

# OVER THE WIRE-NATAS

BASI REDDY ROHITH REDDY,

CB.EN.U4CYS21013.

## Level 0:

Given credentials to login to the web page. After logging in, inspect the page by either right clicking and selecting inspect page or by **“ctrl+u”**. In the source code of the page, you will find the password for level1 commented. Copy it and get going to the next level.

```
<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": "natas0", "pass": "natas0" };</script></head>
<body>
<h1>natas0</h1>
<div id="content">
You can find the password for the next level on this page.

<!--The password for natas1 is g9D9cREhslqBKtcA2uocGHPfMZVzeFK6 -->
</div>
</body>
</html>
```

## Level 1:

This also same as Level0. Just that after logging in the web page, you will get a message saying right click is banned on the page. So, for checking the page source, you should press **“ctrl+u”** instead of right clicking. And then you can inspect the page code where you can find the password for the nextlevel commented. Copy the password and login to next level.

```
<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": "natas1", "pass": "g9D9cREhslqBKtcA2uocGHPfMZVzeFK6" };</script></head>
<body oncontextmenu="javascript:alert('right clicking has been blocked!');return false;">
<h1>natas1</h1>
<div id="content">
You can find the password for the
next level on this page, but rightclicking has been blocked!

<!--The password for natas2 is h4ubbcXrWqsTo7GgnnUMLppXbOogfBZ7 -->
</div>
</body>
</html>
```

## Level 2:

In this level, there is no password in the page source. Instead you will find a `<img src>`. Open the link of the image and you will find yourself at page “<http://natas2.natas.labs.overthewire.org/files/pixel.png>”.




```
<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": "natas2", "pass": "h4ubbcXrWqsTo7GGnnUMLppXb0ogfBZ7" };</script></head>
<body>
<h1>natas2</h1>
<div id="content">
There is nothing on this page

</div>
</body></html>
```

Now we know from the description in level0 that the passwords of the current and next level can be accessed from files inside the current level. So, let's open the files directory by modifying the page url to “<http://natas2.natas.labs.overthewire.org/files>”.

Here, after opening the modified url, you can see the following page.

## Index of /files

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">pixel.png</a>	2022-09-01 06:27	303	
 <a href="#">users.txt</a>	2022-09-01 06:27	145	

*Apache/2.4.52 (Ubuntu) Server at natas2.natas.labs.overthewire.org Port 80*

In this page, open the users.txt file where you can find the password for natas3. Copy it and get going to the next level.

```
# username:password
alice:BYNdCesZqW
bob:jw2ueICLVt
charlie:G5vCxkVV3m
natas3:G6ctbMJ5Nb4cbFwhpMPSvxGHhQ7I6W8Q
eve:zo4mJWyNj2
mallory:9urtcpzBmH
```

### Level 3:

This page is also similar to previous page, but instead, when you view the page source, you will not find any image, instead you will find a comment saying not even google will find the password. Which is a hint saying us to check robots file in the page url as google here refers as a robot. So, check the url

“natas3.natas.labs.overthewire.org/robots.txt”

```
<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": "natas3", "pass": "G6ctbMj5Nb4cbFwhpMPSvxGHhQ7I6W8Q" };</script></head>
<body>
<h1>natas3</h1>
<div id="content">
There is nothing on this page
<!-- No more information leaks!! Not even Google will find it this time... -->
</div>
</body></html>
```



And so, after checking for robots.txt you will find this page.

```
User-agent: *
Disallow: /s3cr3t/
```

Here as the directory s3cr3t is disallowed, that means that directory is hiding something. So, now search for the url

“natas3.natas.labs.overthewire.org/s3cr3t/”

## Index of /s3cr3t

<u><a href="#">Name</a></u>	<u><a href="#">Last modified</a></u>	<u><a href="#">Size</a></u>	<u><a href="#">Description</a></u>
<hr/>			
 <a href="#">Parent Directory</a>		-	
 <a href="#">users.txt</a>	2022-09-01 06:27	40	

