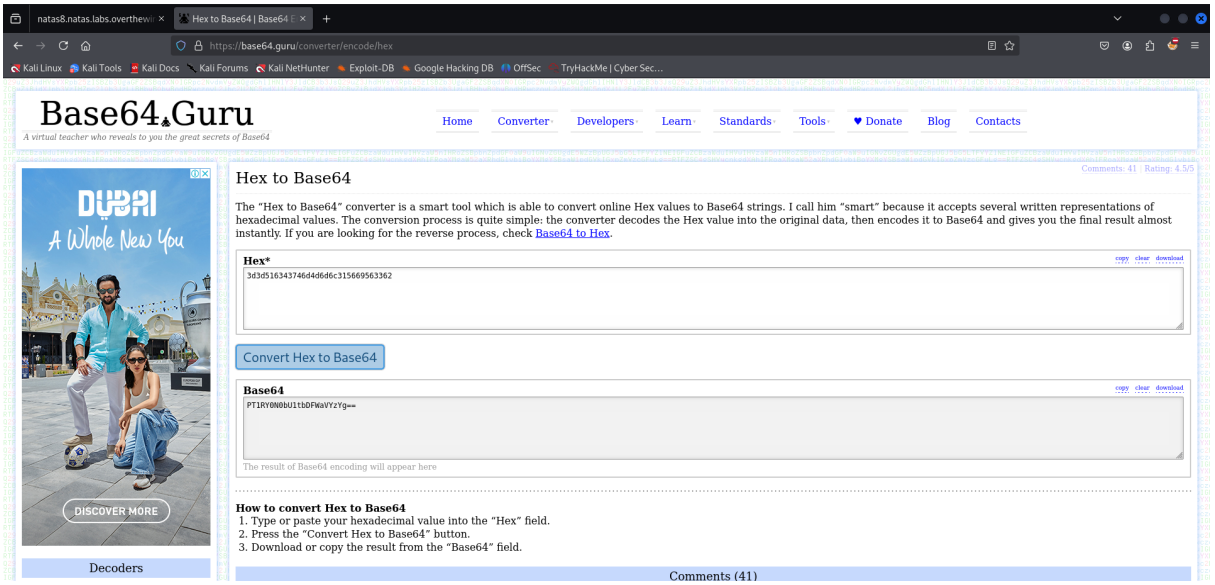
- Now, go to the url http://natas8.natas.labs.overthewire.org and login using *“natas8”* as username and the password found from level 7 to access level 8.



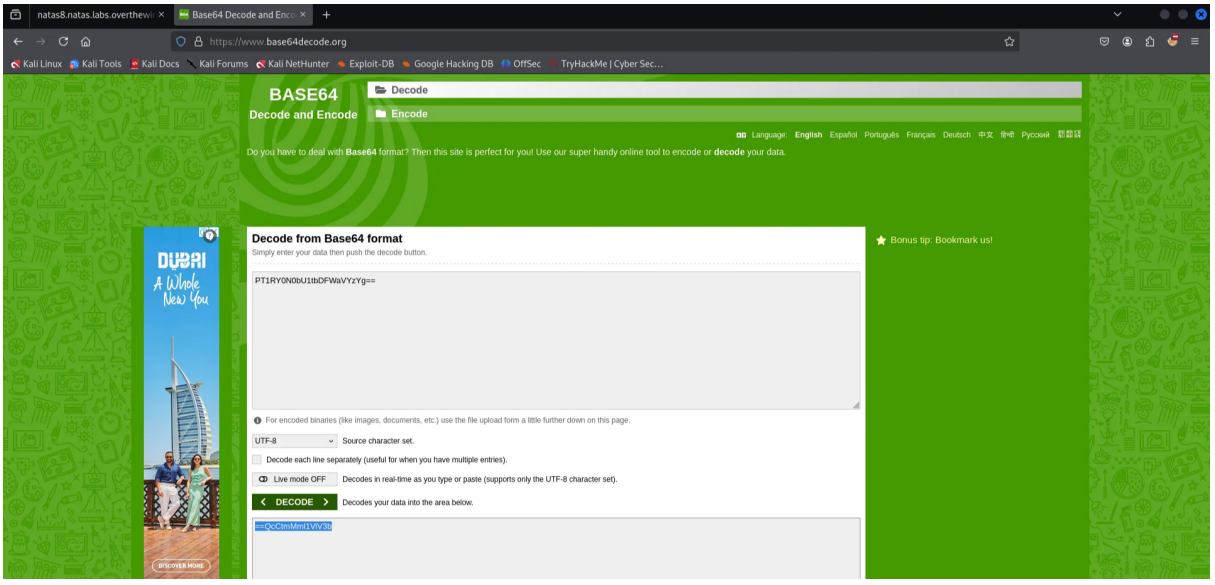
- Now, view the sourcecode of the page using the hyperlink in the page for hint.



