

Project Report

Overthewire Natas

LEVEL 0:

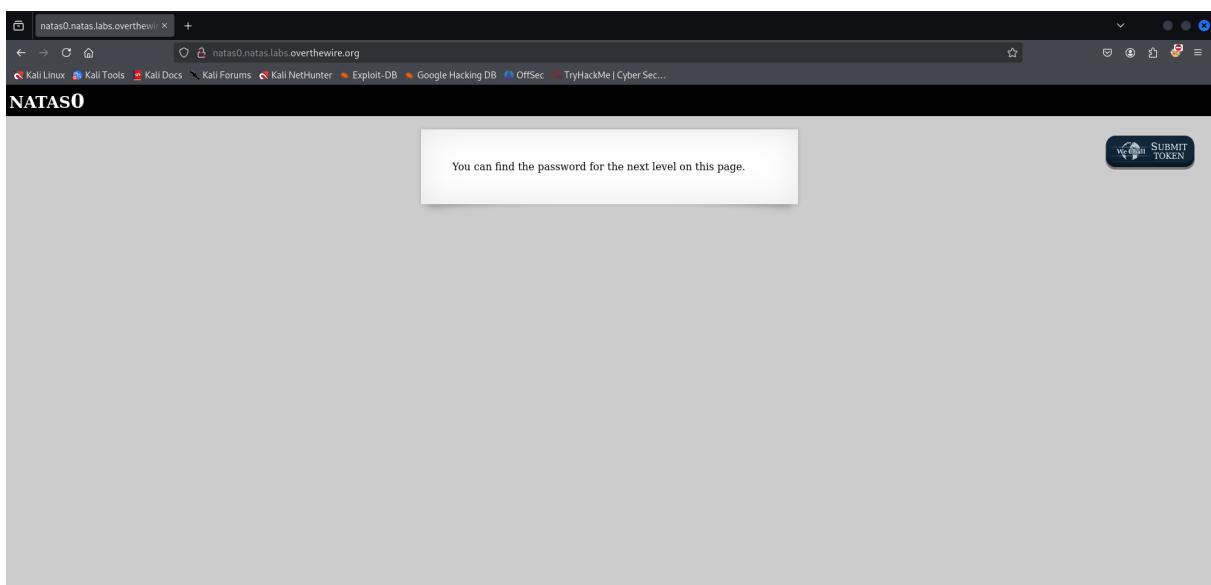
Start here:

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.

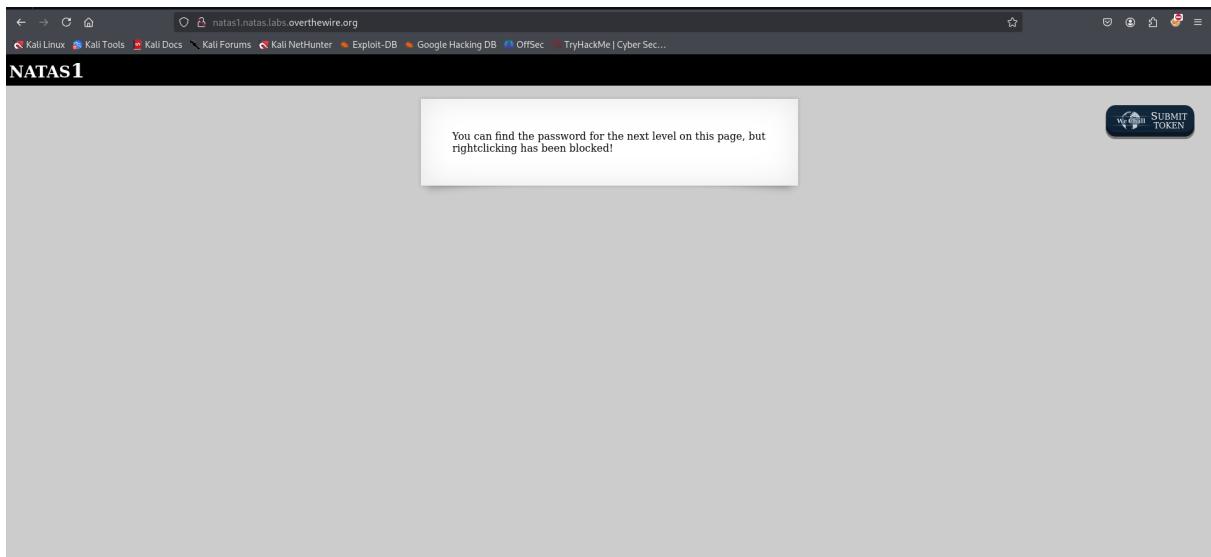


- Now, view the source code of the webpage where the password flag for the next level is in comment.
- Password for level 1: *OnzCigAq7t2iALyvU9xcHlYN4MlkIwlq*.

```
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="http://natas.labs.overthewire.org/css/level.css"/>
5 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-1.3.1.css"/>
6 <link rel="stylesheet" href="http://natas.labs.overthewire.org/js/jquery-1.3.1.js"/>
7 <script src="http://natas.labs.overthewire.org/js/jquery-1.3.1.js"></script>
8 <script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
9 <script src="http://natas.labs.overthewire.org/js/wechallinfo.js"></script>
10 <script>var wechallinfo = { 'level': 'natas0', 'pass': 'natas0' };</script></head>
11 <body>
12 <natas0/>
13 <div id="content">
14 You can find the password for the next level on this page.
15 ...
16 <!--The password for natas1 is 0nztLigq7t2iALyx09xCHlY4M(klwlg -->
17 </div>
18 </body>
19 </html>
```