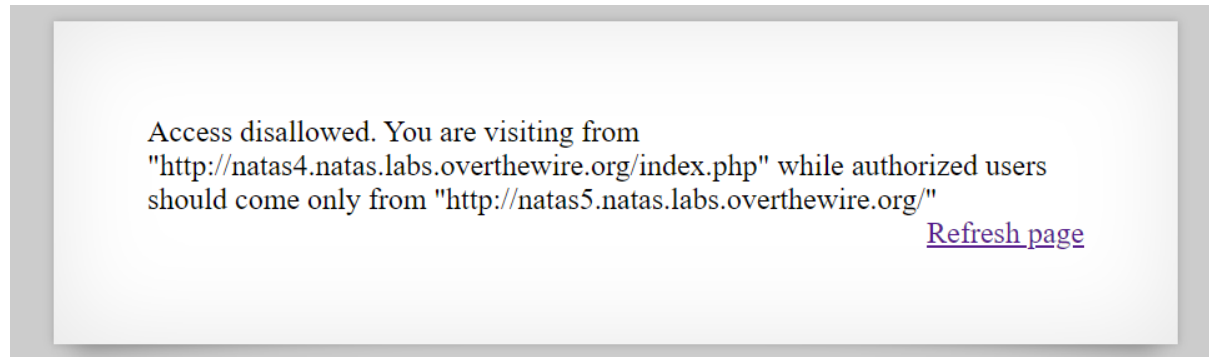
*Apache/2.4.52 (Ubuntu) Server at natas3.natas.labs.overthewire.org Port 80*

After opening the users.txt file in the page, you will find the password for the next level. Copy the password and get going.

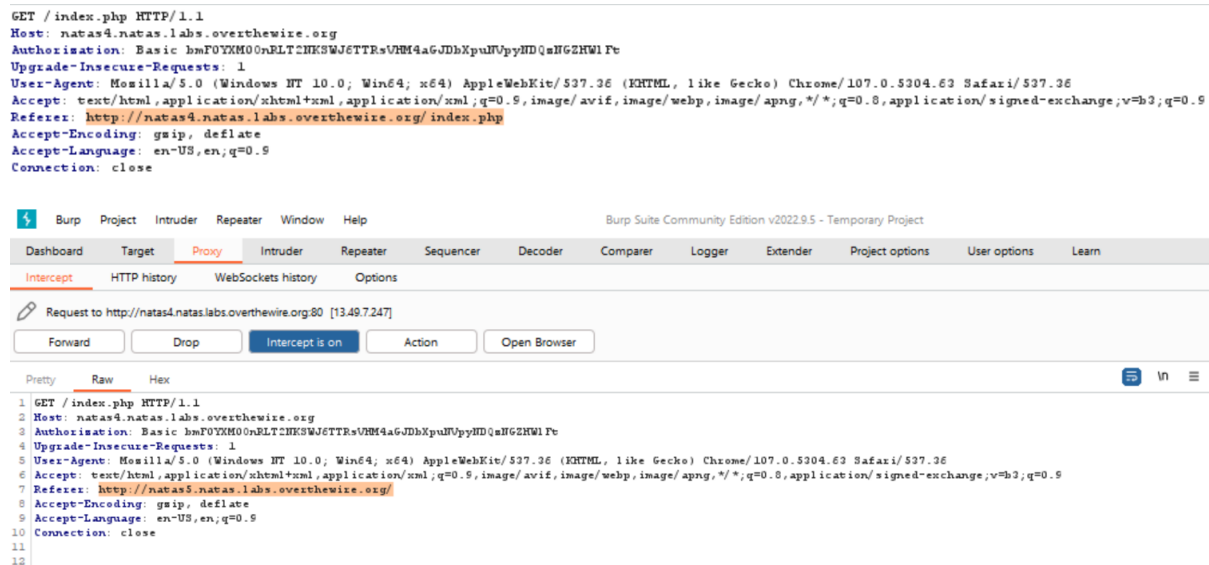
natas4:tK0cJIbzM4lTs8hbCmzn5Zr4434fGZQm

## Level 4:

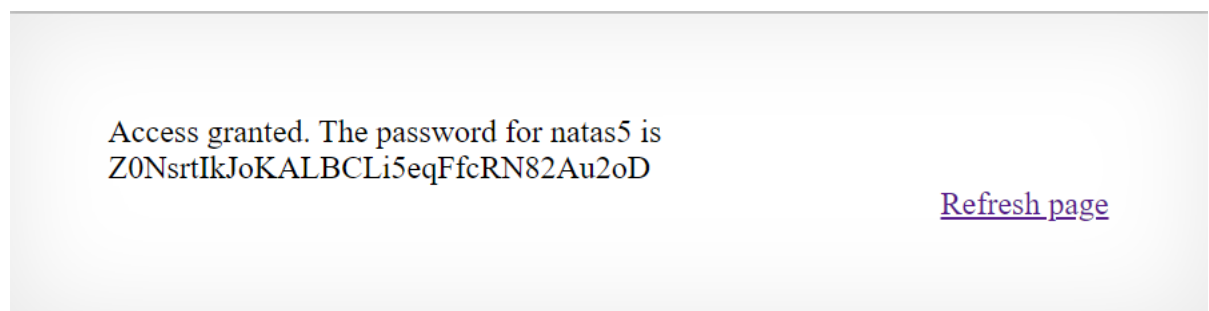
In this level, the page will tell you that access is denied due to unauthorized login.



