IT20028046

GUNATHILAKA S.B.M.B.S.A

**SNP Lab 02**

**Video presentation link**

<https://drive.google.com/file/d/15UzG-CYBFA-my70XnGIbnT0lwWZKAJa-/view?usp=sharing>

During the natas game, we have to find the passwords for further levels.to reach every level we must enter the URL given by Natas game.

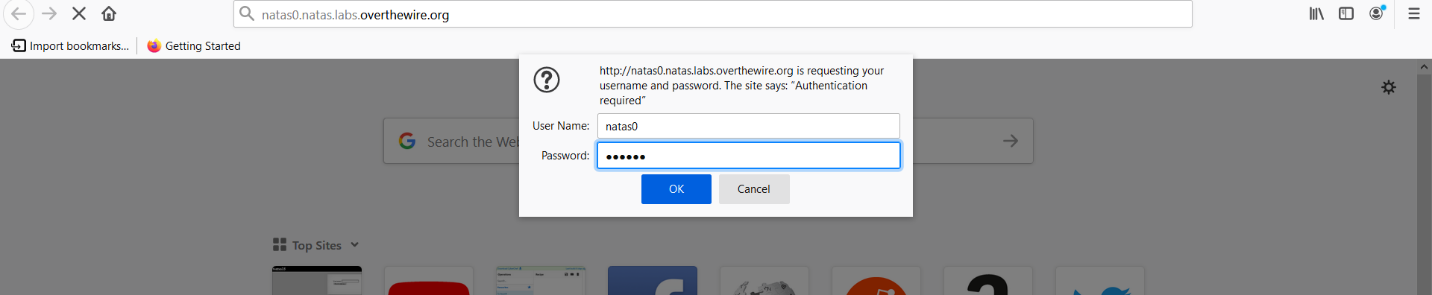
We will have to use a username and its password to access a level. the password is hidden inside the current level so we have to find it to play the next level.

Level 0

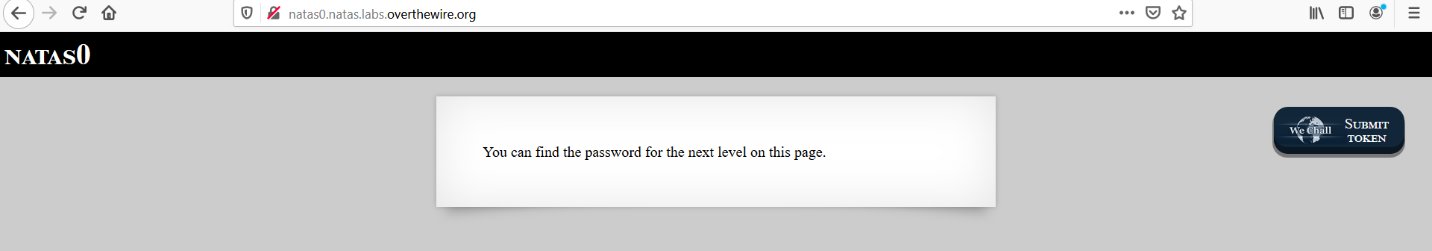
This is a very simple level. the login credentials are given on the natas introduction page. we can log into natas0 using that credentials.

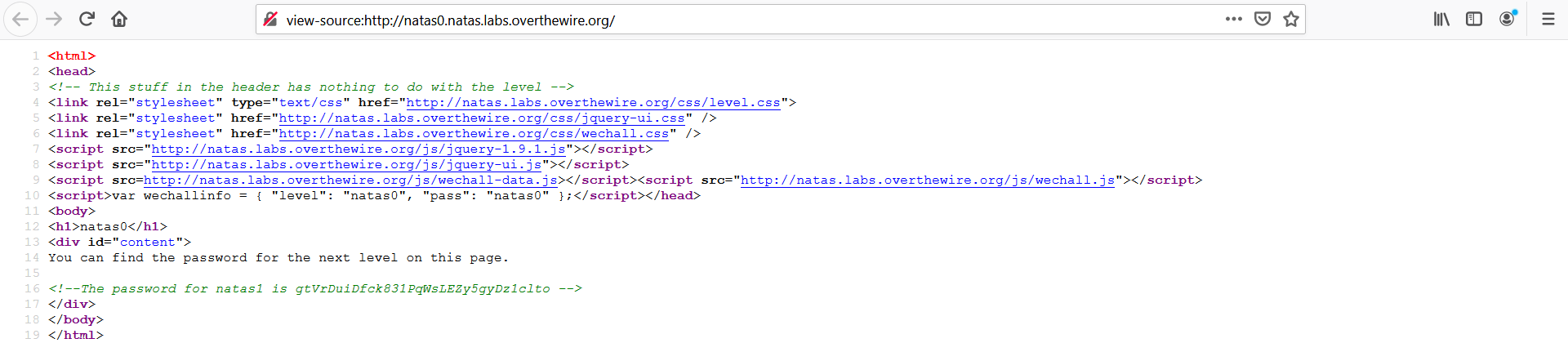
Level 0 – level 1

After giving the correct credentials and login completed then we can see a message on the webpage. it says that “you can find the password for the next level on this page”



To find the password let’s check inside the source code .to view the source code we right-click on the webpage and select “view page source” .now we can see the password for natas1.

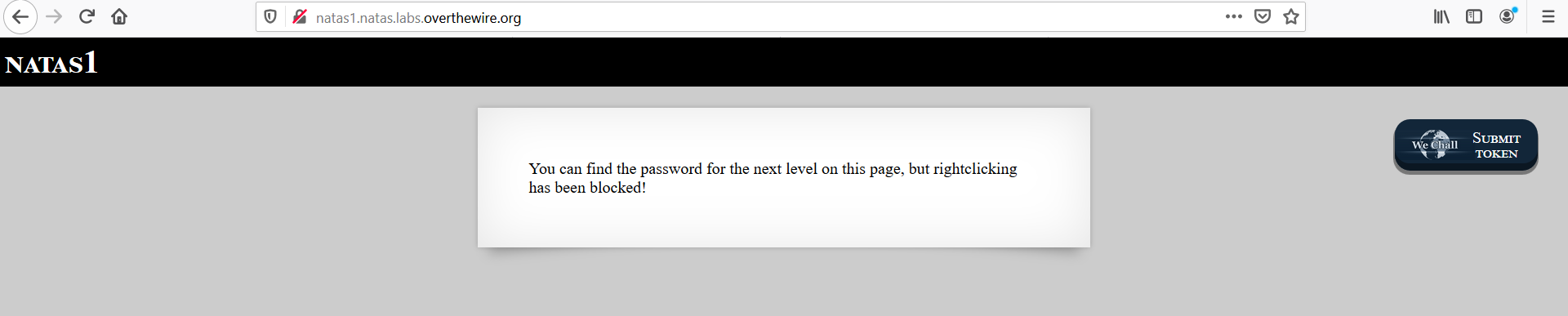


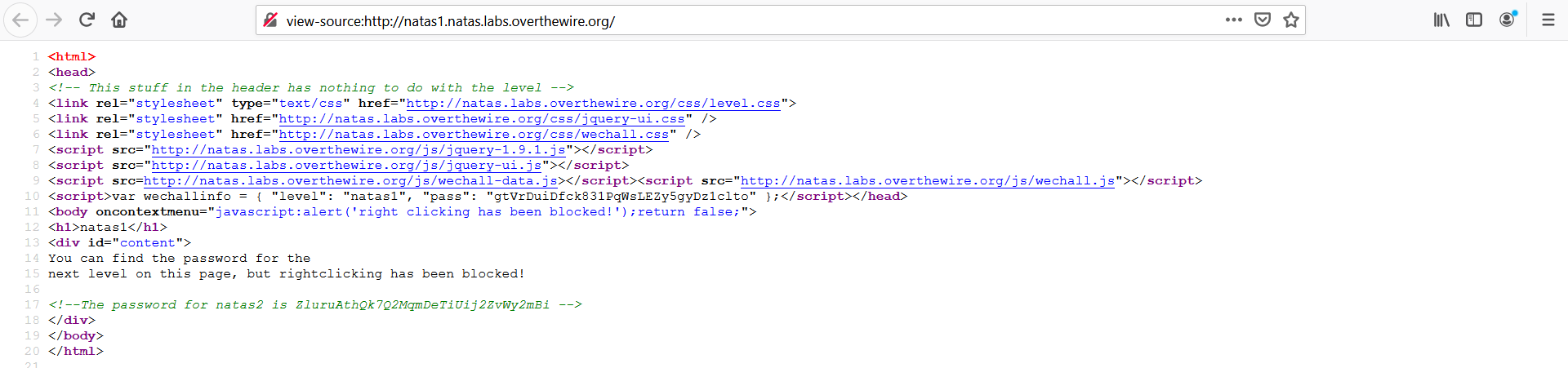


Level 1- level 2

We can use the credentials we found before to login natas1.

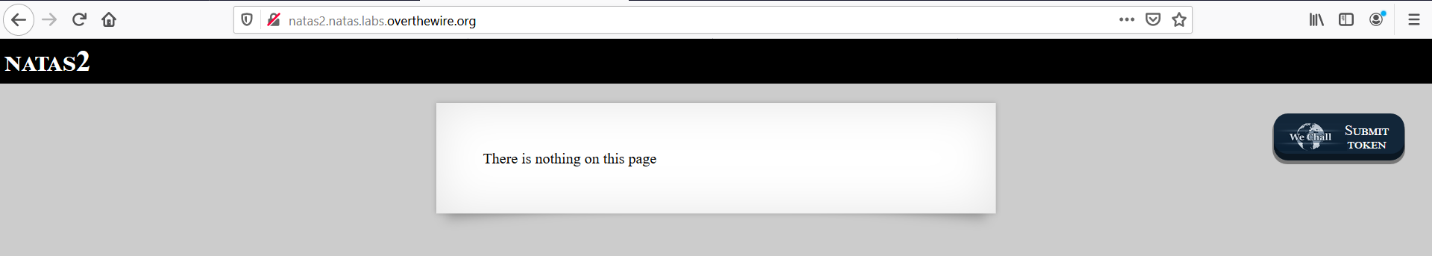
On successful login to the webpage, we will see a message. it says that this time we cant right click on the page.

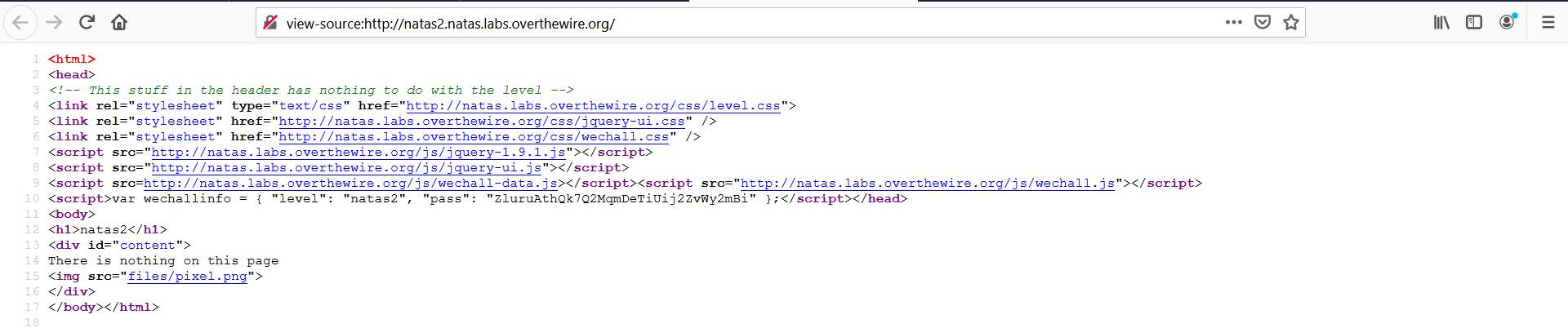


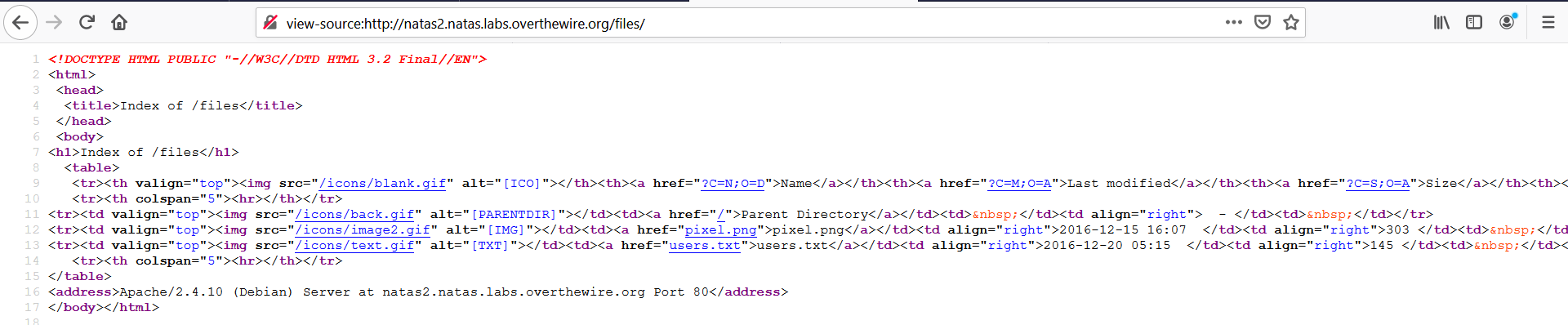
Now we will have to find another way to view the source code. we can use the ctrl+u key combination to get the source code. now we can check for the password on this source code.

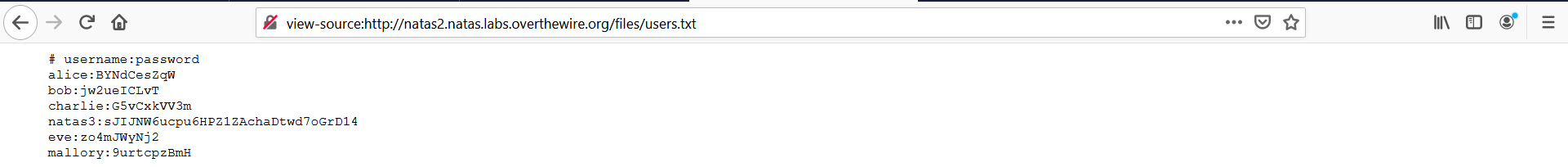
Level 2 - level 3

We can use the credentials we found on the previous level to login level2.

On this level browser shows a message .it says “there is nothing on this page”.

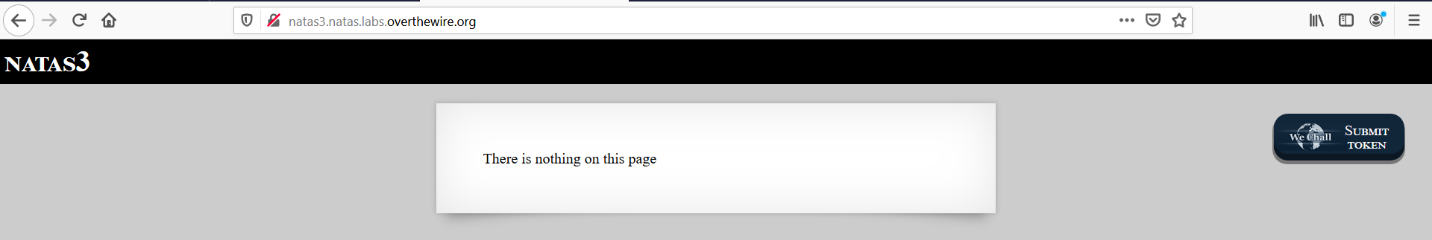
When we check the source code now the password is not inside the source code. we can see an image named pixel.png located in a file directory.