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.

```

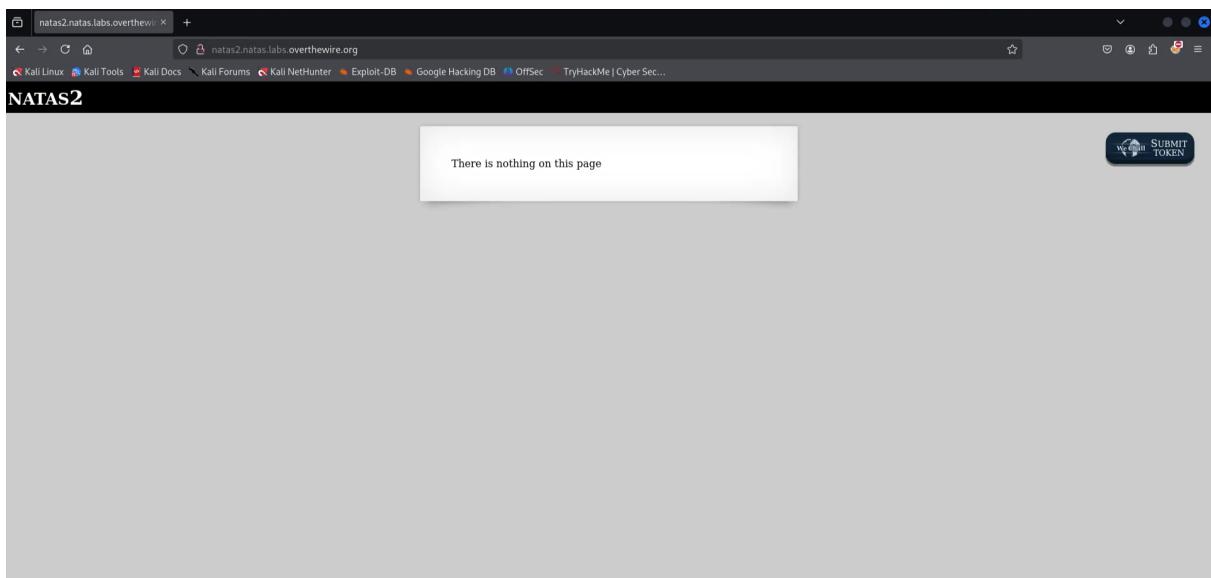
1 <html>
2 <head>
3 <!-- This stuff in the header has nothing to do with the level -->
4 <link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css"/>
5 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/level2.css" />
6 <script src="http://natas.labs.overthewire.org/jquery-1.9.1.js"></script>
7 <script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
8 <script src="http://natas.labs.overthewire.org/jscallback-data.js"></script>
9 <script>var wechallinfo = { 'level': 'natas1', 'pass': '0nzCipAq71zJLyU9uChlYn4MtkIwIq' };</script></head>
10 <body oncontextmenu='javascript:alert("right clicking has been blocked!");return false;'>
11 <div id="content">
12 <div>natas</div>
13 <div id="content">
14 You can find the password for the
15 next level on this page, but rightclicking has been blocked!
16
17 --> The password for natas2 is TguMNxKo1DSa1tujBLuZJnDUICcUAPII -->
18 </div>
19 </body>
20 </html>
21
22

```

- Now, view the source code of the webpage where the password flag for the next level is in comment.
- Password for level 2 : *TguMNxKo1DSa1tujBLuZJnDUICcUAPII*

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 , this shows that there is a directory named files.
- Now, try traversing to the "/files" directory.

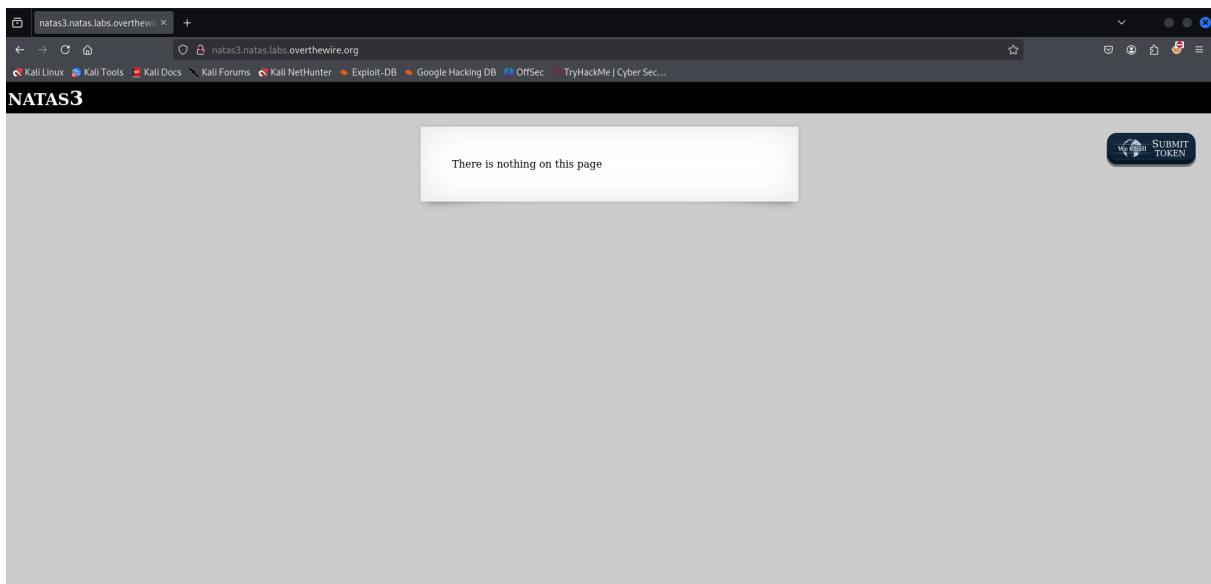
Name	Last modified	Size	Description
.		-	Parent Directory
pixel.png	2024-09-19 07:03	303	
users.txt	2024-09-19 07:03	145	

Apache/2.4.58 (Ubuntu) Server at natas2.natas.labs.overthewire.org Port 80

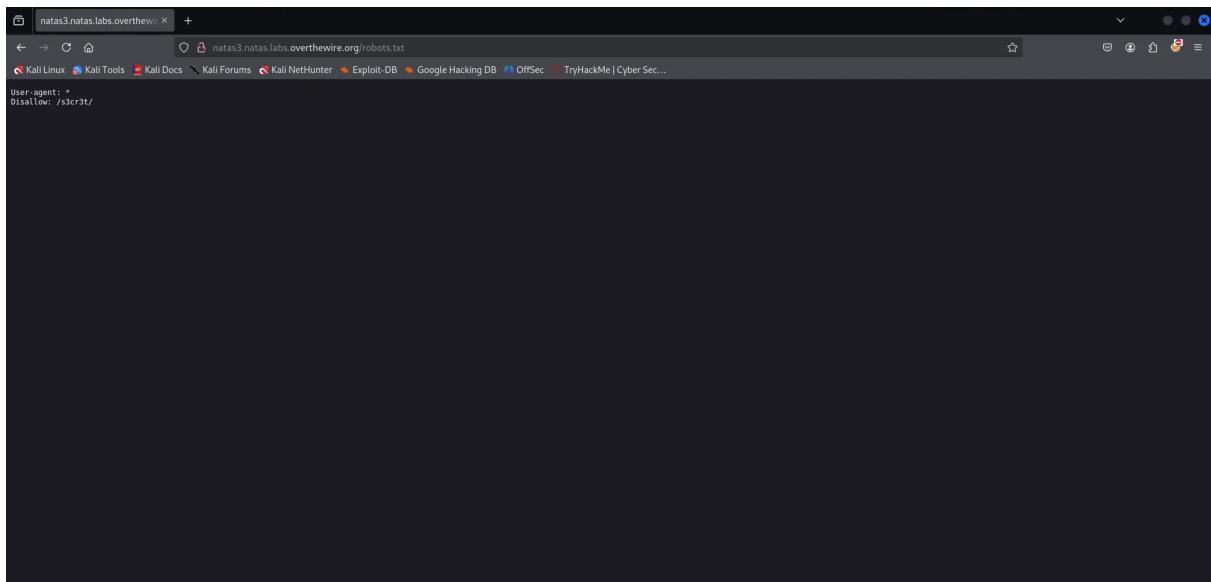
- We can see there is a text file named "users.txt" and contains the password for level 3 in it.
- Password for level 3 : *3gqisGdR0pj6tpkDKdIW02hSvchLeYH*.