So, now you just have to make it such that the request for access is coming from authorized user i.e., <http://natas5.natas.labs.overthewire.org/> and to do that, you can use burp suite to intercept the request while sending and modify the referer part to that of authorized user and forward the request.

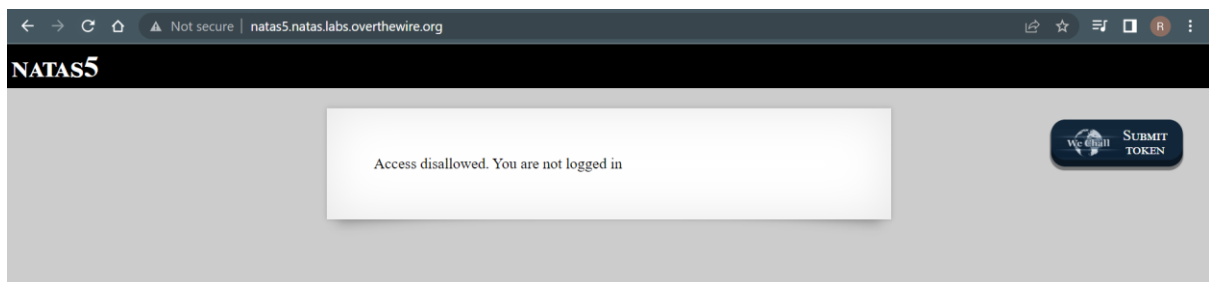


Then you will get the password for level5. Copy it and keep going.

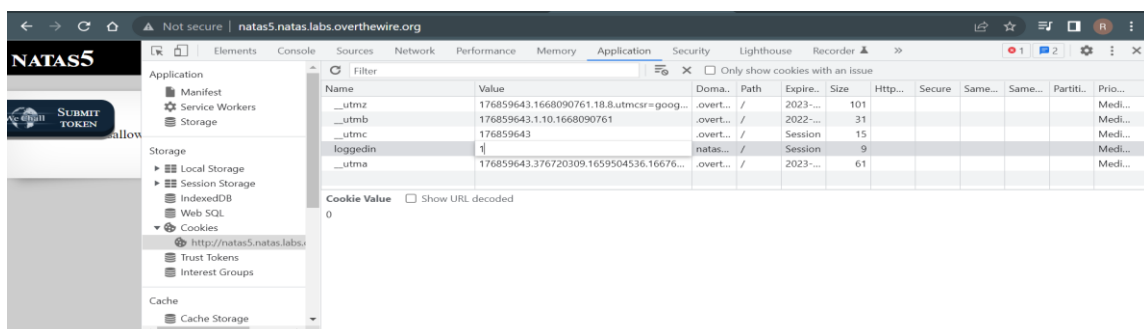
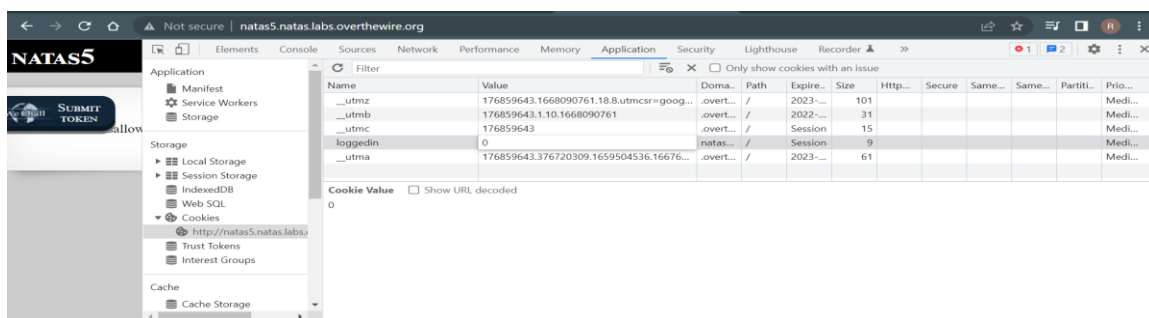