In this file directory, we can find a user.txt file

The user.txt file contains various usernames and passwords with our next-level password.

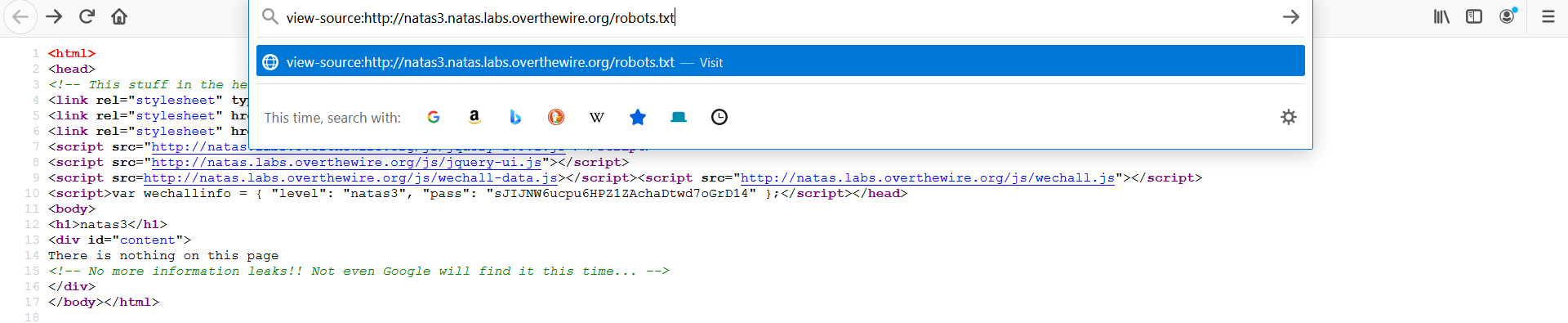
Level 3 – level 4

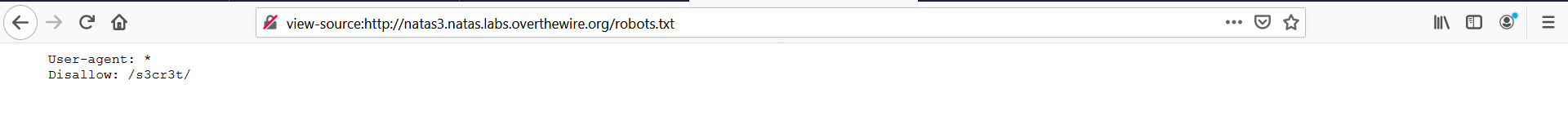
Now we have the natas3 password .therefore we can log in to natas3 without any issue.

This time we have another message from the browser .it says” there is nothing on this page”.

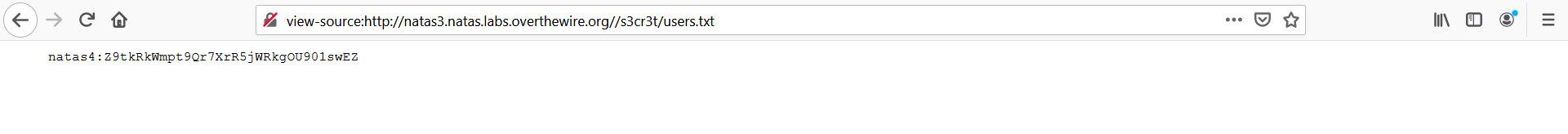
Let's check the source code of this level. in the source code, we can see a comment. it says” not even google will find this time”.

every website has a file named robot.txt. now we can check if this website has that kind of file.

When we opened the robot.txt file we find the scrt directory is disallowed



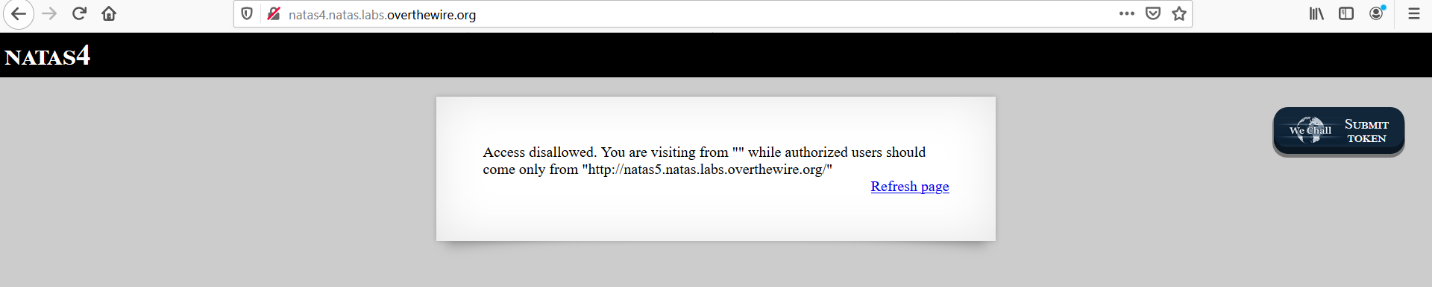
In this directory, we can see a file named user.txt.we can find the password from this text file.

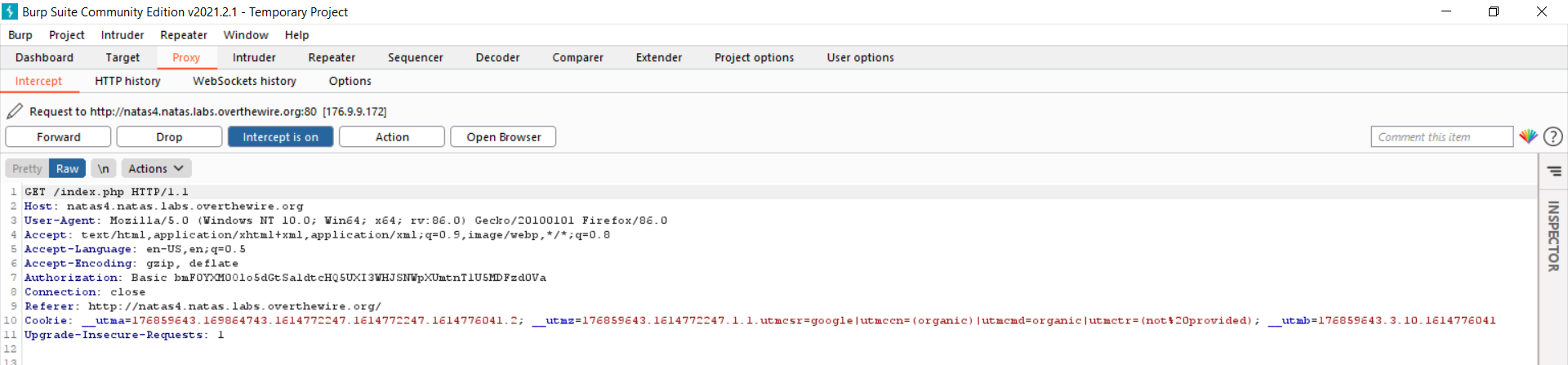


Level 4 - level 5

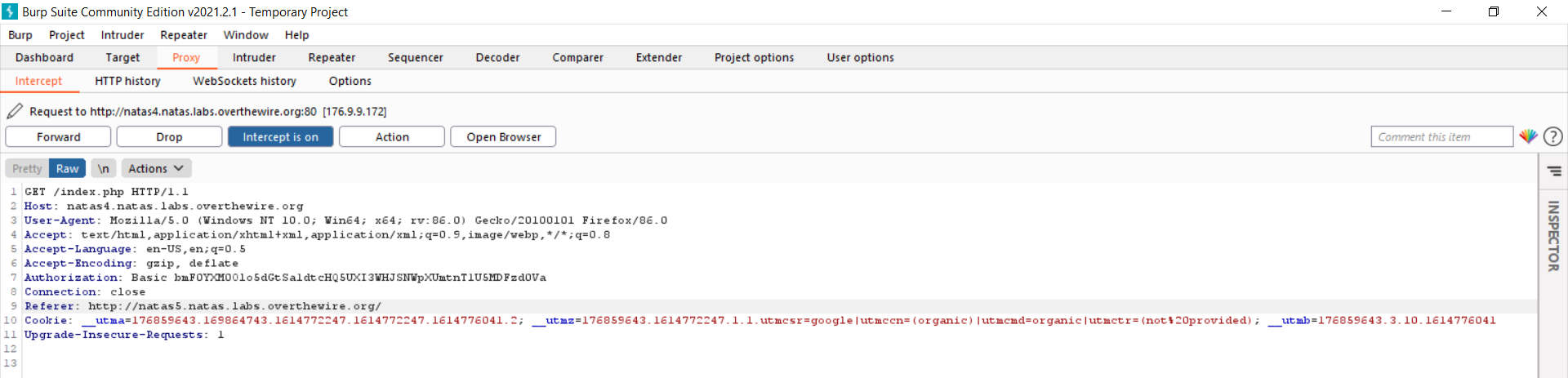
As earlier we can give the credentials and login into natas4.

We will see a message on the webpage. it says” Access disallowed. You are visiting from "while authorized users should come only from <http://natas5.natas.labs.overthewire.org/>”.

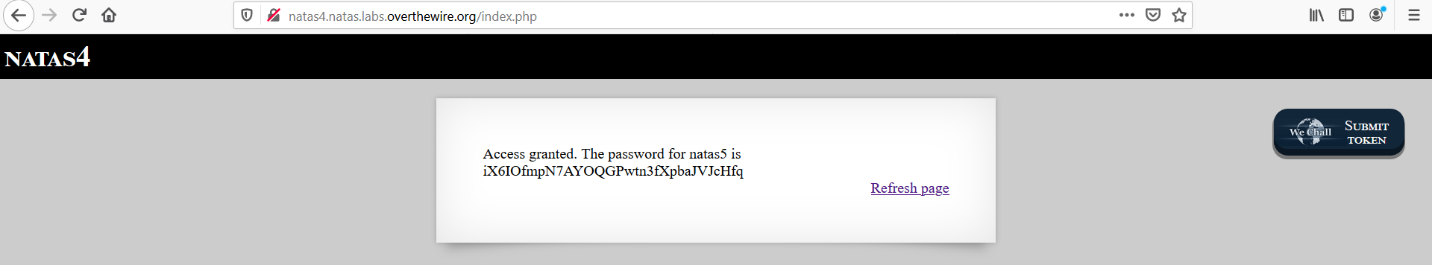


At this time we have to use another tool called burp suite. using burp suite we capture HTTP requests. now we can see a parameter named referrer on the result page it says about natas4.

In this time we can change the parameter value as natas5

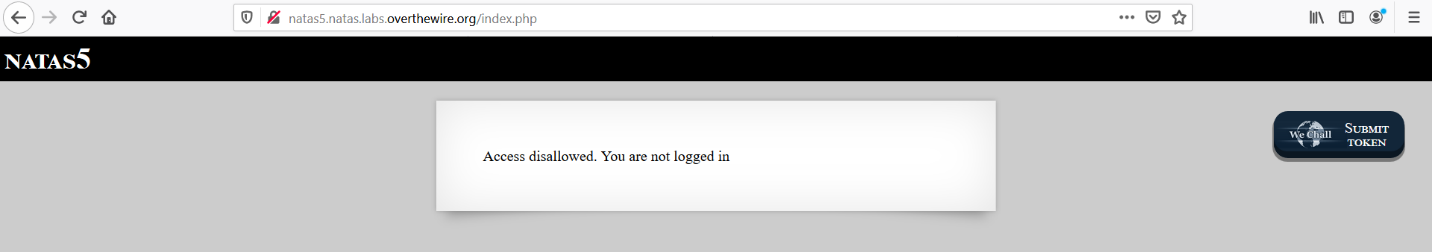


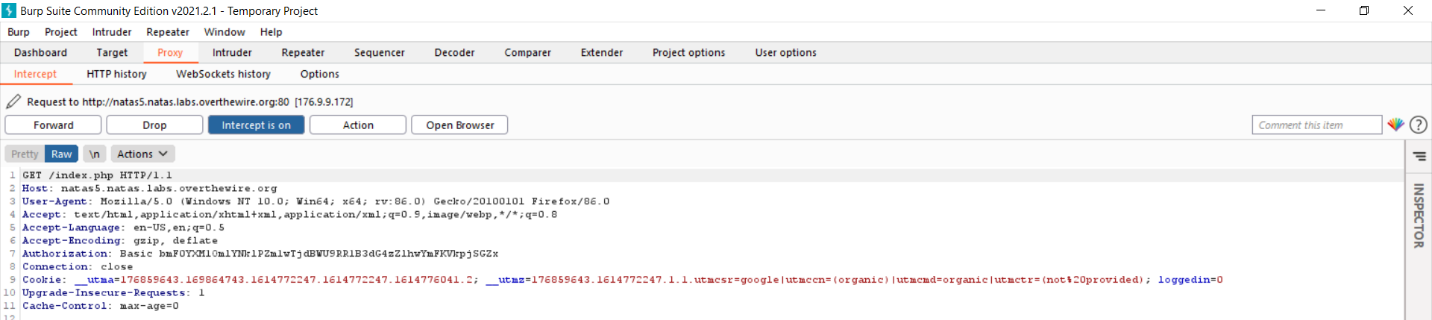
After forwarding the request we get the password of natas5.



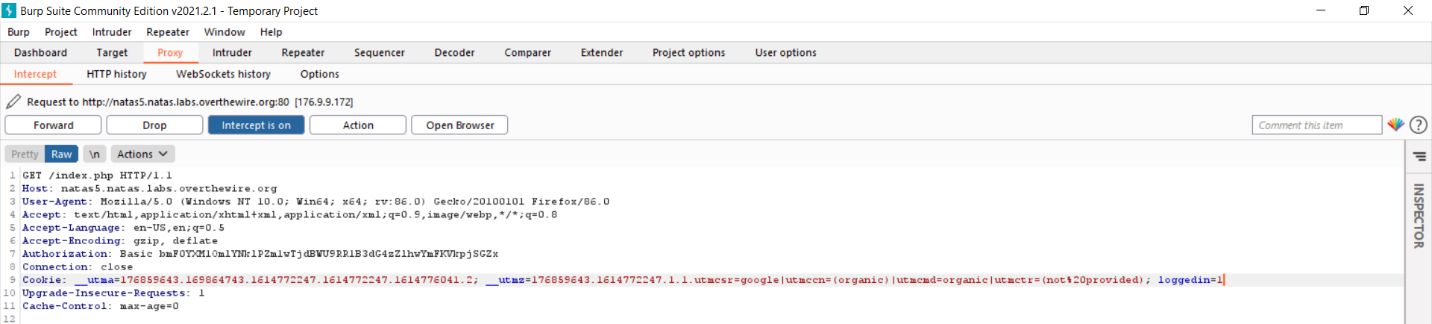
Level 5 – level 6

In this level using credentials before we got from the previous level, we can log into natas5.