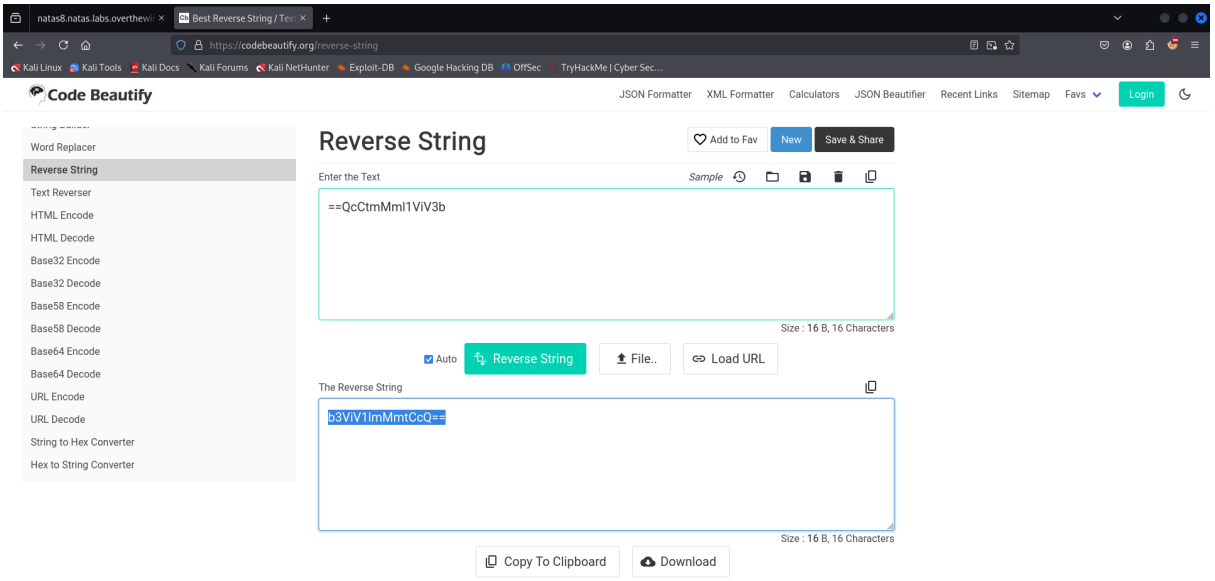
- Here, the input is goes through these conversions `bin2hex(strrev(base64_encode( $secret )))` and compared with `$encodedSecret` , the value of `$encodedSecret` is also given.
- Now try to reverse the coversions to the value of `$encodedSecret` .
- First Hexadecimal to base64, we get PT1RY0N0bU1tbDFWaVYzYg==.