Level 5:

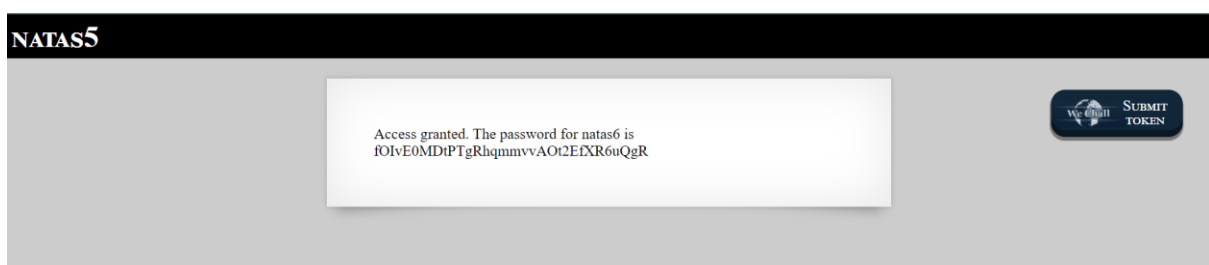
Now in this webpage, you will get access denied saying you are not logged in.



So, here we can see that the problem is with login and the website determines that we are not logged in. A website determines whether a user is logged in or not by using cookies and so to check those cookies, we first need to open the web developer tools by either selecting it manually from “more tools” option or by directly using the shortcut “**ctrl+shift+I**”. Now view the cookies that are stored in the storage tab in the tools that are shown. Here we need to change the value of **0** under loggedin cookie to 1.

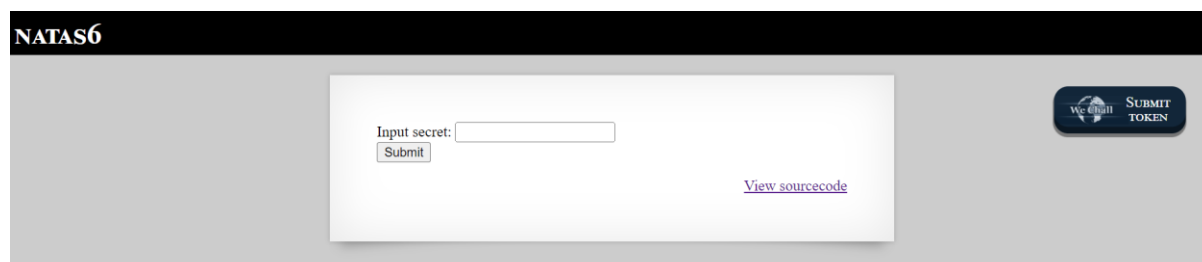


Now try to reload the page, you will get the next level's password.



## Level 6:

Now after getting logged in to level6 using the username **natas6** and the copied password, you will get the following screen.