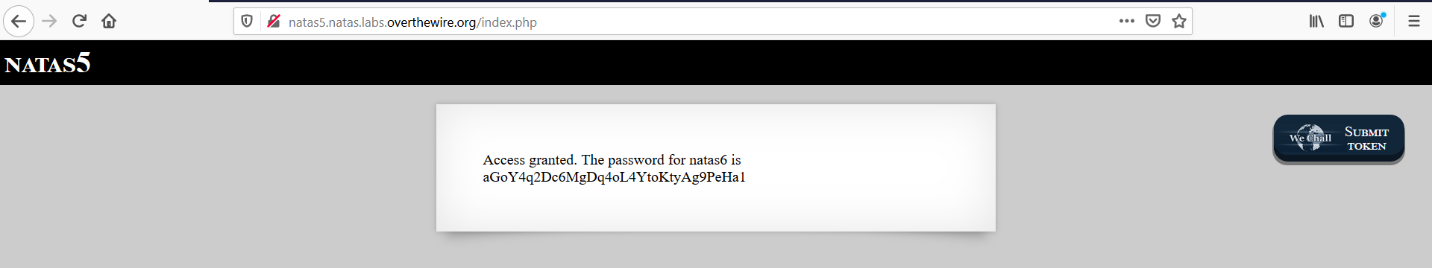
We can see a message from the browser .it says that “Access disallowed. You are not logged in”.

Now we can use the burp suite to capture HTTP requests .here we can see a parameter named logged in.

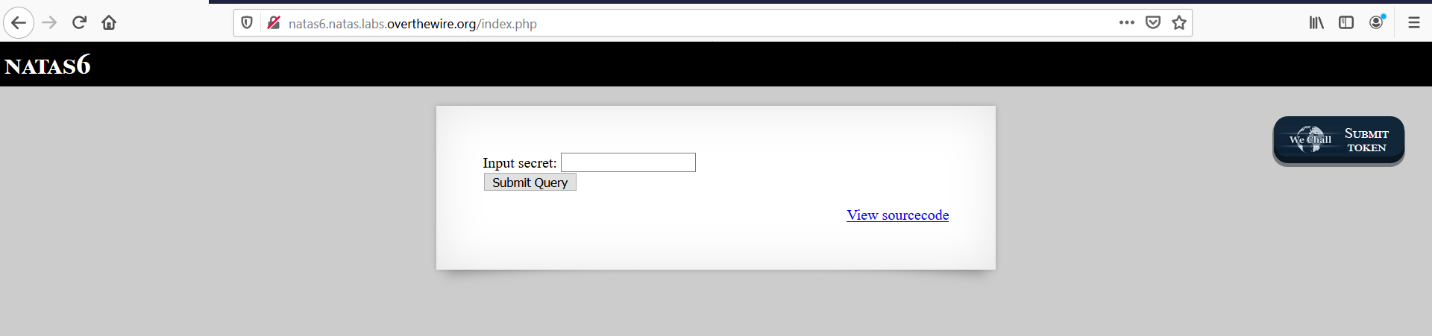
We can change the loggedin parameter value to number 1.



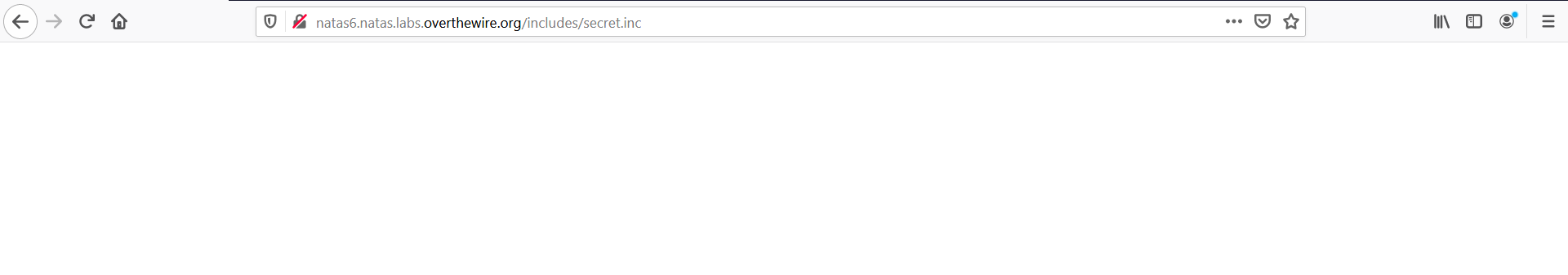
After forwarding this request we get the password.

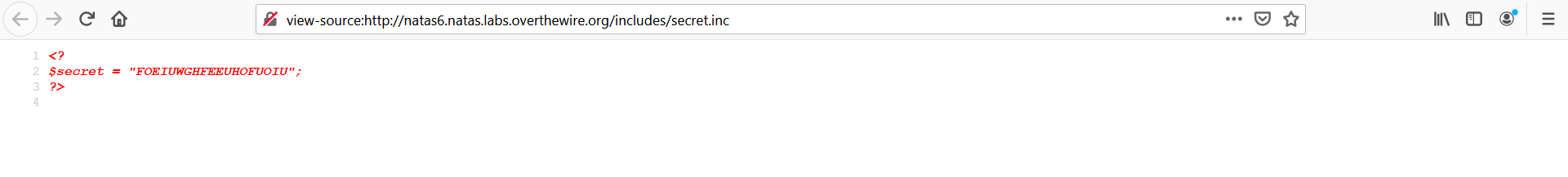


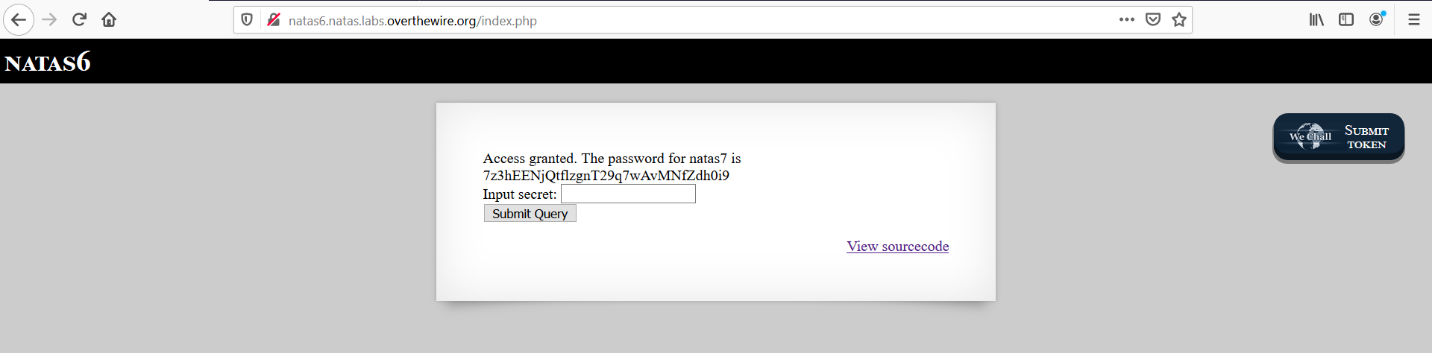
Level 6 - level 7

After login into level6, we will have a small form on the webpage. it says” input secret”.

At this time we should find a secret to get the credential for the next level. here we can see that a file named “secret.inc”.

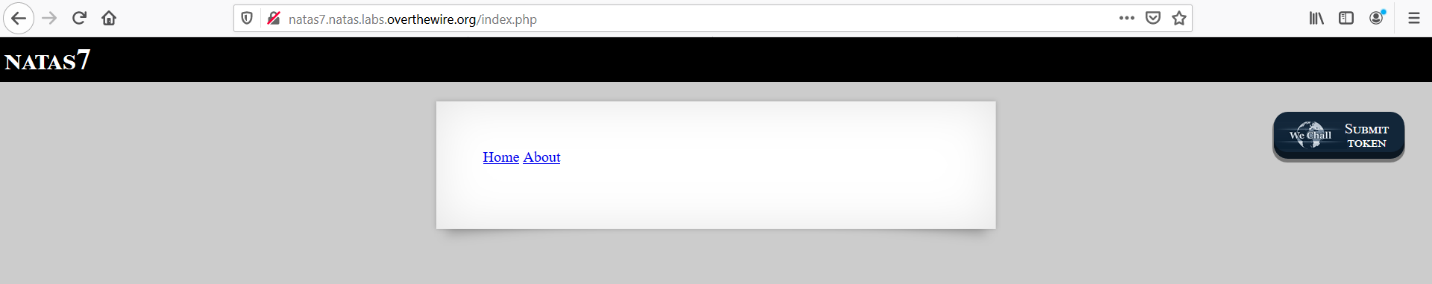
Next, we will enter the location into the URL. we can do it manually. now we can see a blank page. after view the source code of that page we can see the secret.

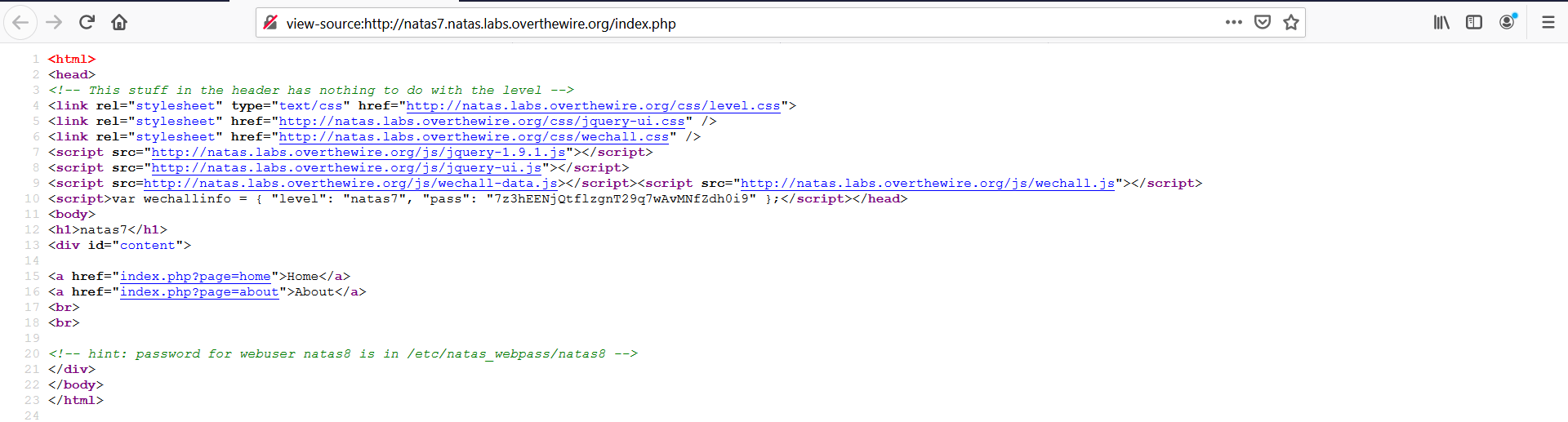


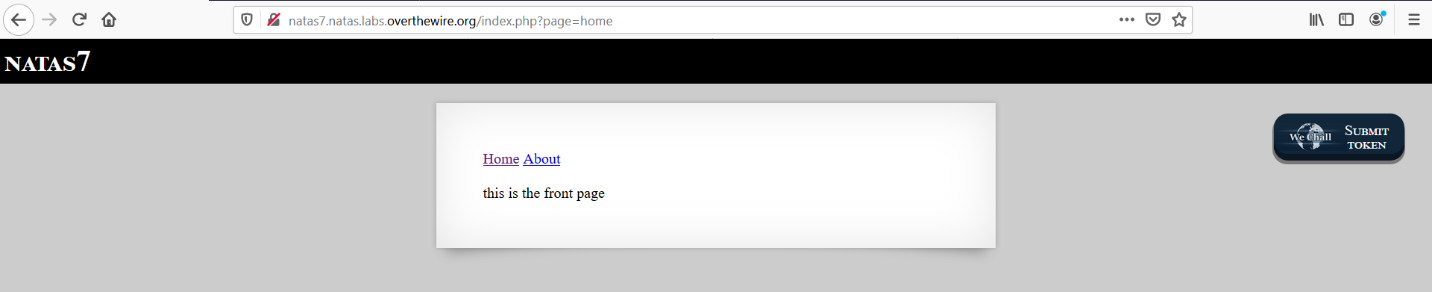
Now we can go back into the form and enter the secret .now we have the password to the next level.

Level 7- level 8

We can use credentials we found before to login to level7.

After successfully logging in, the webpage gives two links to us.

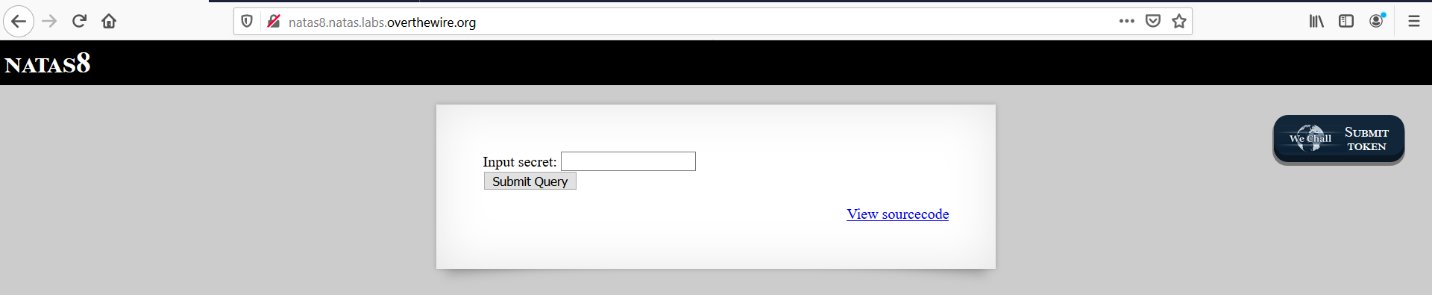
Let's check the source code of the page. we can see links to call PHP files and we have a hint about the location of the password.

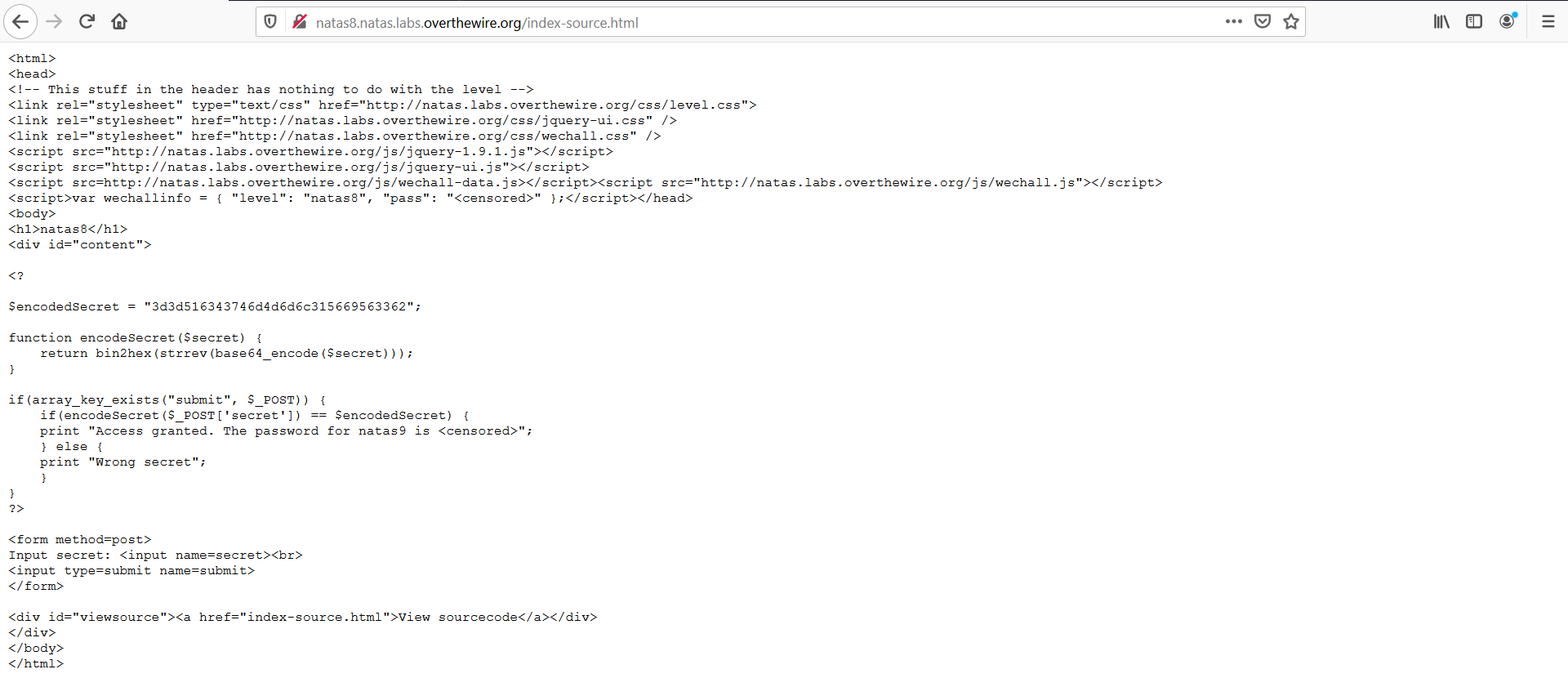
After clicking the home link browser will bring us to another page.