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.

Index of /s3cr3t

Name	Last modified	Size	Description
Parent Directory		-	
users.txt	2024-09-19 07:03	40	

Apache/2.4.58 (Ubuntu) Server at natas3.natas.labs.overthewire.org Port 80

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.

NATAS4

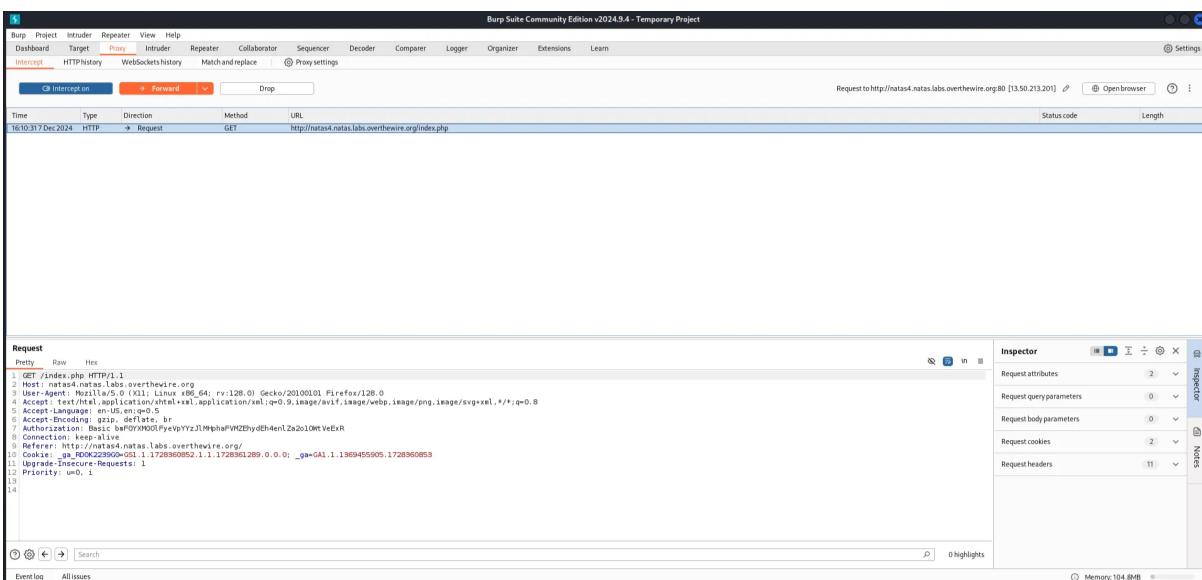
Access disallowed. You are visiting from "" while authorized users should come only from "http://natas5.natas.labs.overthewire.org/"

[Refresh page](#)

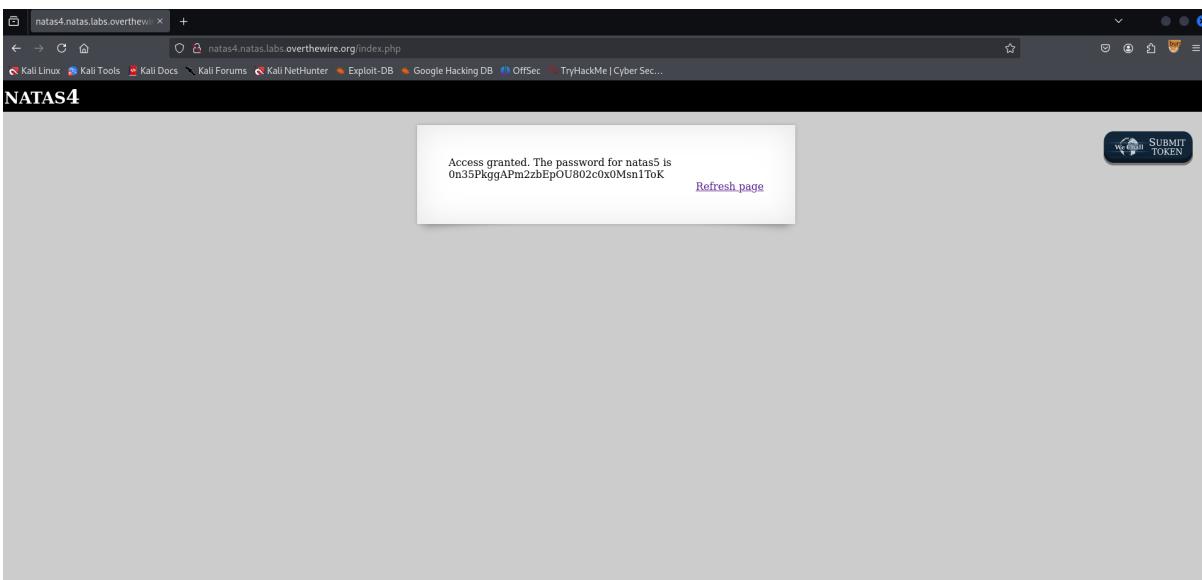
[SUBMIT TOKEN](#)

- 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.