Now click on viewcode to check the code that the website is gonna show(not inspect page source) and here we can see the following code.

```
<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": "natas6", "pass": "<ensored>" };</script></head>
<body>
<h1>natas6</h1>
<div id="content">

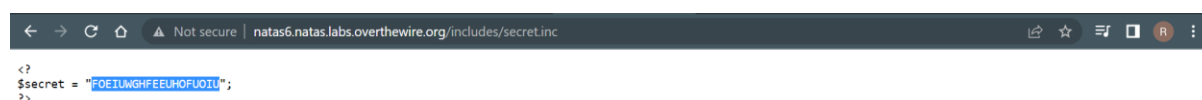
<?
include "includes/secret.inc";

    if(array_key_exists("submit", $_POST)) {
        if($_secret == $_POST["secret"]) {
            print "Access granted. The password for natas7 is <ensored>";
        } else {
            print "Wrong secret";
        }
    }
?>

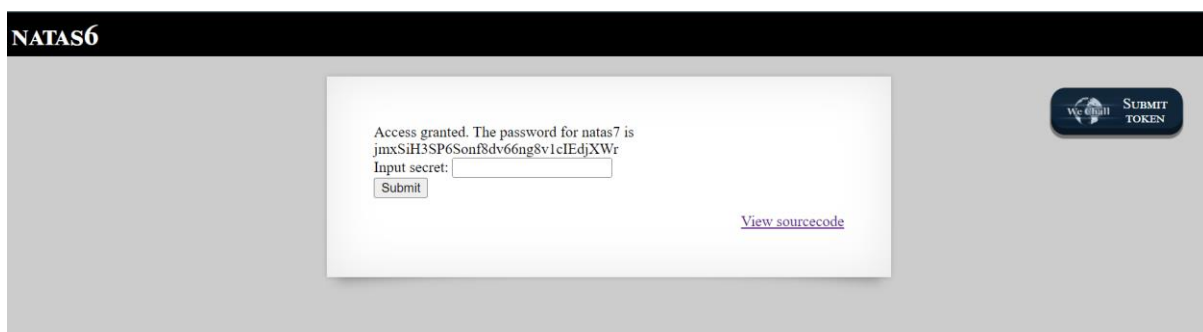
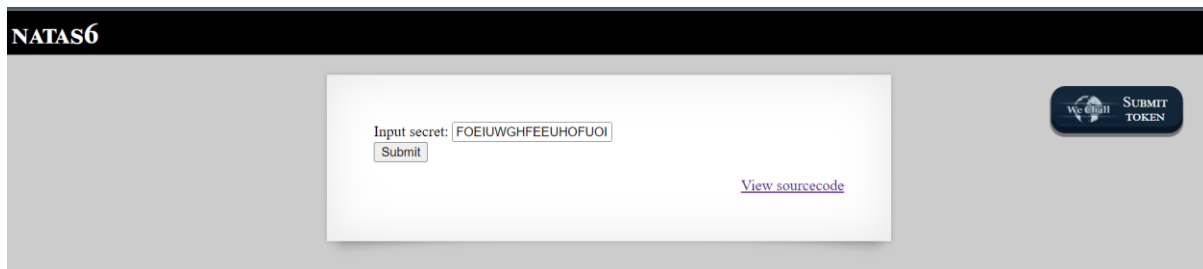
<form method=post>
Input secret: <input name=secret><br>
<input type=submit name=submit>
</form>

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

Here in this code we can see that the page is checking the input that we need to submit with a variable **secret** and to do this it is including **"includes/secret.inc"** and so, we should add this path to level6 url link which will lead us to the value of secret.

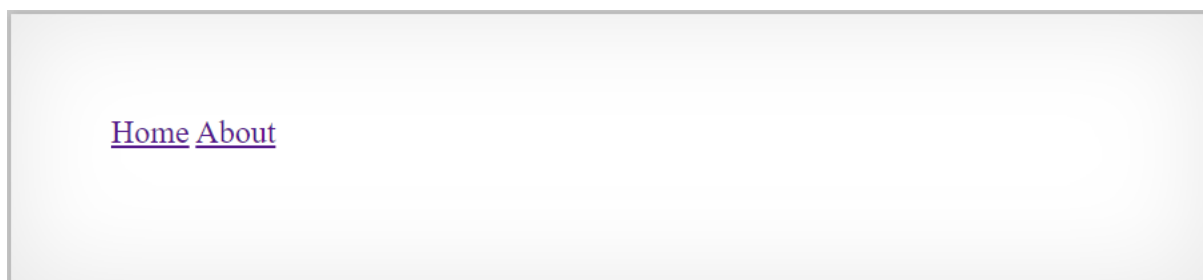


Copy the string and paste it in the level6 and submit it. You will get the password for level7. Keep going after copying the password.



## Level 7:

In this level we will get a page like this and opening either home page or about page will get us a message of either “this is the front page” (or) “this is the about page”.



Now, by inspecting the page source, we can see that there is a comment telling us a hint of where the password is located.

```

Line wrap ☐
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-ui.css" />
6 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
7 <script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
8 <script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
9 <script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
10 <script>var wechallinfo = { "level": "natas7", "pass": "jmxSiH3SP6Sonf8dv66ng8v1cIEdjXWr" };</script></head>
11 <body>
12 <h1>natas7</h1>
13 <div id="content">
14
15 <a href="index.php?page=home">Home</a>
16 <a href="index.php?page=about">About</a>
17 <br>
18 <br>
19
20 <!-- hint: password for webuser natas8 is in /etc/natas_webpass/natas8 -->
21 </div>
22 </body>
23 </html>
24

```

All we got to do is copy the path they have given and paste it in the place of home (or) about in the url depending on what page you are on. That is

[http://natas7.natas.labs.overthewire.org/index.php?page=/etc/natas\\_webp/ass/natas8](http://natas7.natas.labs.overthewire.org/index.php?page=/etc/natas_webp/ass/natas8)

Here you can see the password for the level8. Copy the password and open level 8 using the password.

Level 8:

Now after opening level 8, we will get a page similar to level6.



And as usual, we try to see the source code of the page and we will get the following page.