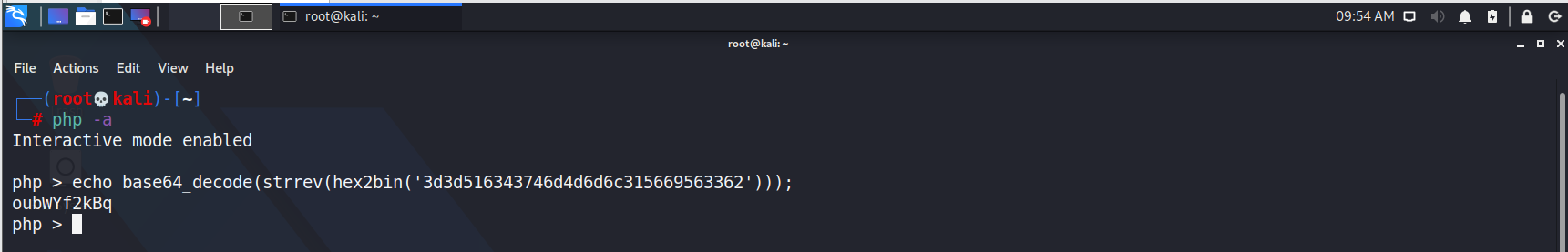
Now we can modify the URL to read the password stored in the natas\_webpass. after entering this URL, we have the next level password.

Level 8 - level 9

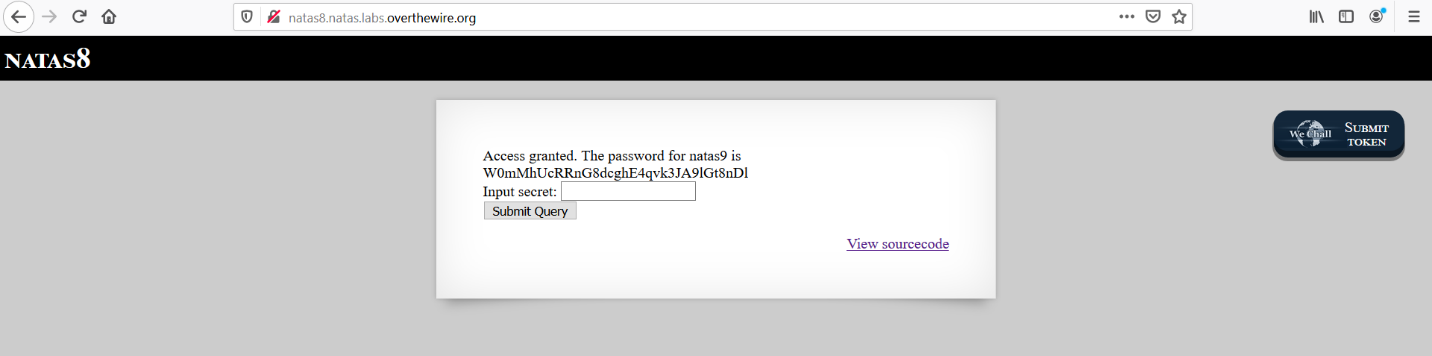
Using a suitable password we found earlier we can log in to level8.

On the webpage, we have a form it says “input secret”.

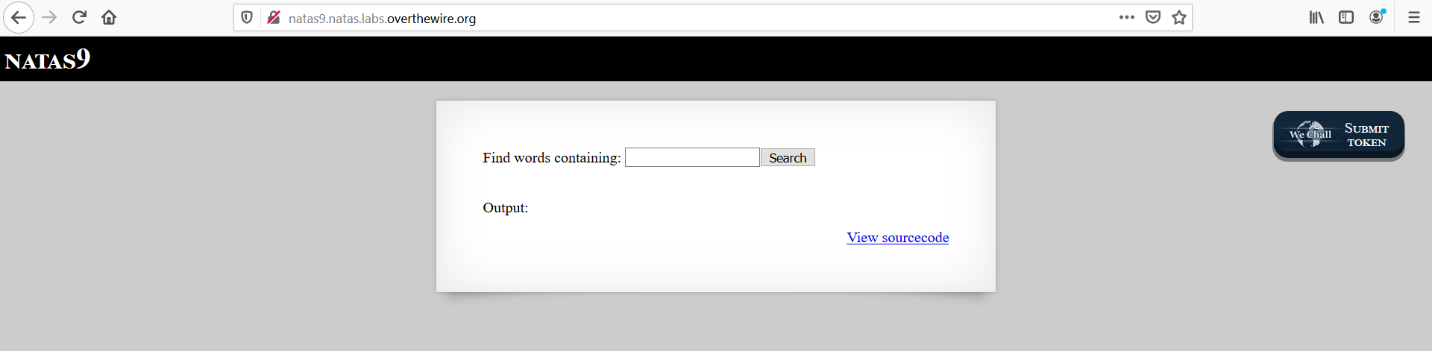
Now we can see an encoded secret inside the source code .also we have the encoding function on the source code.

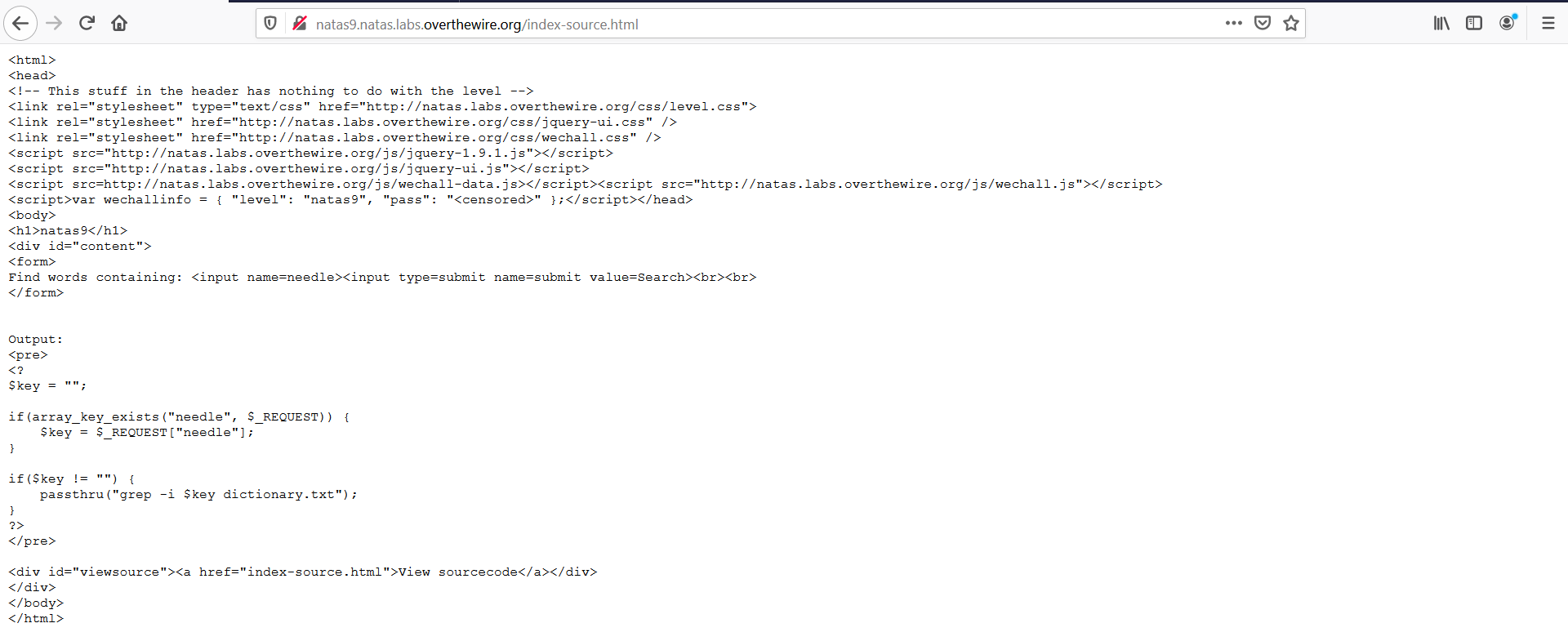
Now we have to create a function to decode the secret. we can use a Unix environment to decode the secret.

So now we have the decoded secret. We can use it to extract the password.



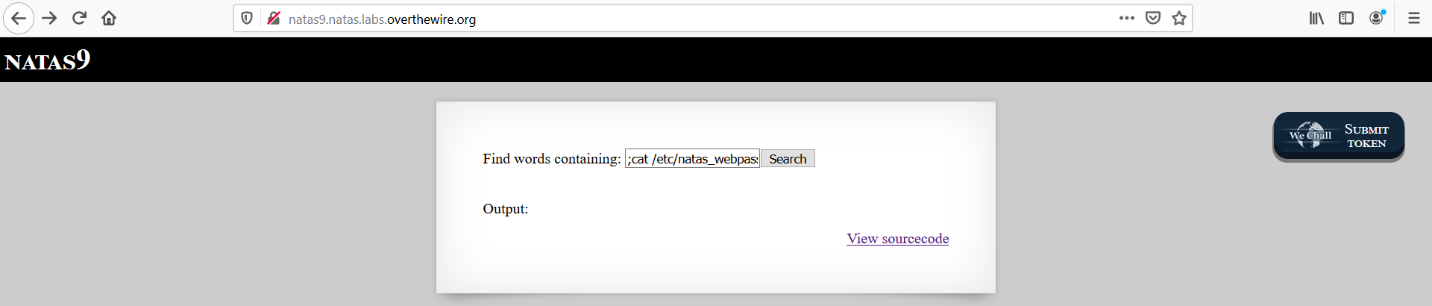
Level 9 – level 10

At this time we have another form .it says “Find words containing”.

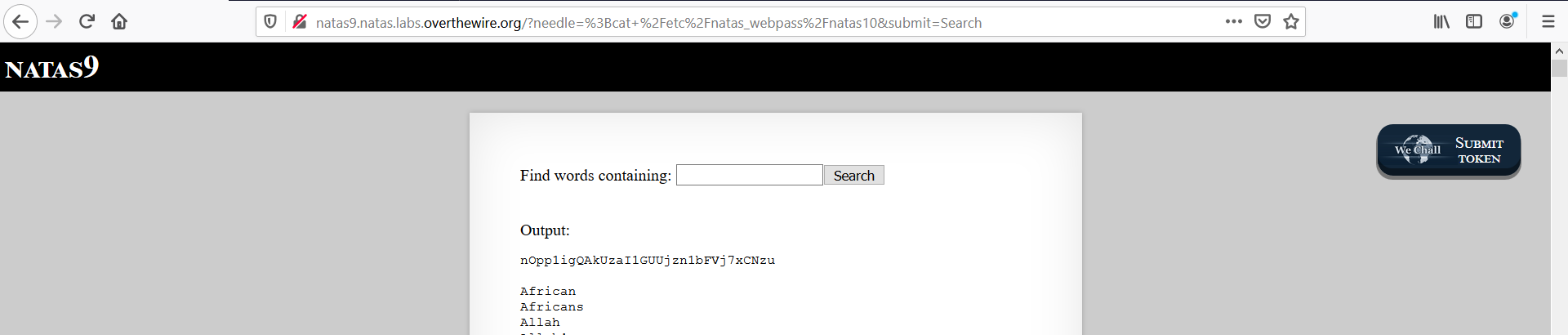
When we opened the source code, we can see a function named passthru. when we enter a value to passthru function it will take by the $key and execute it.

So we can use (;) to execute multiple commands. let's try to read the password.

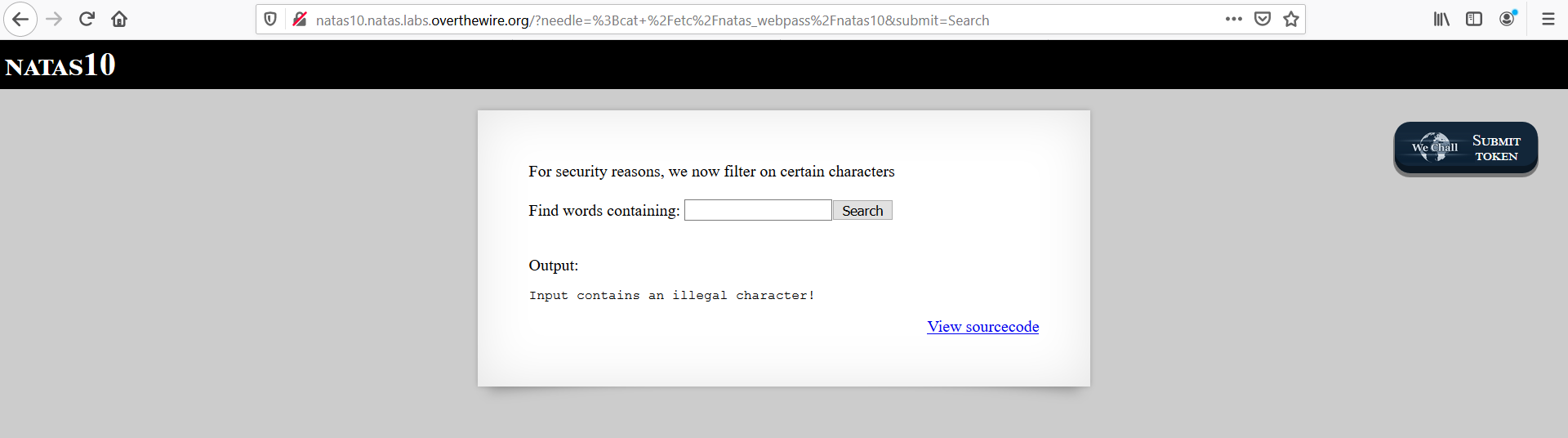
;cat /etc/natas\_webpass/natas10



Now we can see the password inside the output.