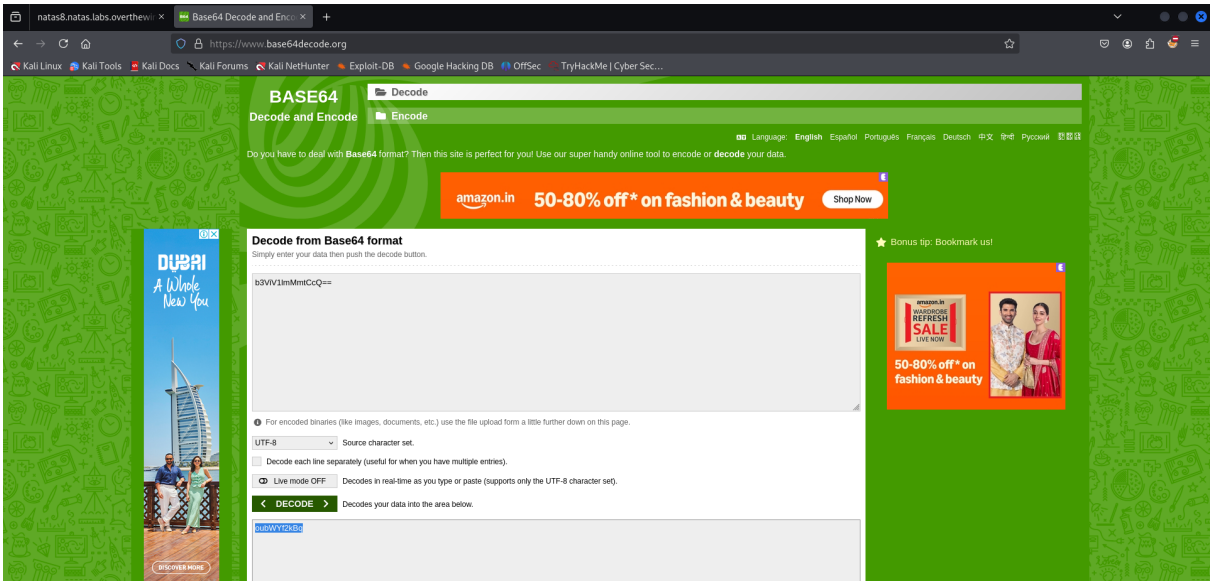
- Now, decode it with base64 decoder we get ==QcCtmMml1ViV3b.



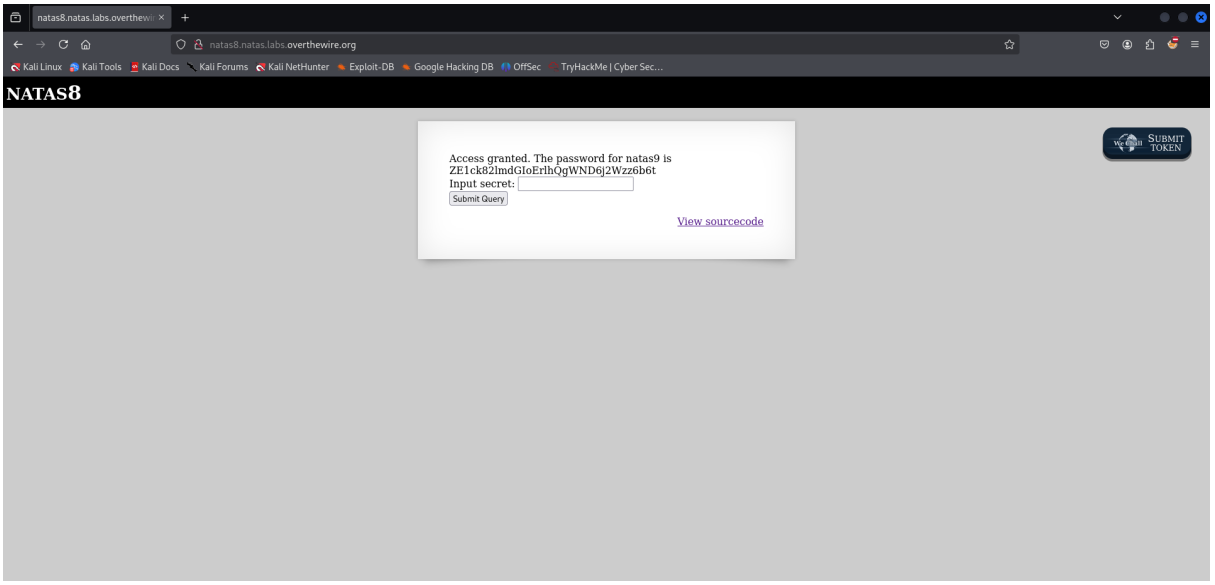
- Then, reverse the cipher text we got above, we get b3ViV1lmMmtCcQ==.



- Now again decode the cipher text and we get oubWYf2kBq.