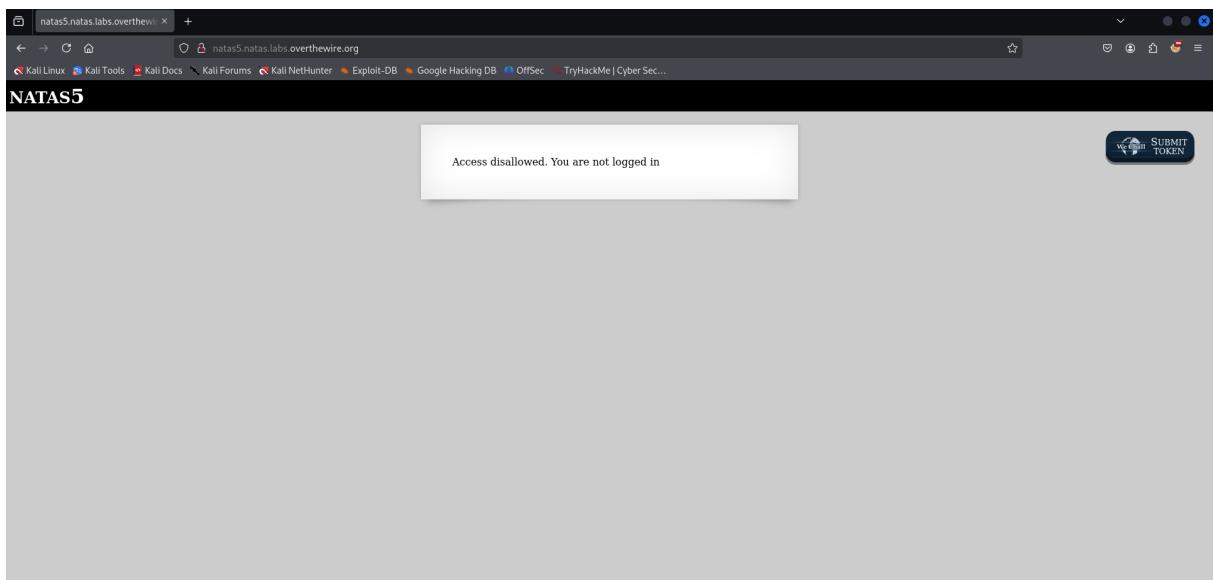


- Now, check for Referer parameter and alter it to "<http://natas5.natas.labs.overthewire.org/>" and forward the request.
 - Now the password flag is available in the webpage.
 - Password for level 5 : *On35PkqqAPm2zbEpOU802c0x0Msn1ToK*.

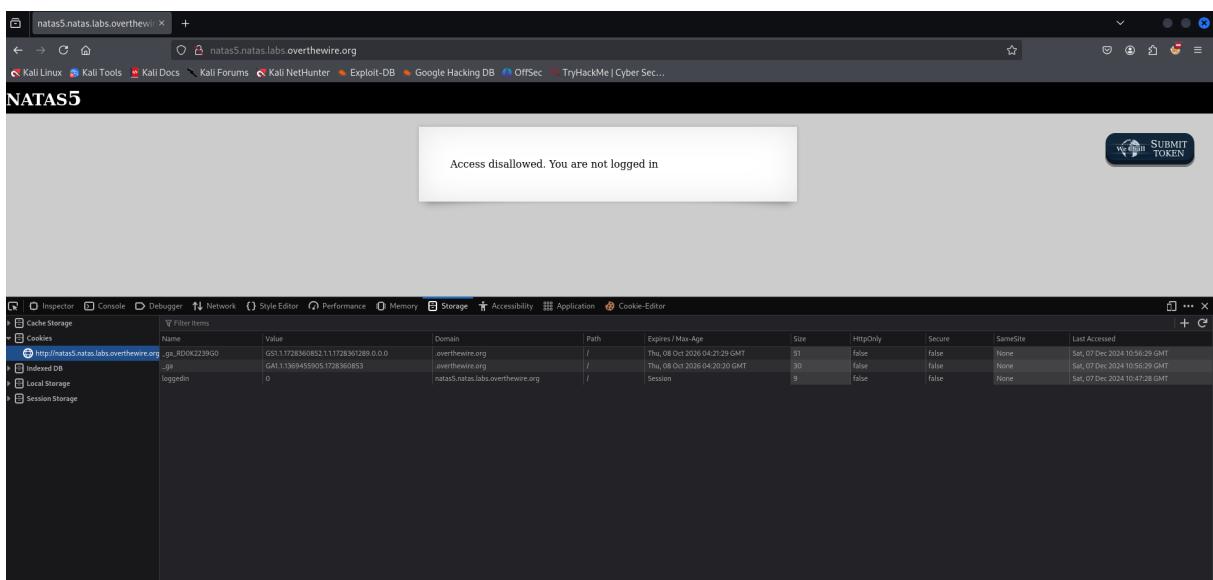


LEVEL 5:

- 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.

The screenshot shows the Firefox developer tools Network tab. A successful POST request to `http://natas5.natas.labs.overthewire.org` is listed. The response body contains the message: "Access granted. The password for natas6 is 0RoJwHdSKWFTYR5WuiAewauSuNaBXned". To the right of the response, there is a "SUBMIT TOKEN" button.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
<code>_ga_RD0K22396G0</code>	<code>GAI11728360852.11728361289.0.0</code>	<code>overthewire.org</code>	<code>/</code>	<code>Thu, 08 Oct 2026 04:21:29 GMT</code>	<code>51</code>	<code>false</code>	<code>false</code>	<code>None</code>	<code>Sat, 07 Dec 2024 10:58:17 GMT</code>
<code>_gat</code>	<code>GAI1159645905.1728360853</code>	<code>overthewire.org</code>	<code>/</code>	<code>Thu, 08 Oct 2026 04:20:20 GMT</code>	<code>30</code>	<code>false</code>	<code>false</code>	<code>None</code>	<code>Sat, 07 Dec 2024 10:58:17 GMT</code>
<code>loggedIn</code>	<code>1</code>	<code>natas5.natas.labs.overthewire.org</code>	<code>/</code>	<code>session</code>	<code>9</code>	<code>false</code>	<code>true</code>	<code>None</code>	<code>Sat, 07 Dec 2024 10:58:18 GMT</code>

- 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.

The screenshot shows the Firefox developer tools Network tab. A successful POST request to `http://natas6.natas.labs.overthewire.org` is listed. The response body contains an input field labeled "Input secret:" with a placeholder "Submit Query" and a link "View sourcecode". To the right of the response, there is a "SUBMIT TOKEN" button.