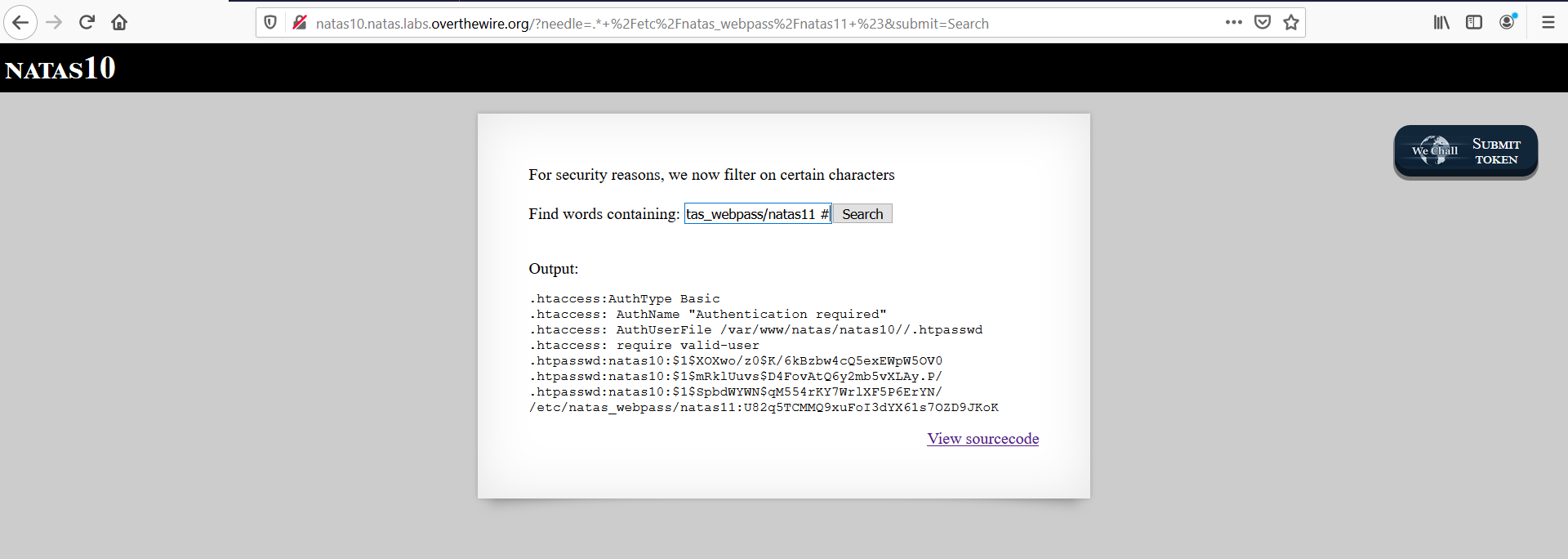
Level 10 – level 11

After logging into level10, we will have a form in front of us. it says” For security reasons, we now filter on certain characters”.

Next, we check the source code .when we open the source code we have the same function called passthru().it takes the value given by us to $key variable and it filters the input of the characters.

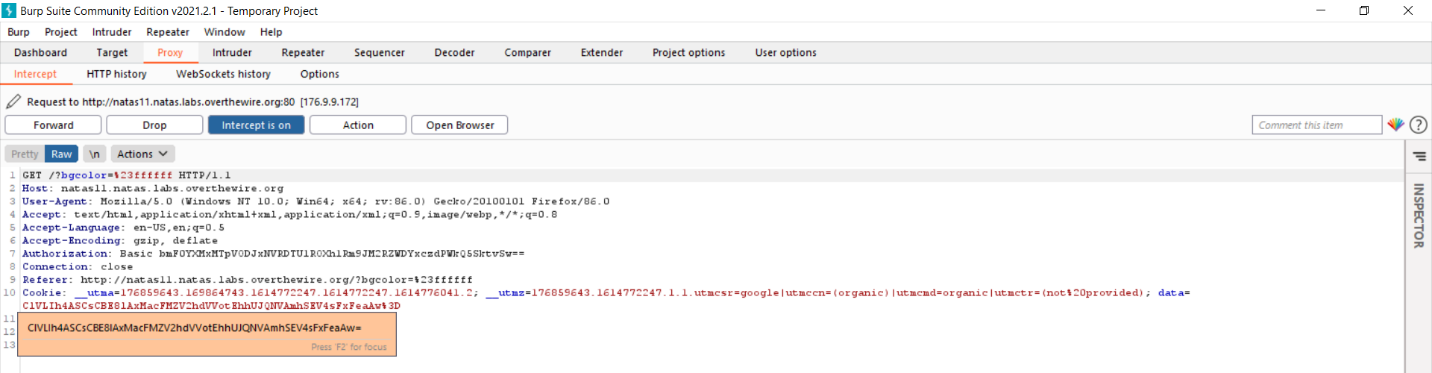
So we can use (. \*)to execute multiple commands. let's try to read the password.

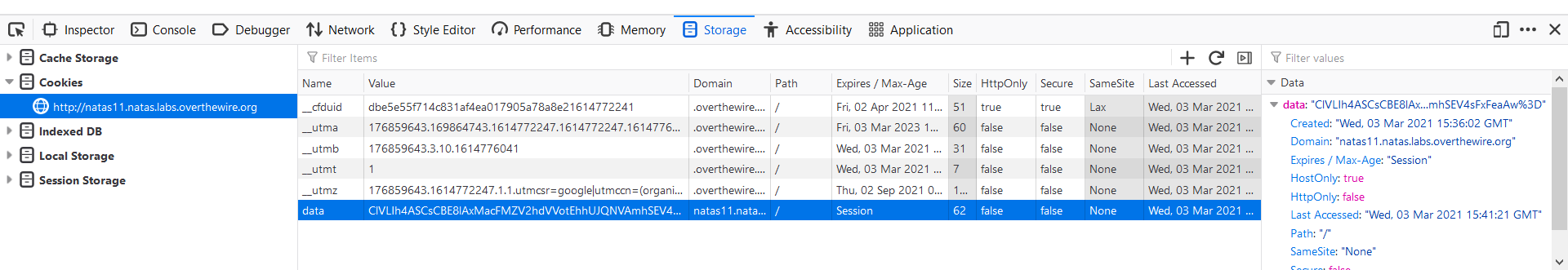
.\* /etc/natas\_webpass/natas11 #



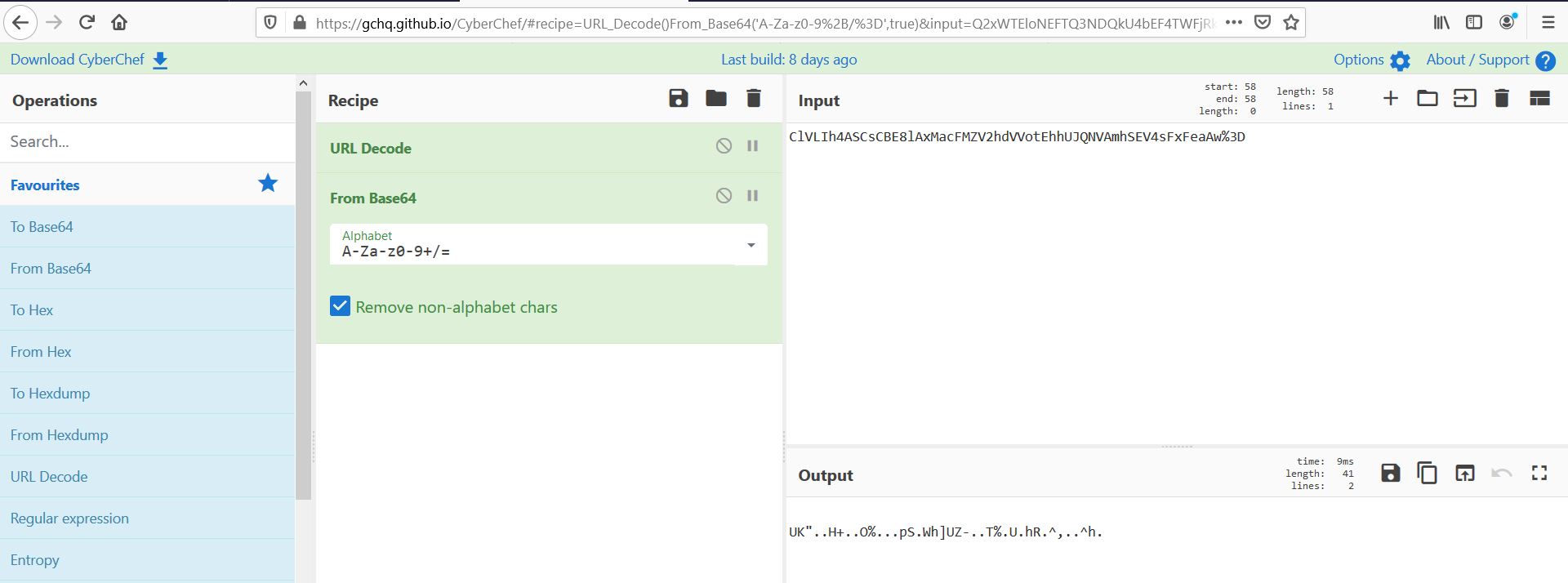
Now we can see the password under the output.

Level 11 - Level 12

Now we can see a form with a message .it says” Cookies are protected with XOR encryption”.now we have to grab the XOR encrypted cookie that the site is using. we can use burp suite or inspector on firefox to get the cookie.



Let's check the source code .we can see some functions with XOR encryption. after analyzing the source code we can see the function to decode the key.so now we should find the key. the source code gives us an idea about how should be the key. we can use Unix commands or decoders like cyber chef to decode encoded things. so we can use cyber chef to decode the cookie.

First, we do a URL decode to the cookie.

The xor cipher has 3 parts

Key=?

Ciper text= UK"..H+..O%...pS.Wh]UZ-..T%.U.hR.^,..^h.

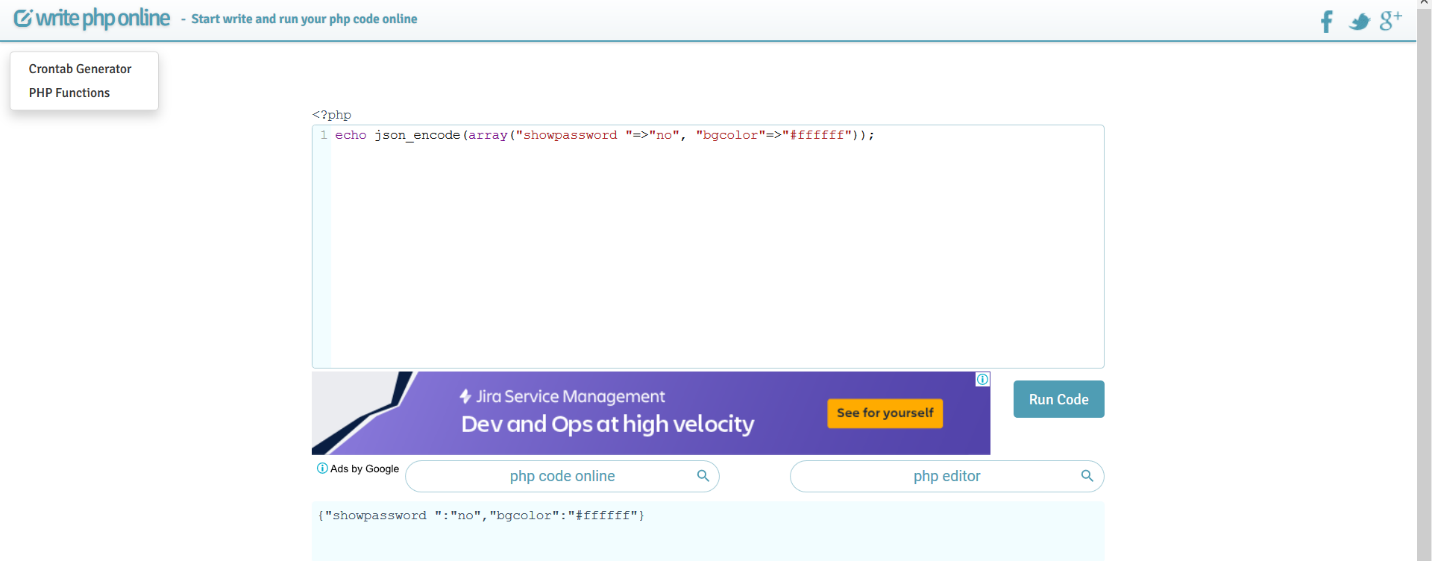
this could be the ciphertext

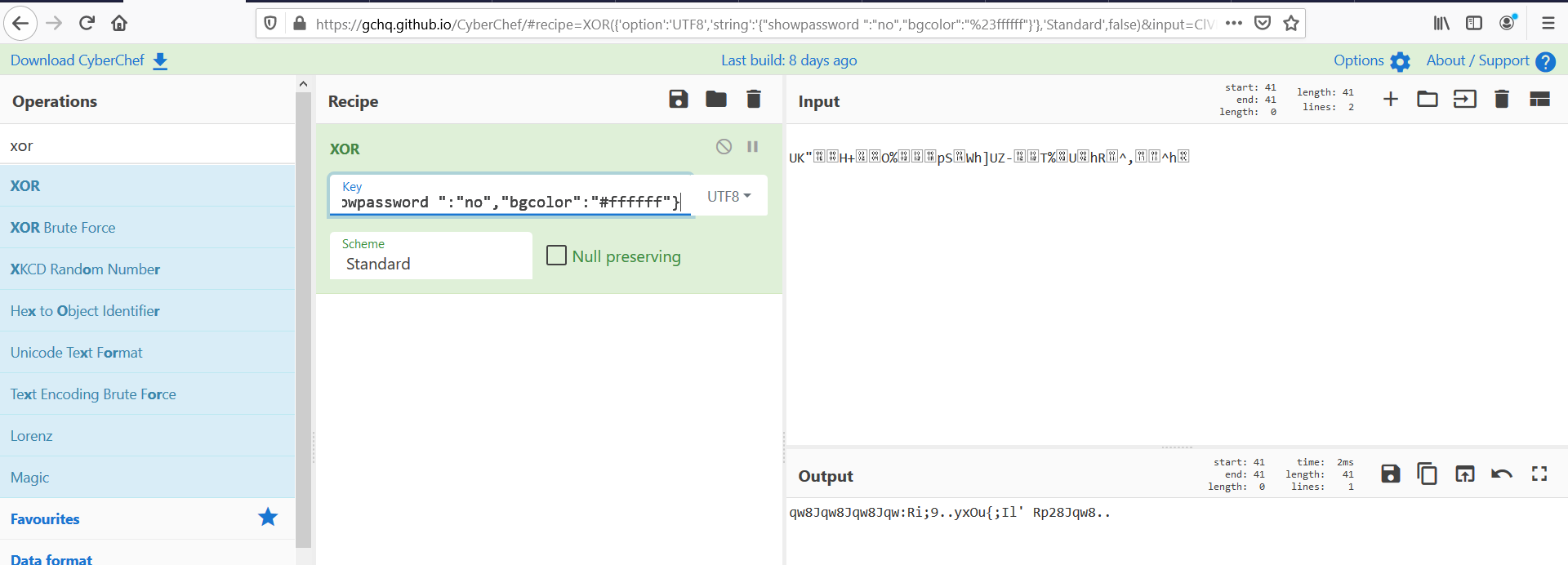
Clear text=?