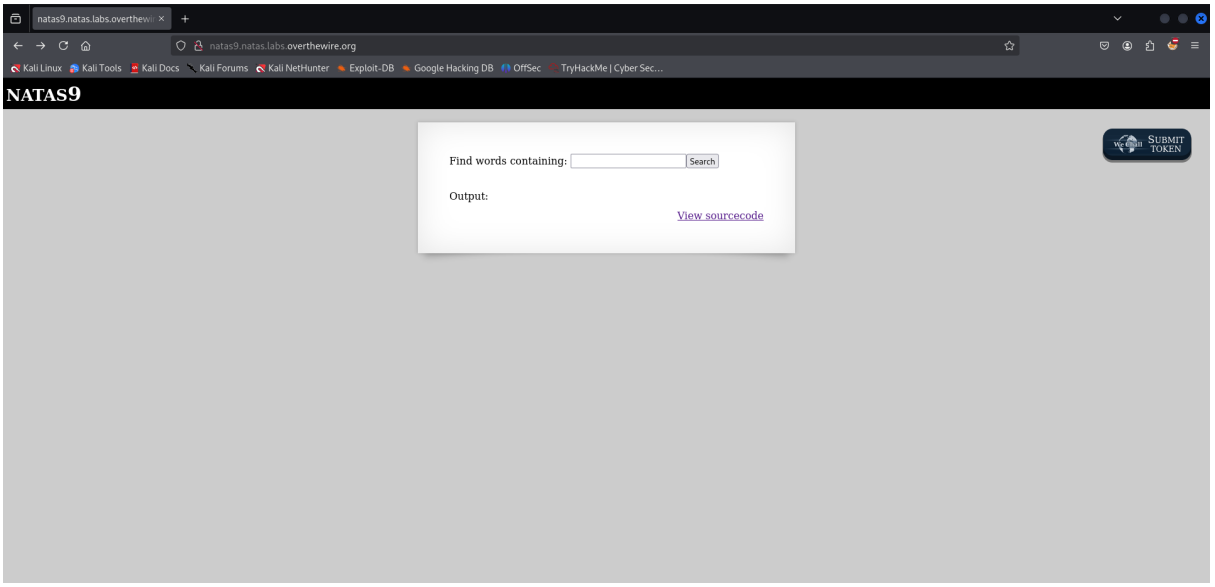
- Now input the above derived string as secret.



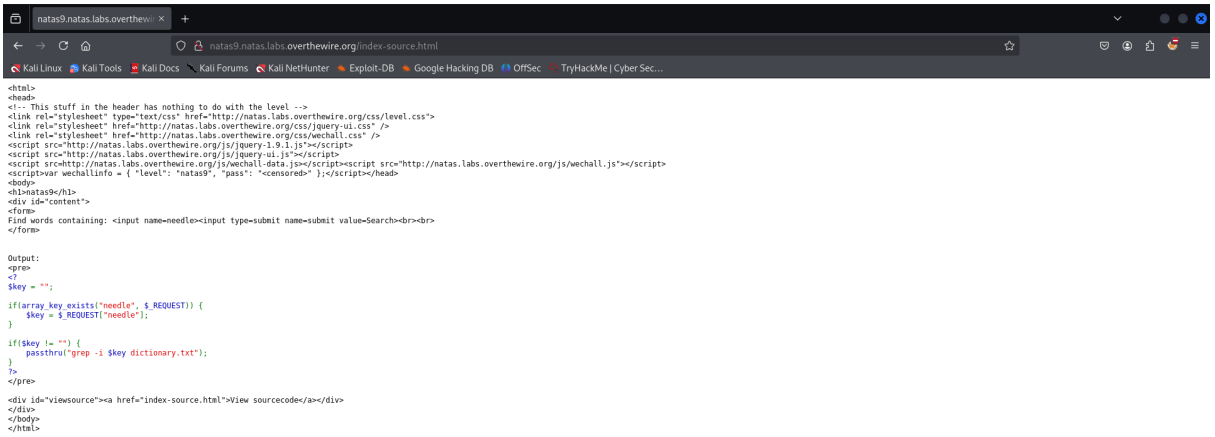
- Now, we got the flag, password for level 9 : *ZE1ck82lmdGIoErlhQgWND6j2Wzz6b6t*.