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

```

<html>
<head>
</head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/natas6.css" />
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
<script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
<script>var wechallInfo = {'level': 'natas6', 'pass': '<censored>'};</script></head>
<body>
<h1>natas6</h1>
<div id="content">
<?
include "includes/secret.inc";
if(array_key_exists('submit', $_POST)) {
    if($secret == $_POST['secret']) {
        print "Access granted. The password for natas7 is <censored>";
    } else {
        print "Wrong secret";
    }
}
?>
<form method="post">
    Input secret: <input name=secret><br>
    <input type=submit name=submit>
</form>
<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>

```

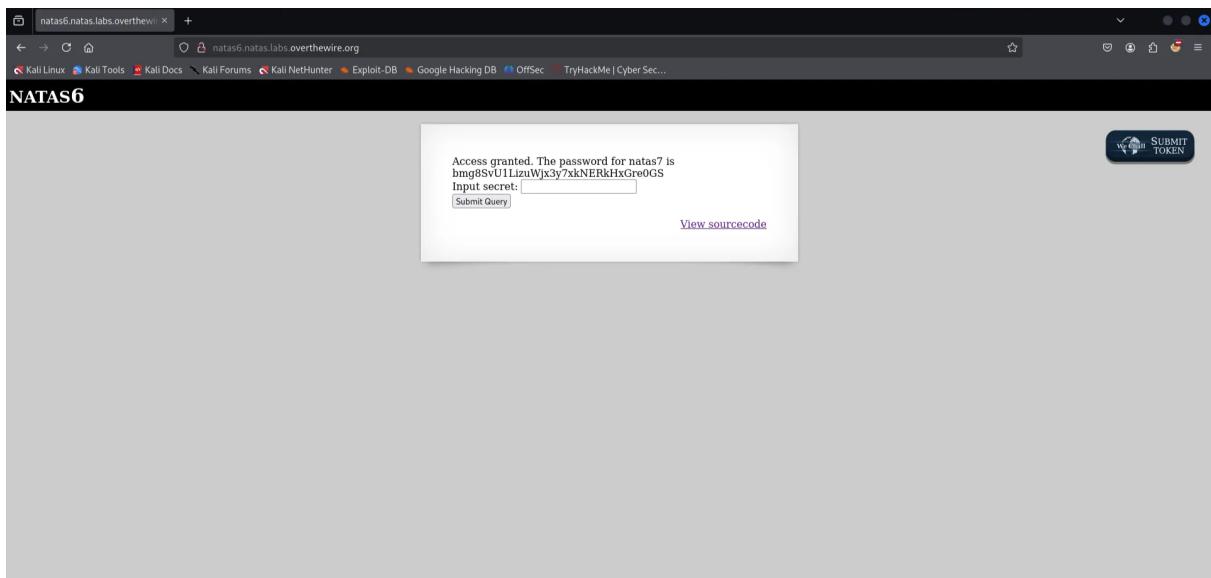
- We can see that the secret is located in "*includes/secret.inc*", traverse to the directory.
- Now, we can see a empty webpage with no clue. So view page source to identify any hint.

```

1 <?
2 $secret = "FOEIUWGHFEEUHOFUOIU";
3 ?>
4

```

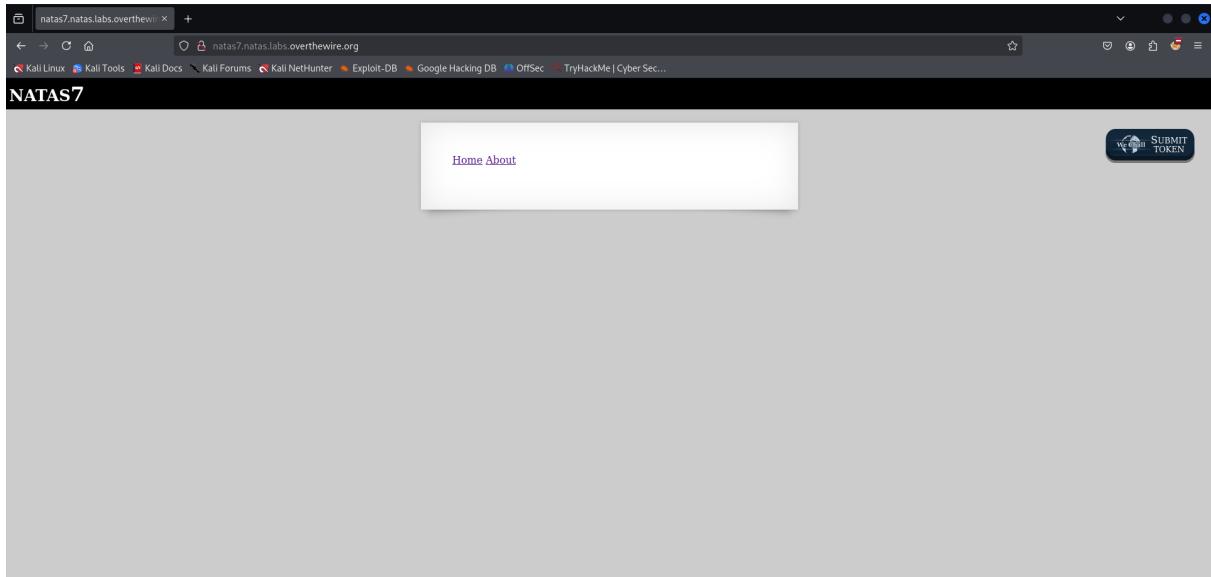
- Now we got the secret "FOEIUWGHFEEUHOFUOIU", try this as input in the first page.



- 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.