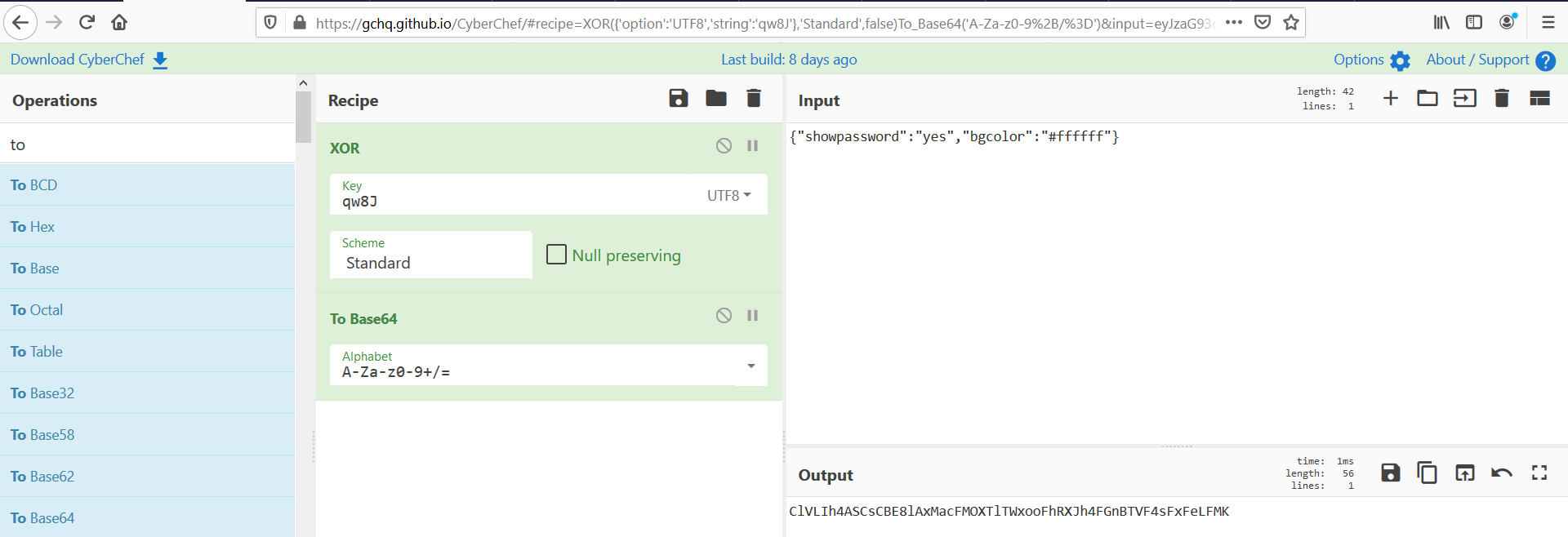
If we can find any two of these values then we can retrieve the third one.

$defaultdata array can be the key but we should Json encode it.

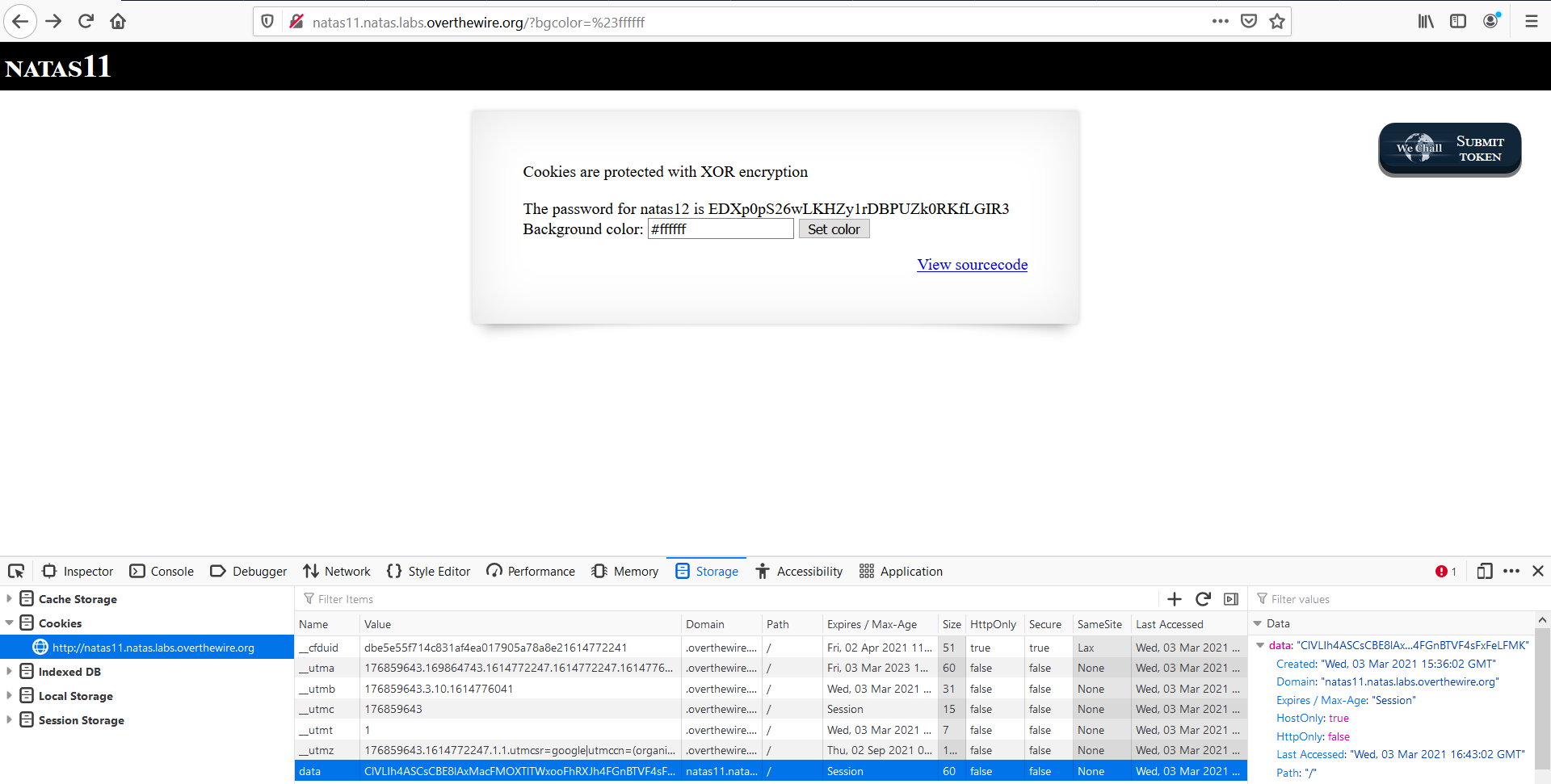
echo json\_encode(array("showpassword "=>"no", "bgcolor"=>"#ffffff"));



This result can be the clear text. now go to the cyber chef and move output to input. now we use XOR to decode and give the key we found before.

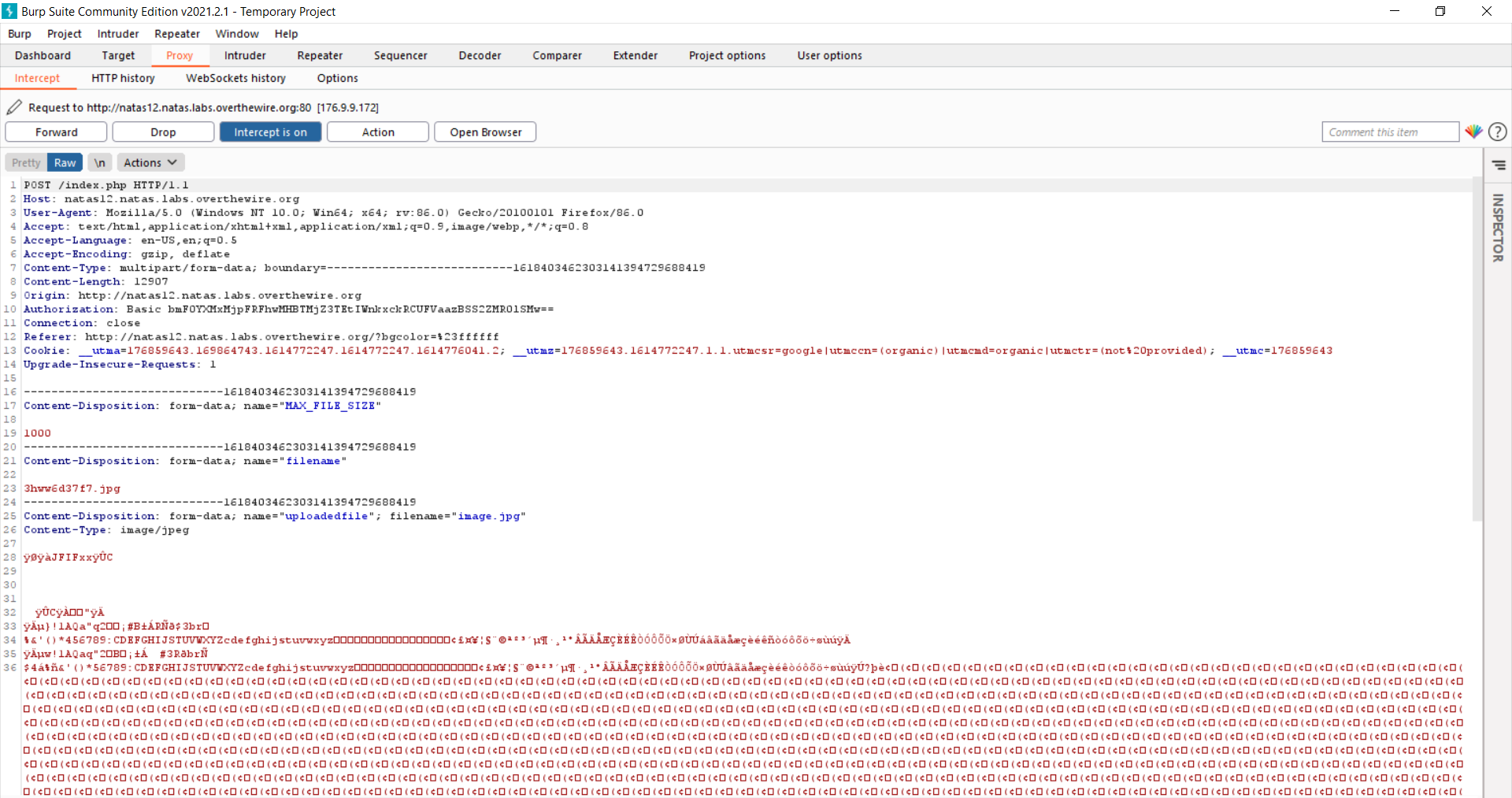
Now we can see a repeating key in the output. next, we change the show password value to yes and give the first 4 letters of repeating key as the key .now we convert to base64.

Now we have the decrypted cookie so, let's overwrite the old cookie with the new one we got now.

Now we have the password to the next level after refreshing the page.

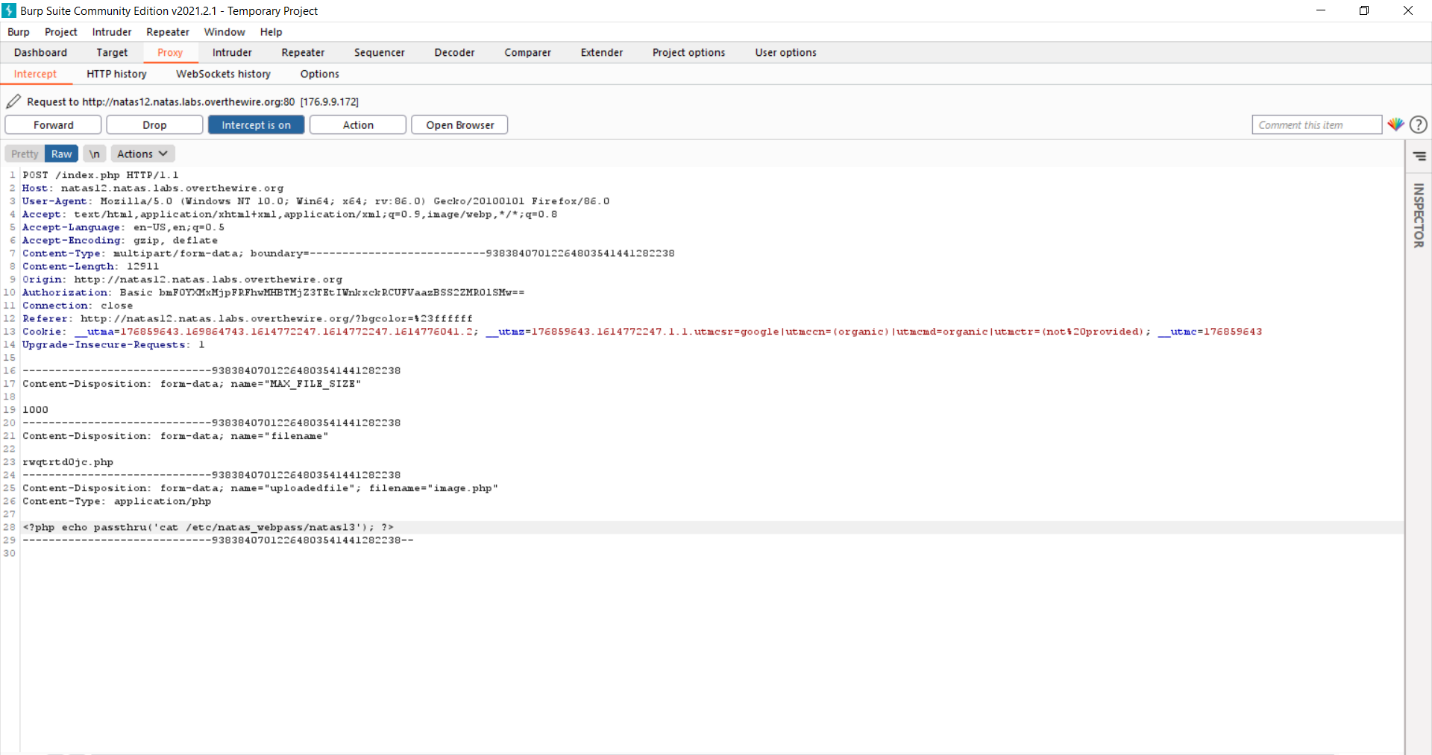
Level 12 – level 13

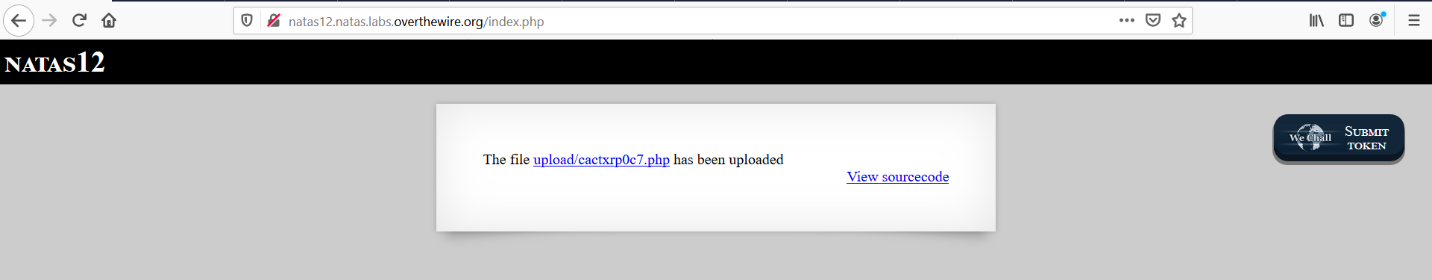
At this level, we have to upload a jpeg file. let's create and upload an image file.