LEVEL 9:

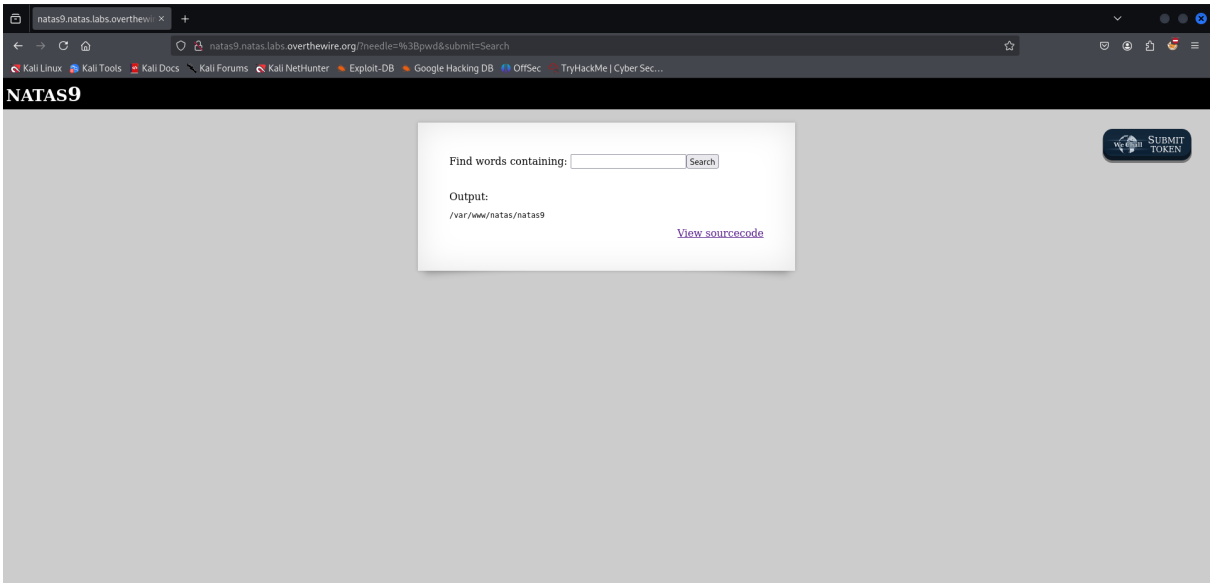
- Now, go to the url http://natas9.natas.labs.overthewire.org and login using “*natas9*” as username and the password found from level 8 to access level 9.



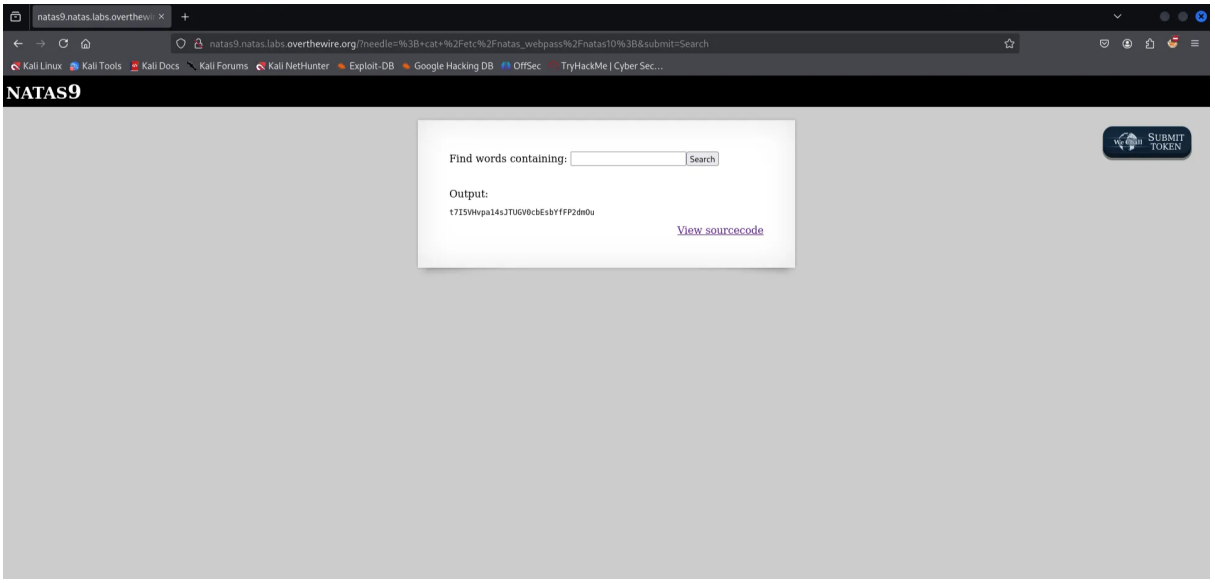
- Now, view the sourcecode of the page using the hyperlink in the page for hint.