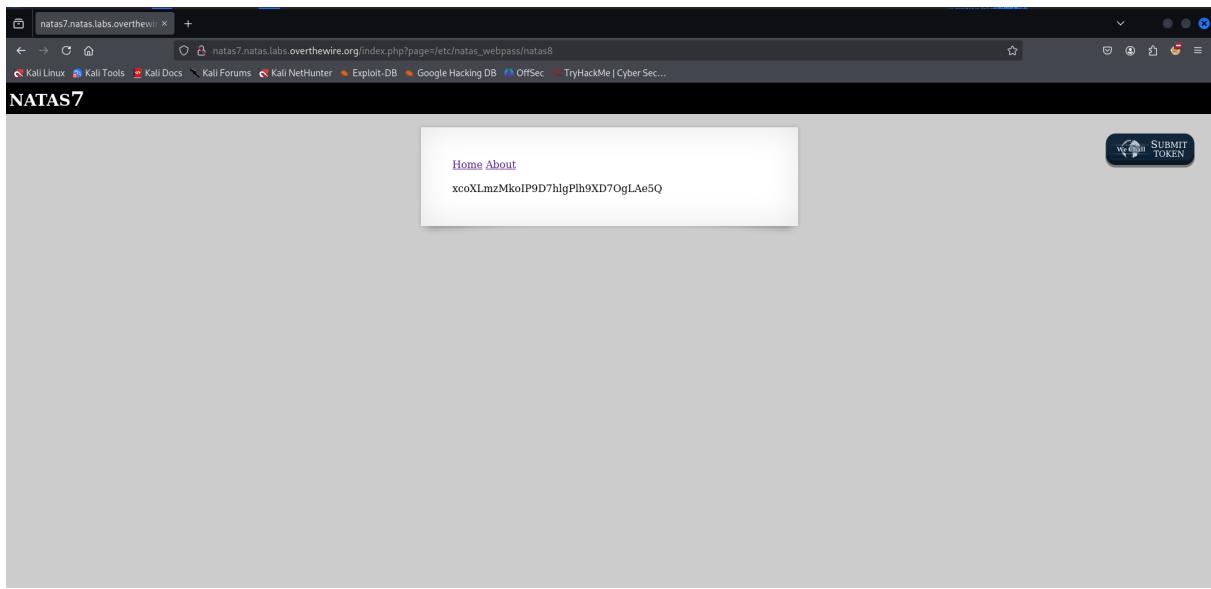
- In page source we find a hint for the flag, it say that flag can be found in "/etc/natas_webpass/natas8".

```

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="http://natas.labs.overthewire.org/css/level.css"/>
5   <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/level_01.css" />
6   <script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
7   <script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
8   <script src="http://natas.labs.overthewire.org/js/wechallinfo.js"></script>
9   <script src="http://natas.labs.overthewire.org/js/wechallinfo.js"></script>
10  <script>var wechallinfo = { 'level': 'natas8', 'pass': 'bmgBSwrlizWjx3y7xNERkhGrc0GS' };</script></head>
11 <body>
12   <h1>natas7</h1>
13   <div id="content">
14     <a href="index.php?page=home">Home</a>
15     <a href="index.php?page=about">About</a>
16   </div>
17 <br>
18 <br>
19 this is the front page
20
21 <!-- hint: password for webuser natas8 is in /etc/natas_webpass/natas8 -->
22 </div>
23 </body>
24 </html>
25

```

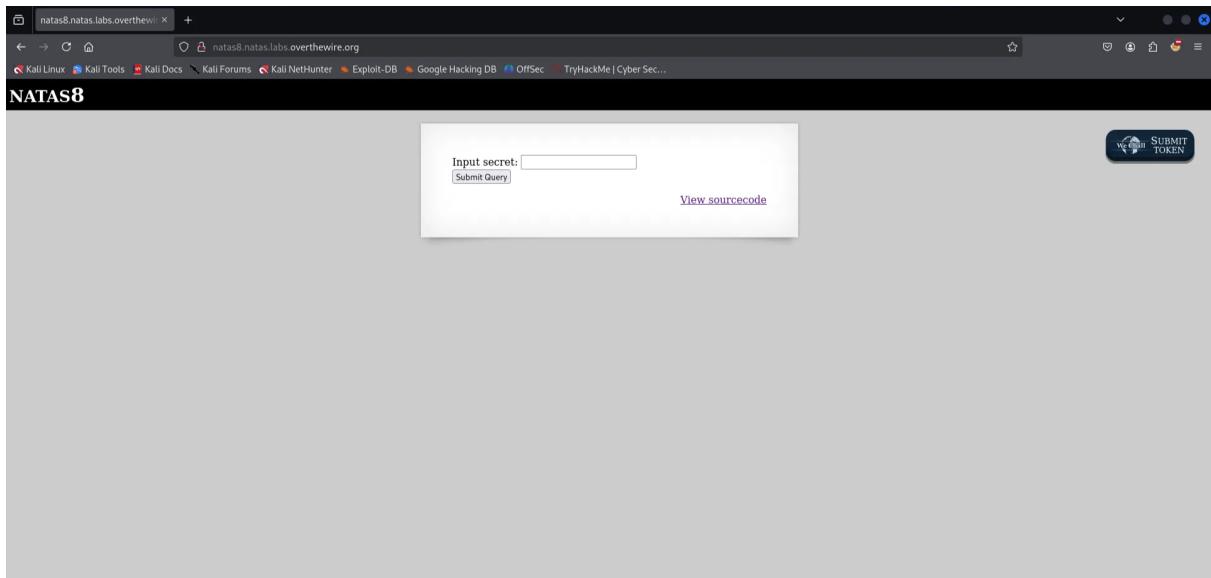
- In the URL of the homepage, it gets a parameter "?page=home". Now try replacing "home" with "/etc/natas_webpass/natas8".



- 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.

```

natas8.natas.labs.overthewire.org + 
natas8.natas.labs.overthewire.org/index-source.html
natas8.natas.labs.overthewire.org/index-source.html
natas8.natas.labs.overthewire.org/index-source.html

<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
<script src="http://natas.labs.overthewire.org/js/wechal.js"></script>
<script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script>
<script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
<?>
$encodedSecret = "3d3d51634374bd4d96d6c315669563362";
function encodeSecret($secret) {
    return bin2hex(strrev(base64_encode($secret)));
}
if(isset($_POST['submit'])) {
    if($encodedSecret == $_POST['secret']) {
        print "Access granted. The password for natas9 is <censored>";
    } else {
        print "Wrong secret";
    }
}
<form method=post>
Input secret: <input name=secret><br>
<input type=submit name=submit>
</form>
<div id=viewsource><a href="index-source.html">View sourcecode</a></div>
</body>
</html>

```

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

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

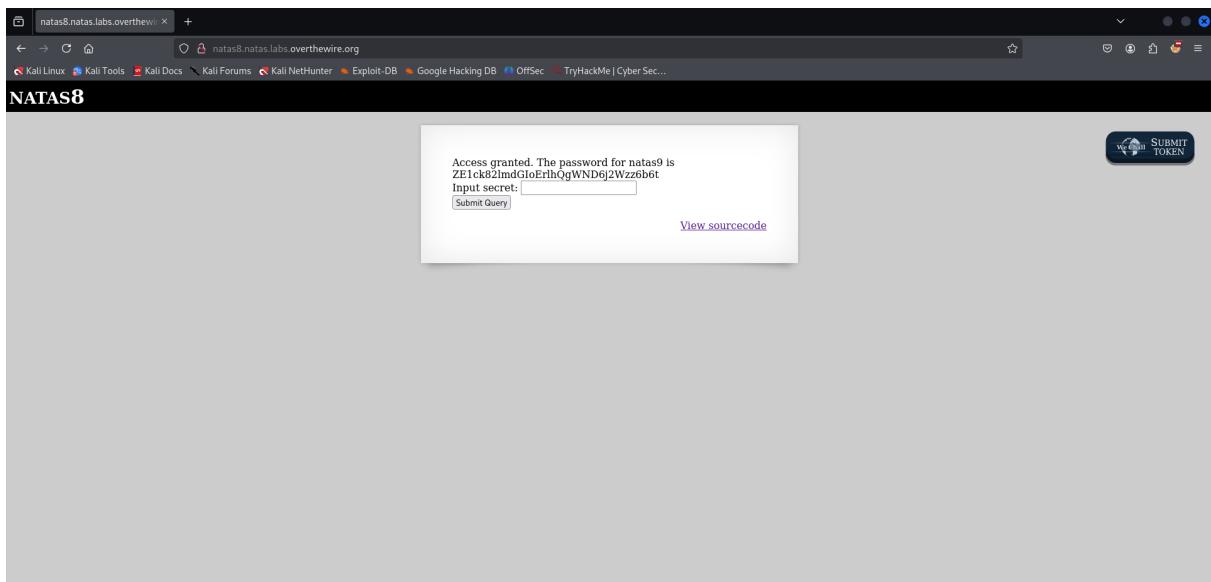
- Then, reverse the cipher text we got above, we get b3ViV1lmMmtCcQ==.