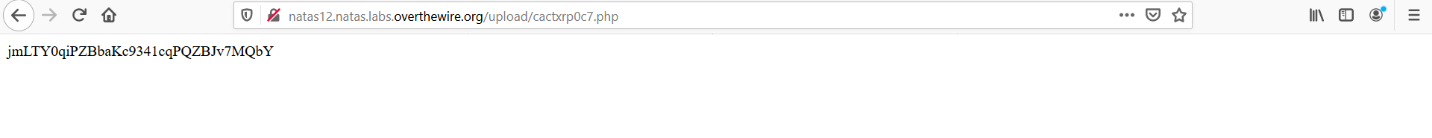
Now using burp suite to capture the HTTP request.

We can see some jpg files and we have to change these file extensions to PHP.next we change the content-type to application/php .now we can remove the image data and give a PHP script to find the password file.

<?php echo passthru('cat /etc/natas\_webpass/natas13'); ?>



Now we can forward the new request and turn off the intercept. next, we can see the file uploaded message from the browser.

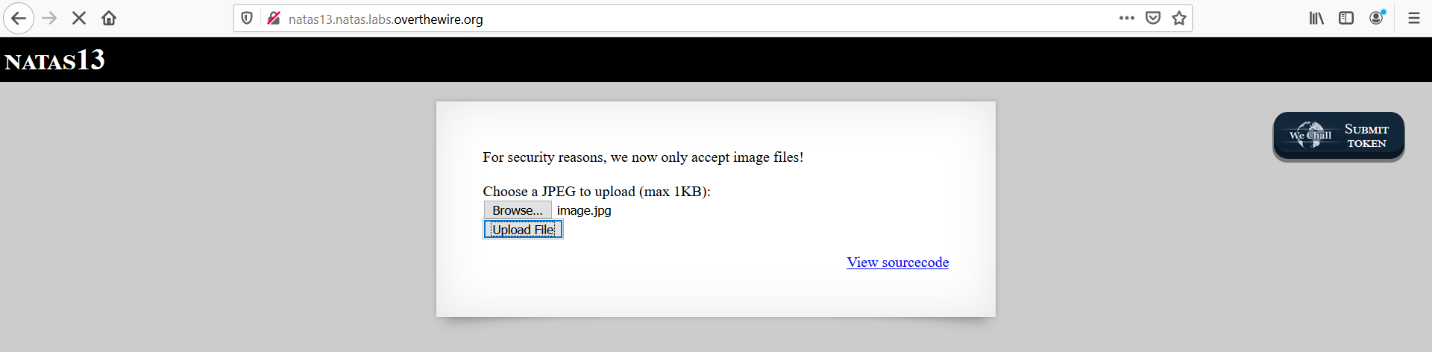
let's click on the file name.

Now we can see the password of level13.

Level 13-level 14

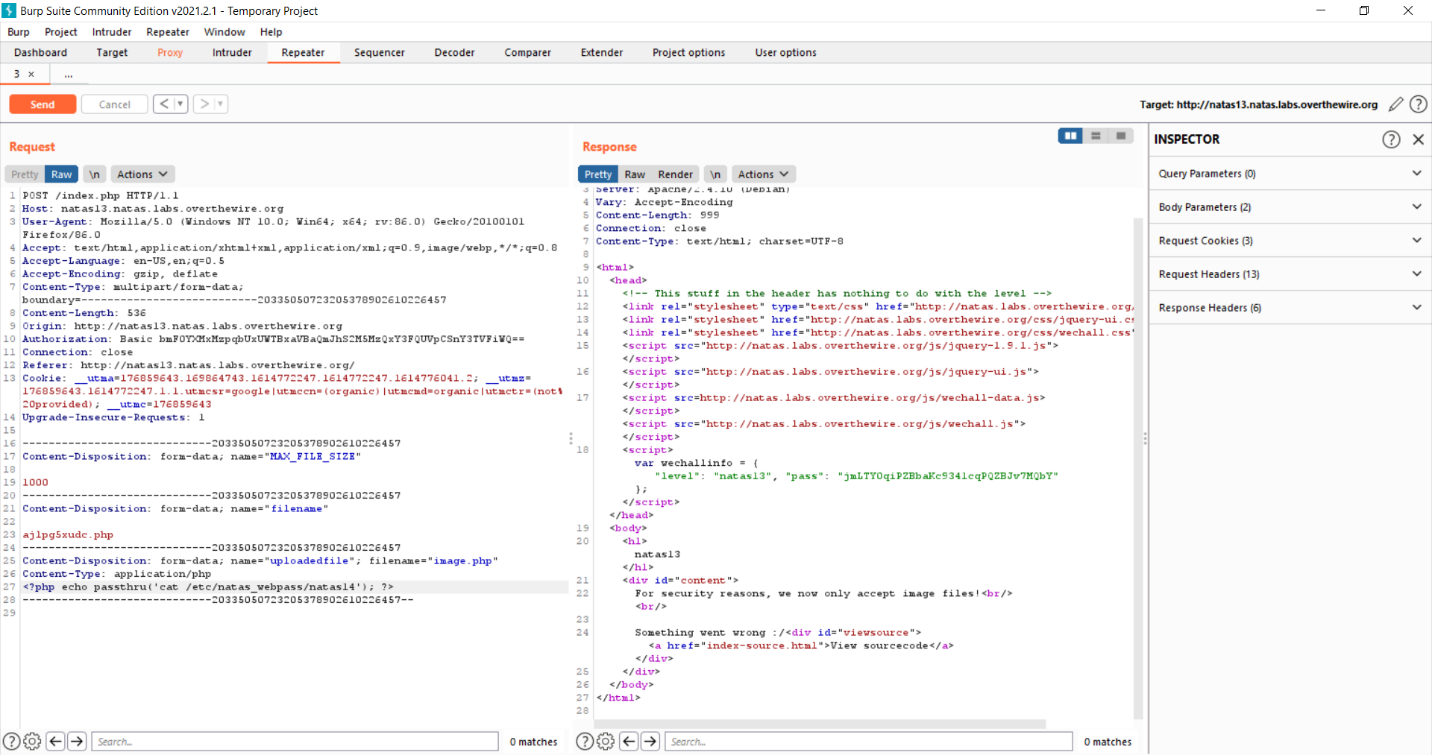
This level seems like level12 .but this time the upload accepts only image files.

Let's upload an image file and capture the request using the burp suite.

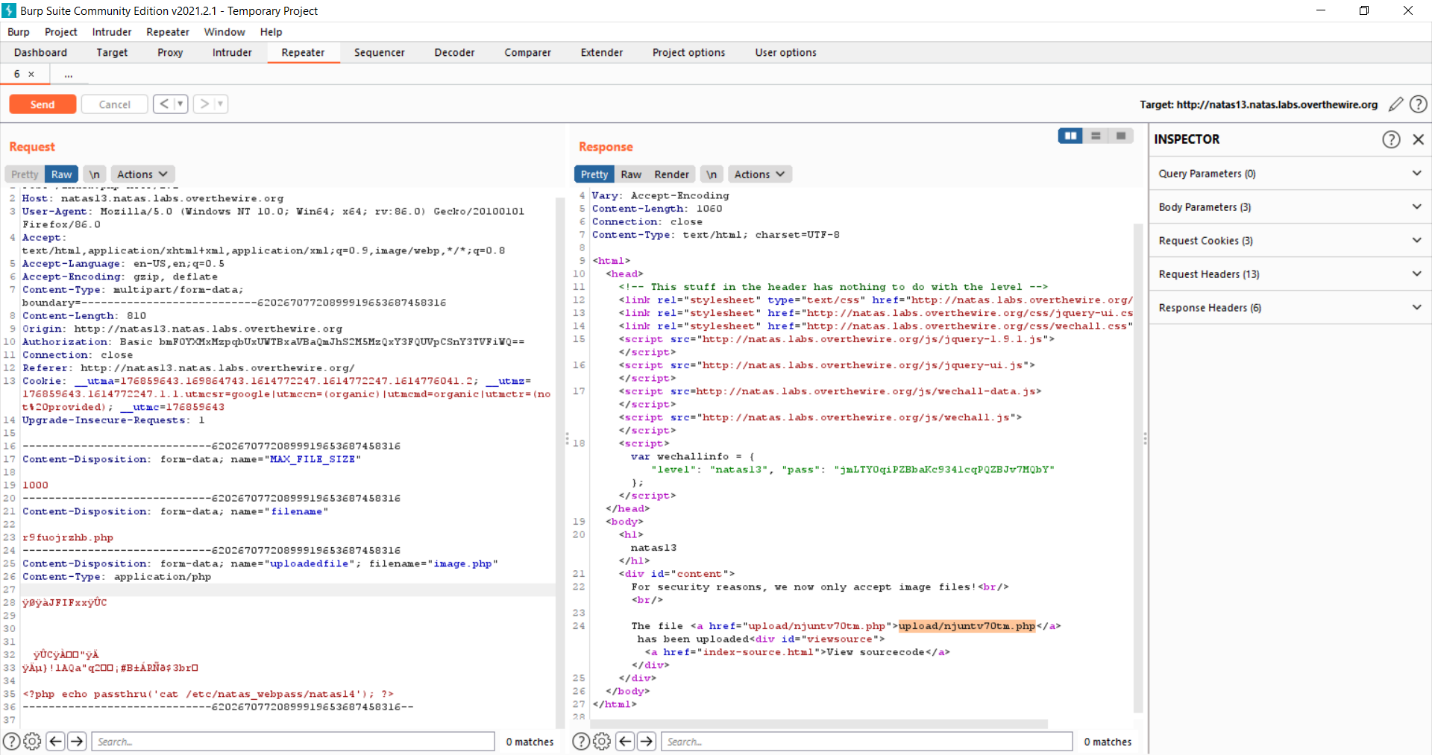


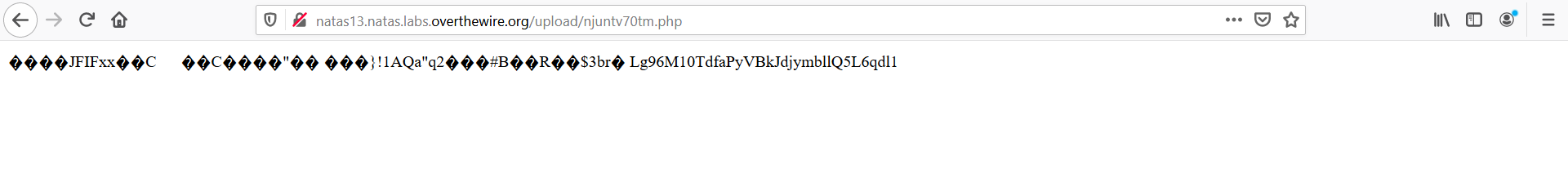


Now we send this request data to the repeater on burpsuite. after that we can change the jpg extension to PHP and change the content type to application/php.

Next, we give a PHP script to check is it working at this time as before. let's send this request.

This time website checks the file and confirms it’s an image file or not. so we cant use the previous method now.

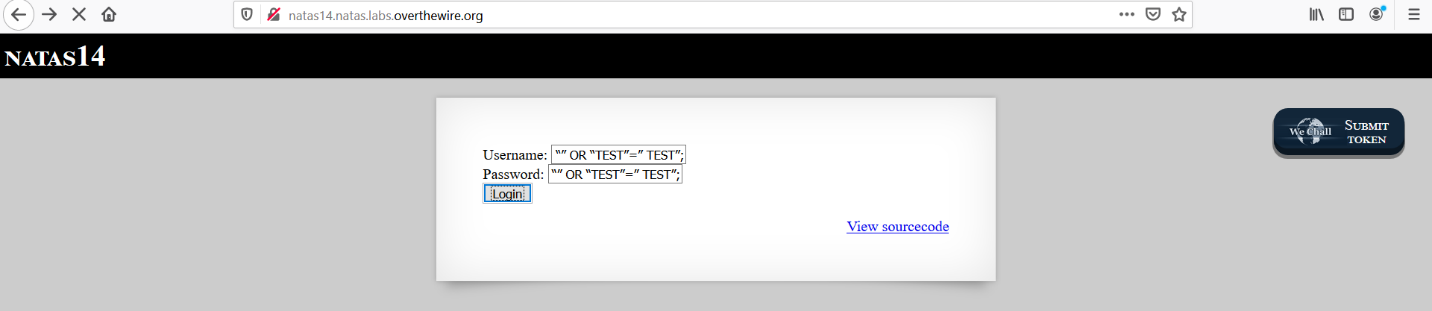
This time We can add a PHP script between the image header and footer data on the HTTP request.

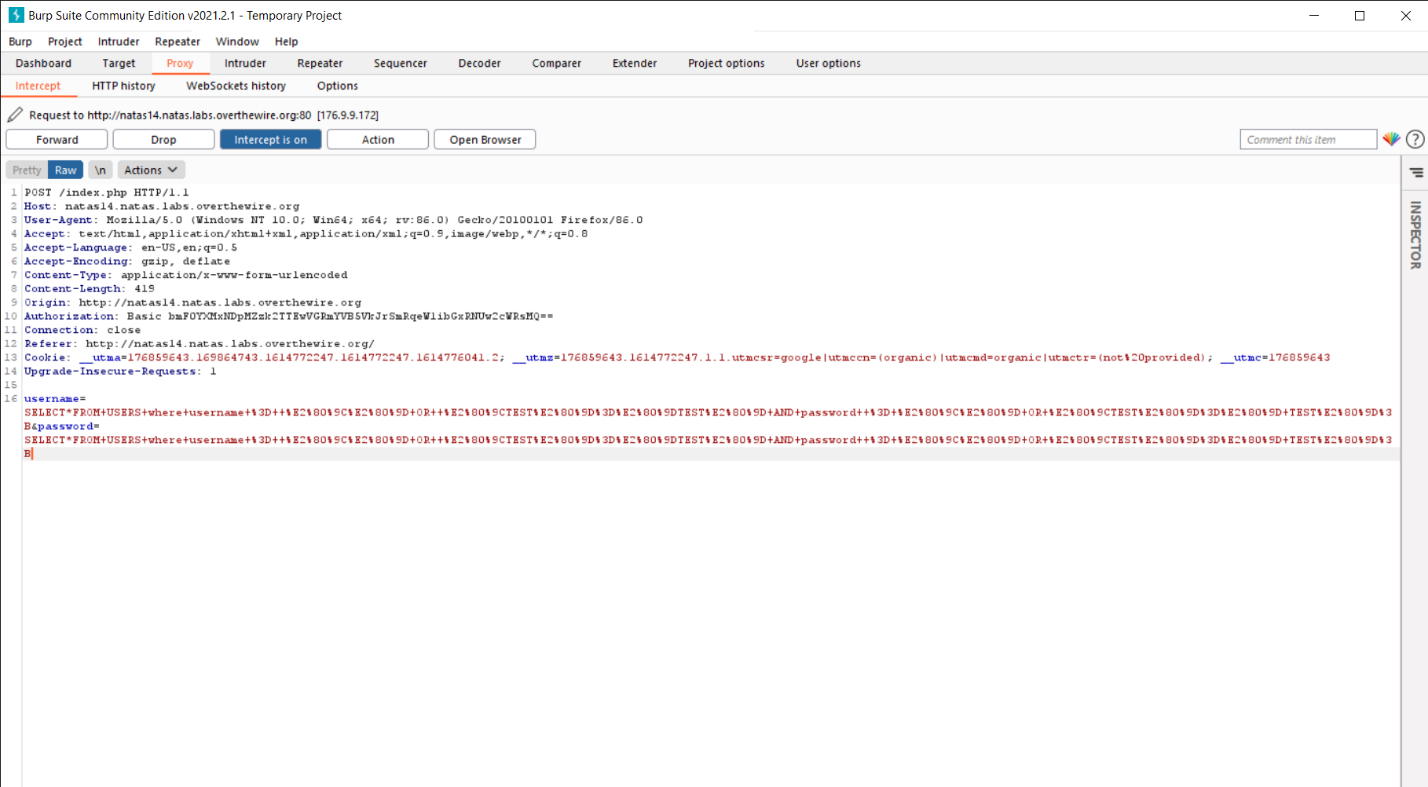
Now we can see an upload file so we can copy it to the URL and enter it. now we got the password to the next level.