- We can see that page executes grep command in a file “dictionary.txt”.
- Now try command injection with “; pwd”.



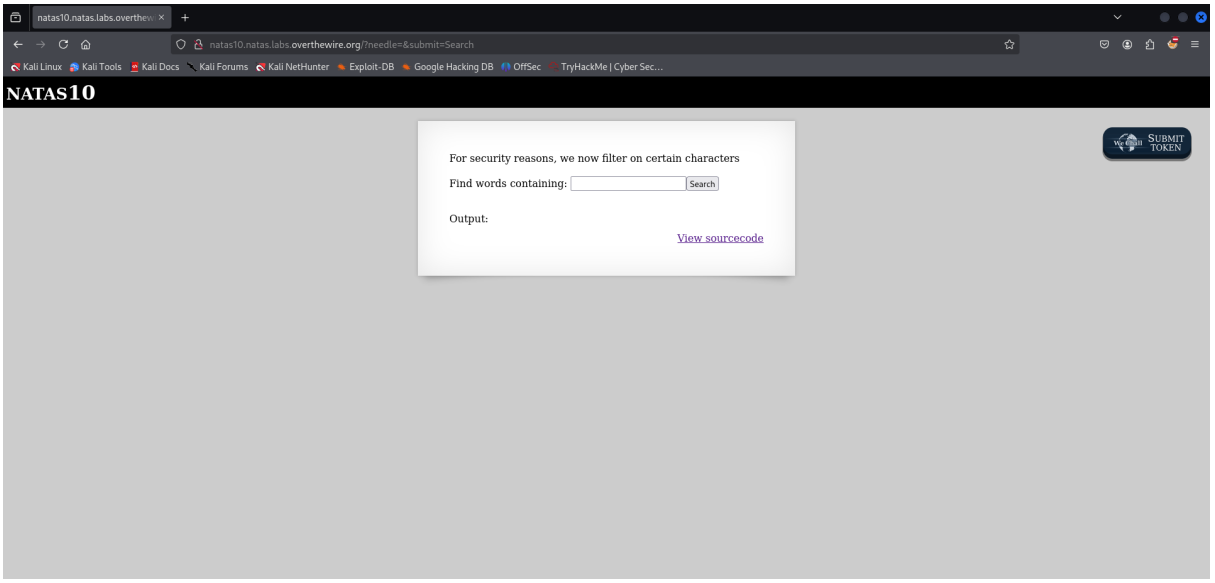
- Since we know that “*/etc/natas_webpass/natas10*” contains the flag.
- Try “; cat /etc/natas_webpass/natas10;”.