The screenshot shows the 'Reverse String' tool on the Code Beautify website. The input field contains the string ==QcCtmMml1ViV3b. The output field shows the reversed string b3ViVi1mMmtCcQ==. The interface includes buttons for 'Auto', 'Reverse String', 'File...', 'Load URL', 'Copy To Clipboard', and 'Download'.

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

The screenshot shows the 'Decode from Base64 format' tool on the Base64 Decode and Encode website. The input field contains the string b3ViVi1mMmtCcQ==. The output field shows the decoded string oubWYf2kBq. The interface includes options for 'Source character set' (UTF-8), 'Decode each line separately', and 'Live mode OFF'. There is also an advertisement for Amazon.in.

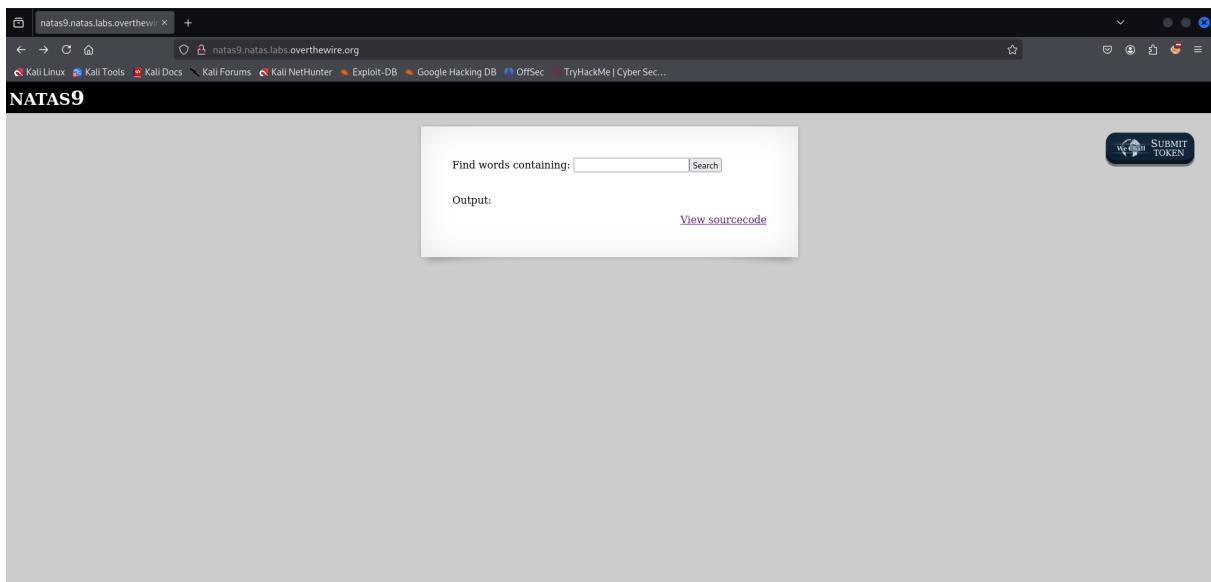
- Now input the above derived string as secret.



- Now, we got the flag, password for level 9 :
ZE1ck82lmdGloErlhQgWND6j2Wzz6b6t.

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.

```

<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
<script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script>
<script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
<script>var wechallInfo = { 'level': 'natas9', 'pass': '<!--censored-->' };</script>
</head>
<body>
<h1>natas9</h1>
<div id="content">
<form>
Find words containing: <input name=needle><input type=submit name=submit value=Search><br><br>
</form>