Level 14 - level 15

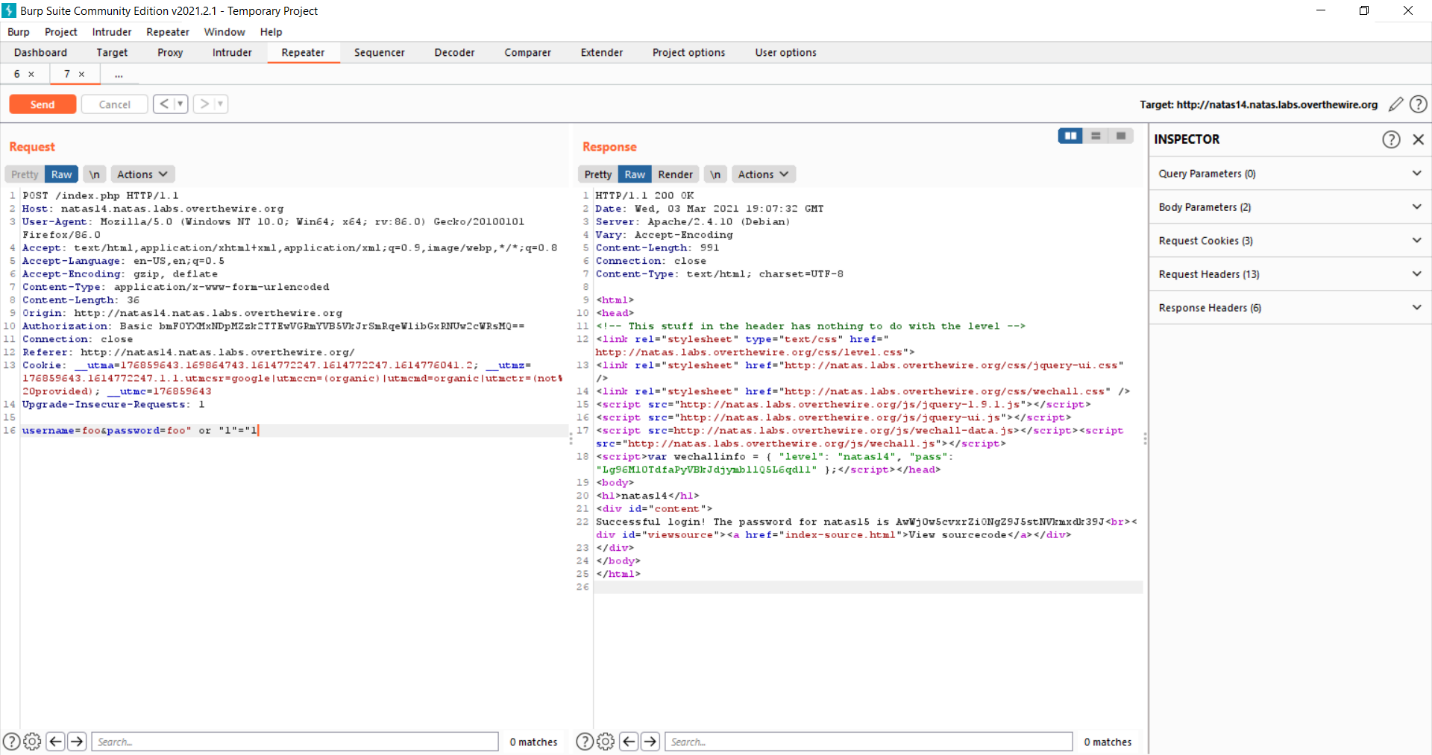
At this level, we have to do a SQL injection to extract the next level password.we can use this kind of SQL query to get the password

SELECT\*FROM USERS where username = “” OR “TEST”=”TEST” AND password = “” OR “TEST”=” TEST”;

We can Enter this query into the form and capture that request using burpsuite.

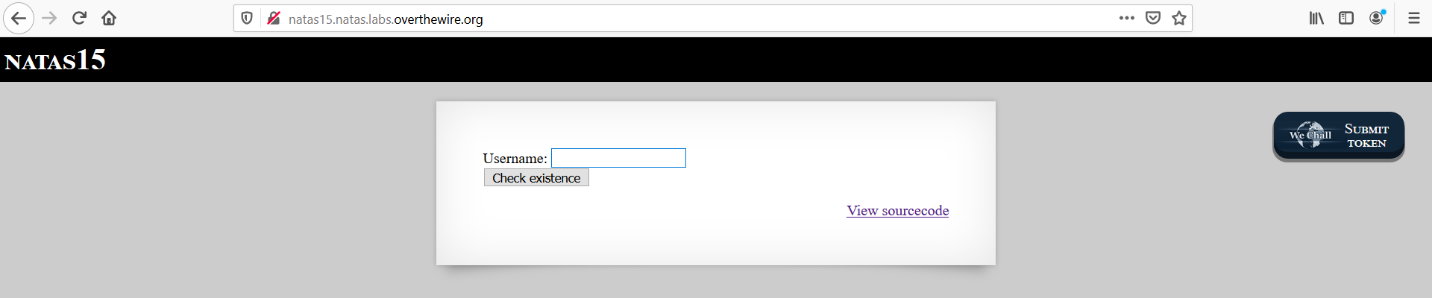


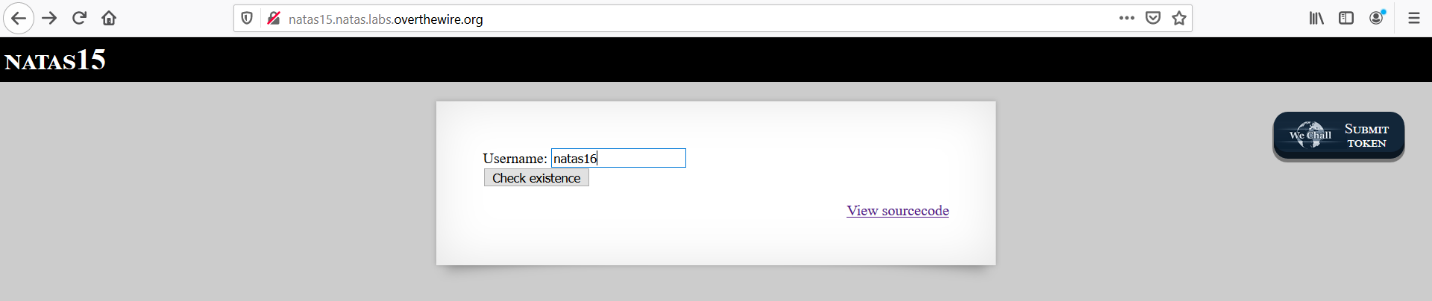
Now we can use the repeater to extract the password.

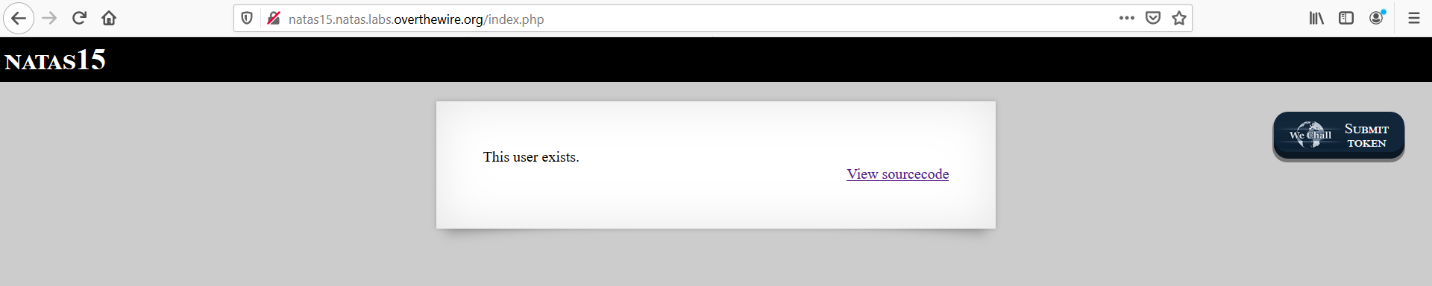
username=foo&password=foo” or “1”=”1

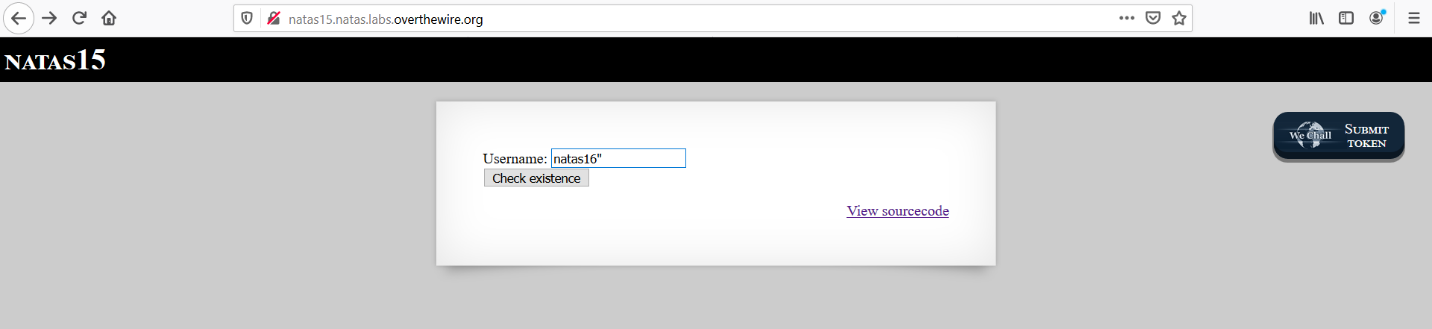
now we can see the password of natas15.

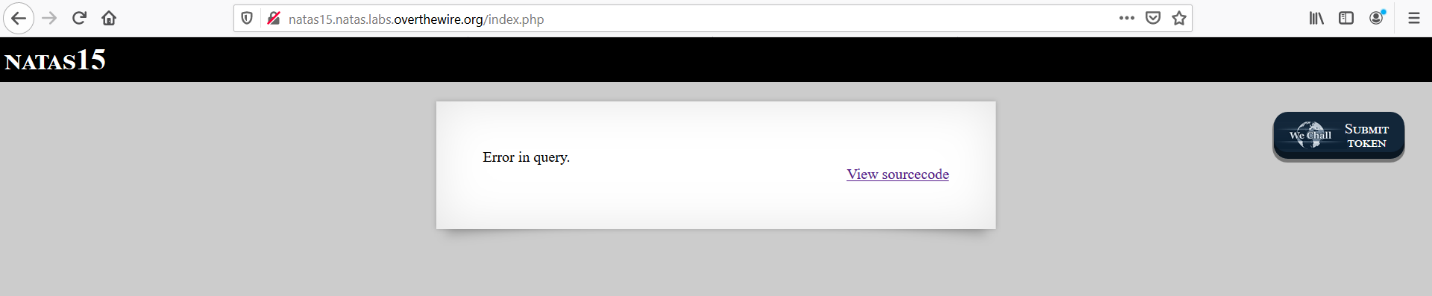
Level 15 – level 16

This time we have only the name field.

let's check natas15. we can see now, it does not exist. we can check natas16 next.it exists in the database. so let's check if the form response to a SQL injection. we can enter any word with double-quotes. now we can see a message it says error in the query. its means we can use a SQL injection without any problem.

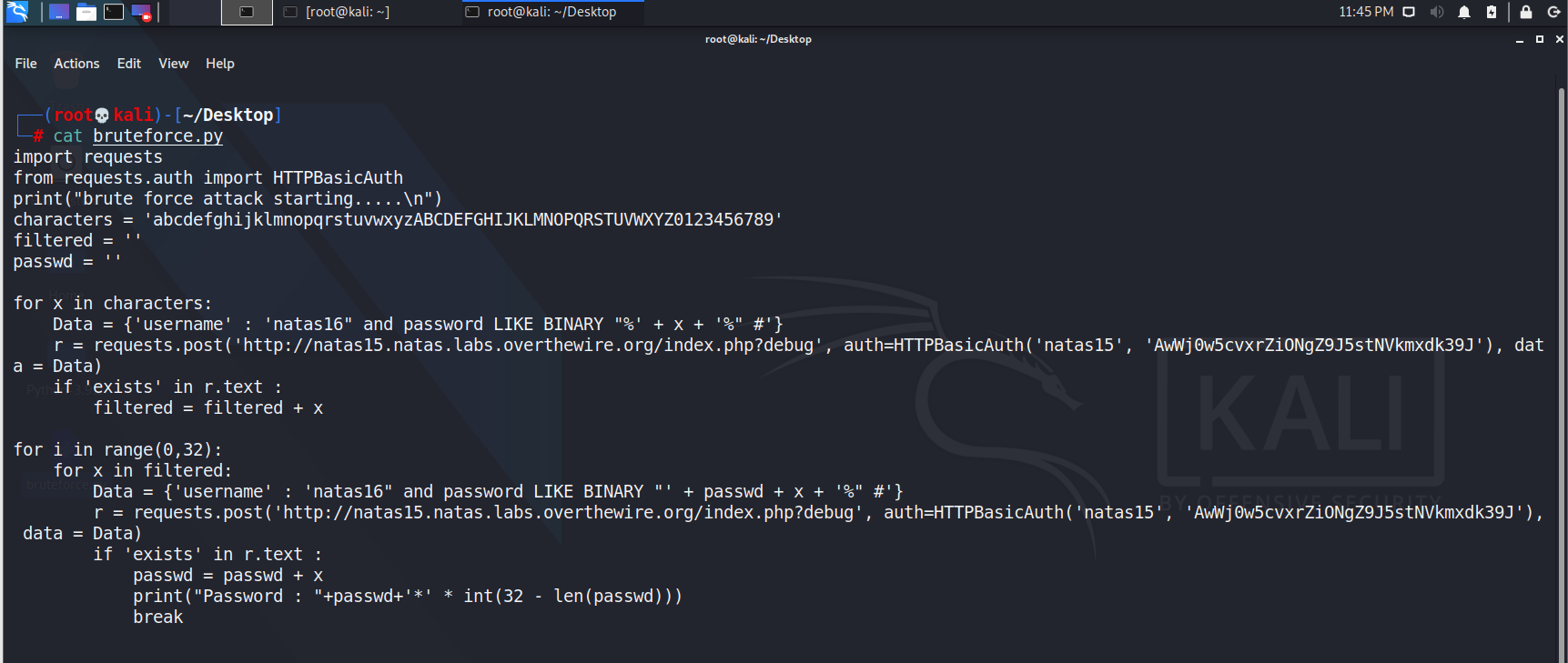






Now we have to look for natas16. we have to do a brute-force attack to get the password from the database. we can use Unix or Windows environment to launch the attack.so I created a python file including a python code.

**Python code**



For that, we can use python. using python we can send requests to natas15 with URL and username with password. so using this method we can send every letter to the database and make sure that letter exists on the database. after that, we can find the password.

To do that we should give 32 characters including letters and numbers. let's launch our python code.



Now we have the natas16 password.

I completed 15 levels of Natas wargame .this is the end of my presentation. thank you.