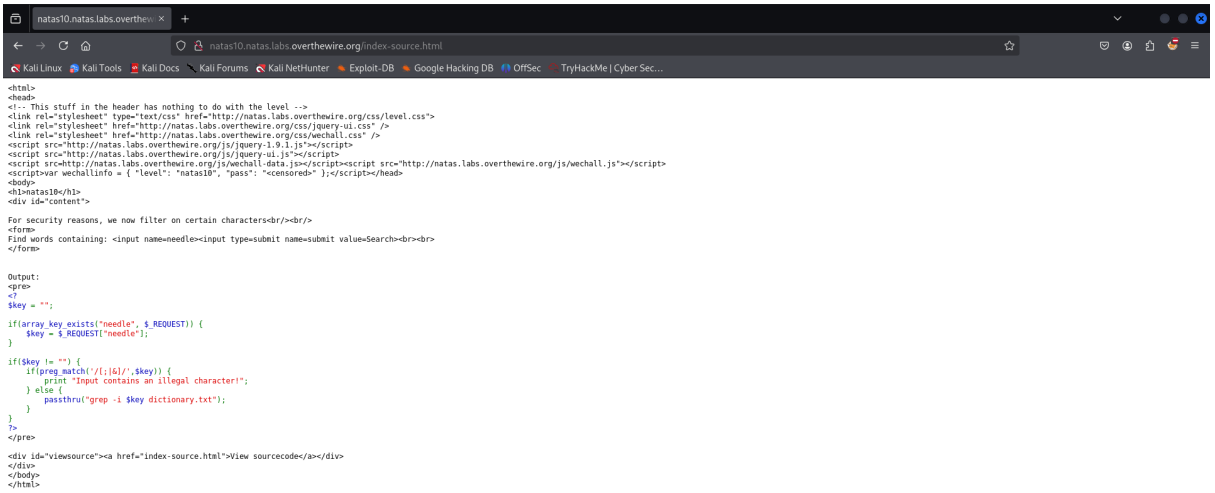
- Now, we got the flag, password for level 10 : *t7I5VHvpa14sJTUGV0cbEsbYfFP2dmOu*.

LEVEL 10:

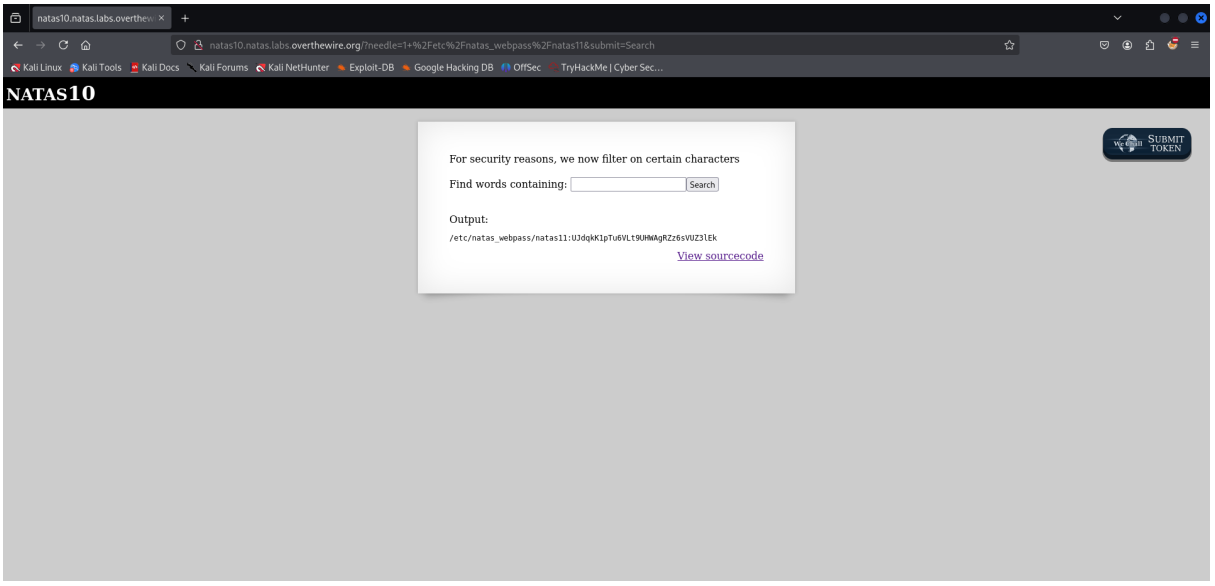
- Now, go to the url http://natas10.natas.labs.overthewire.org and login using “*natas10*” as username and the password found from level 9 to access level 10.



- Now, view the sourcecode of the page using the hyperlink in the page for hint.



- The command used in previous level doesn't work here since it filters ; & | .
- So lets try "1 */etc/natas_webpass/natas11*".



- Now, we got the flag, password for level 11 : *UJdqkK1pTu6VLt9UHWAgRZz6sVUZ3lEk.*