```

Output:

```

<pre>
$key = '';
if(array_key_exists('needle', $_REQUEST)) {
    $key = $_REQUEST['needle'];
}

if($key != "") {
    passthru("grep -i $key dictionary.txt");
}
</pre>

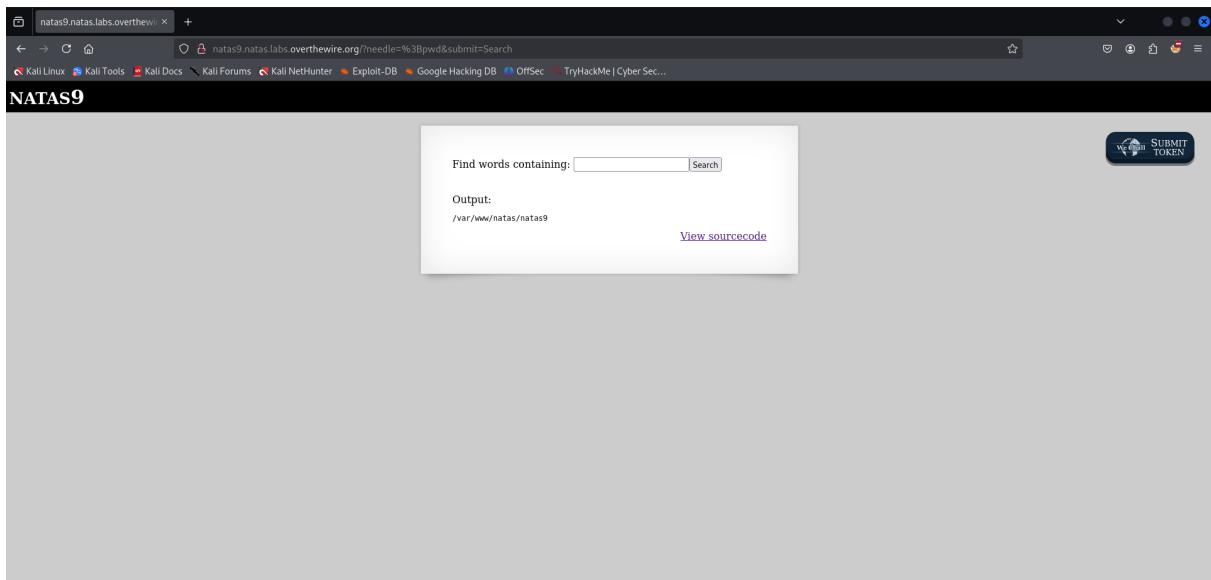
```

```

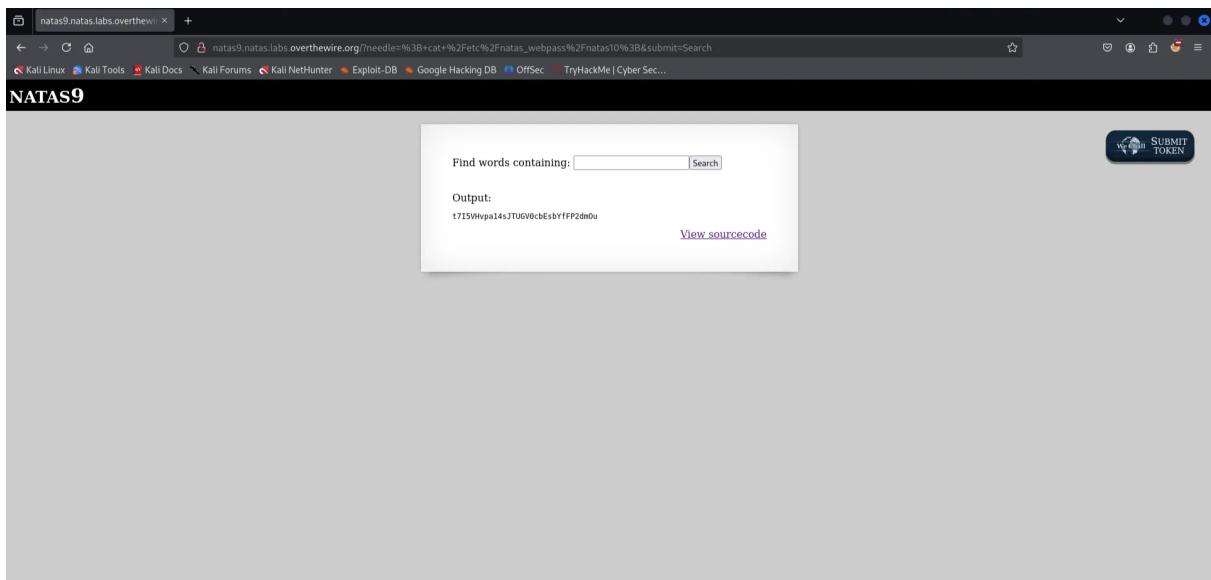
<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>

```

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



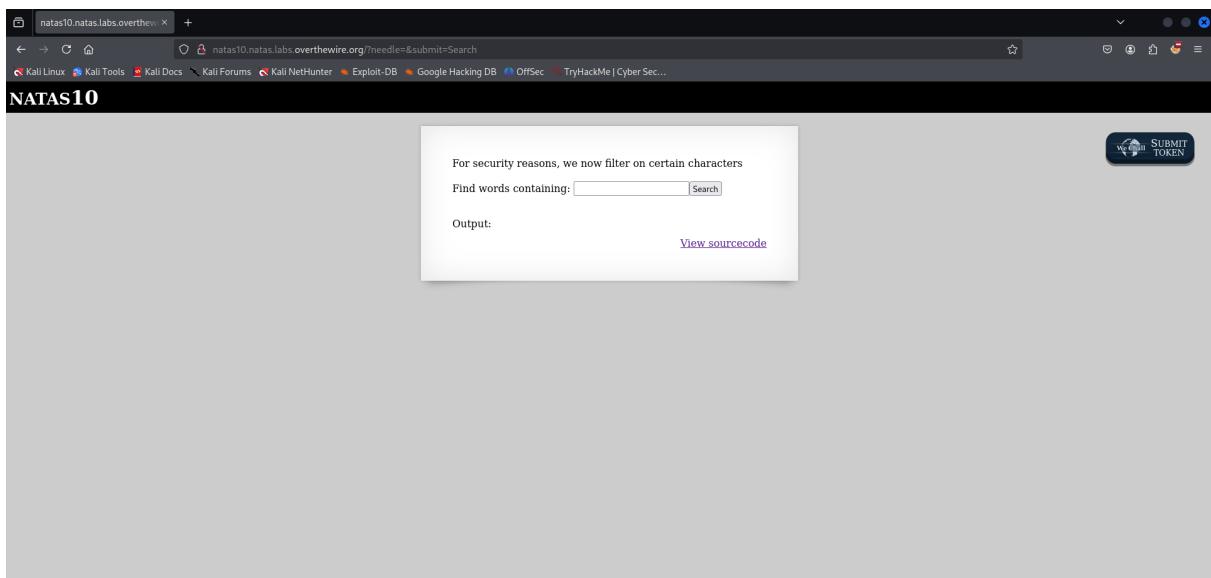
- Since we know that “/etc/natas_webpass/natas10” contains the flag.
- Try “; cat /etc/natas_webpass/natas10;”.



- 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.

```

<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/natas10.css" />
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
<script src="http://natas.labs.overthewire.org/js/wechall-data.js"><script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script></script>
<script>var wechallInfo = { 'level': 'natas10', 'pass': '<censored>' };</script></head>
<body>
<h1>natas10</h1>
<div id="content">
    For security reasons, we now filter on certain characters<br/><br/>
    <form>
        Find words containing: <input name="needle"><input type="submit" name="submit" value="Search"><br/><br/>
    </form>
    <pre>
        <?php
        $key = '';
        if(array_key_exists("needle", $_REQUEST)) {
            $key = $_REQUEST['needle'];
        }
        if($key != "") {
            if(preg_match('/[|;|&]/', $key)) {
                print "Input contains an illegal character!";
            } else {
                passthru("grep -i $key dictionary.txt");
            }
        }
    </pre>
    <div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>

```

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

NATAS10

For security reasons, we now filter on certain characters

Find words containing:

Output:

```
/etc/natas_webpass/natas11:UJdqkK1pTu6VLt9UHWAgrRZz6sVUZ3IEk
```

[View sourcecode](#)

- Now, we got the flag, password for level 11 : **UJdqkK1pTu6VLt9UHWAgrRZz6sVUZ3IEk**.