```
<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": "natas8", "pass": "<censored>" };</script></head>
<body>
<h1>natas8</h1>
<div id="content">

<?

$encodedSecret = "3d3d516343746d4d6d6c315669563362";

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

if(array_key_exists("submit", $_POST)) {
    if(encodeSecret($_POST['secret']) == $encodedSecret) {
        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>
</div>
</body>
```

From here, we can infer that whatever we are going to type in the textbox to submit is gonna be encrypted by the means shown in the function **encodeSecret** i.e., bin2hex, strrev and base\_64. And this encrypted secret should be equal to the encodedSecret they have in the code i.e.,

**3d3d516343746d4d6d6c315669563362.**

Now we decode this in reverse order to get the secret that we need to input to get the password for next level.



The first screenshot shows the 'From Hex' recipe applied to the input '3d3d516343746d4d6d6c315669563362', resulting in the output '==QcCtmMm11ViV3b'.

The second screenshot shows the 'Reverse' recipe applied to the input '==QcCtmMm11ViV3b', resulting in the output 'b3ViV11mMmtCcQ=='.

The third screenshot shows the 'From Base64' recipe applied to the input 'b3ViV11mMmtCcQ=='. The 'Alphabet' is set to 'A-Za-z0-9+/' and 'Remove non-alphabet chars' is checked. The output is 'oubWYf2kBq'.

And so after decoding the encodedSecret, we will get the secret that we need to submit i.e., “oubWYf2kBq”

NATAS8

Access granted. The password for natas9 is  
Sda6t0vkOPkM8YeOZkAGVhFoaplvIJFd

Input secret:

[View sourcecode](#)

Now copy the password and go to the next level.

## Level 9:

After logging in to level9, you will get this page.

Find words containing:

Search

Output:

[View sourcecode](#)

Now click on **view sourcecode** and you will get the following page.

```
<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>
```

Now we know that the word we typr in the box is searched in dictionary.txt file using grep and given as output to us. And so we should now find the password that is in the file dictionary.txt. To do that, we will first search for some word in the file let's say **natas**.

← → ↻ 🏠 🔒 Not secure | natas9.natas.labs.overthewire.org/?needle=natas&submit=Search

**NATAS9**

Find words containing:

Search

Output:

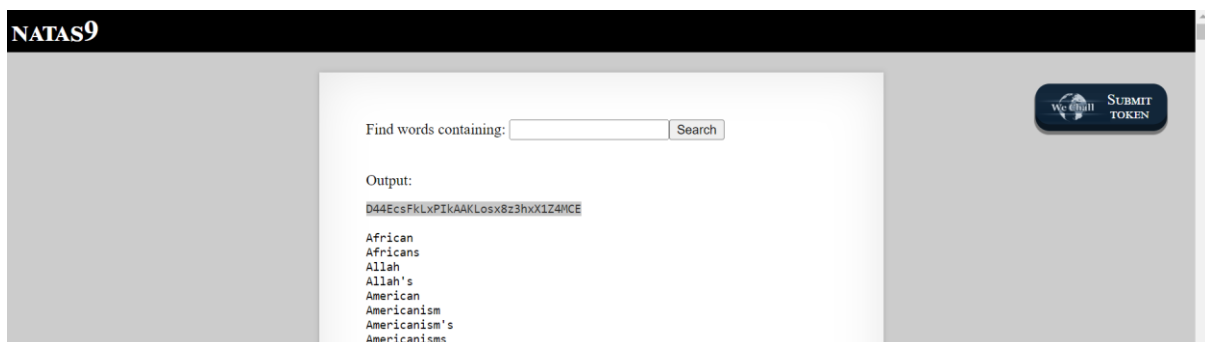
sonatas

[View sourcecode](#)

And now we need to check for the password by changing the url to

[http://natas9.natas.labs.overthewire.org/?needle=;cat/etc/natas\\_webpass/natas9&submit=Search](http://natas9.natas.labs.overthewire.org/?needle=;cat/etc/natas_webpass/natas9&submit=Search).

This is because we know that the password is always in the /etc/natas\_webpass/natasx file where x is level number to which we are trying to find the password and so we will try to get the password inside the file by using **cat /etc/natas\_webpass/natas10** and the ';' is so that we can use command here.



Now you will get the password for level 10, so copy the password.