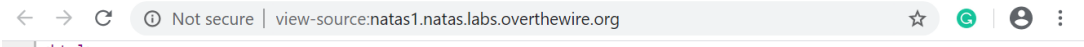
Level 0


```
<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>
```

The only thing I want to do is to view the page source first, then I get password for natas1 is 【gtVrDuiDfck831PqWsLEZy5gyDz1clto】
Time: 1 mins

Level 0 --> Level 1




```
<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>
```

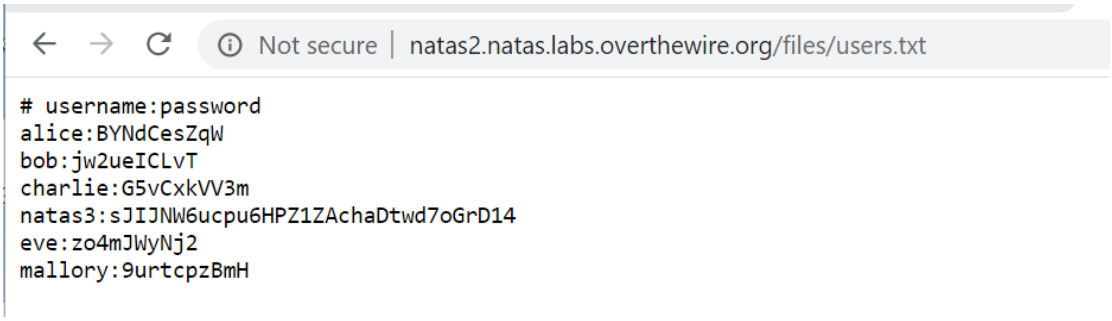
Right clicking blocked
To find another way to view the source page, press “Ctrl+U”
Then we find the password for natas2 is 【ZluruAthQk7Q2MqmDeTiUij2ZvWy2mBi】

Time:~5 mins

Level 1 --> Level 2

In source page, i see there is a img tag.

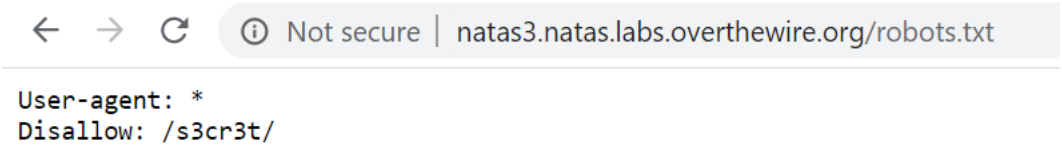
After i click it, it go to another website
http://natas2.natas.labs.overthewire.org/files/pixel.png
It didn't show anything. Let's see what under the /files. Then i delete the pixel.png
I see there is another files"users.txt"



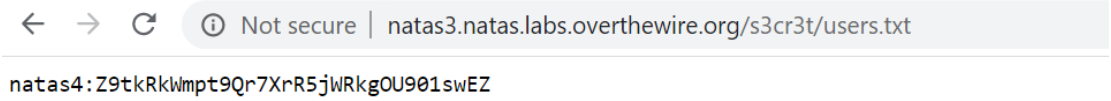
This might be the password, let's try
The password for natas3 is 【sJIJNW6ucpu6HPZ1ZAchaDtwd7oGrD14】

Time:~30mins

Level 2 --> Level 3
To view the source page, there is an weird sentence" Not even Google will find it this time.."
We know that Robots.txt is the first file to be viewed when accessing a website in a search engine.
It will tell the spider what files are viewable on the server.
Add robots.txt to the end of URL: http://natas3.natas.labs.overthewire.org/robots.txt



Then we can see that access to the directory under / s3cr3t / is prohibited
Let's try http://natas3.natas.labs.overthewire.org/s3cr3t/

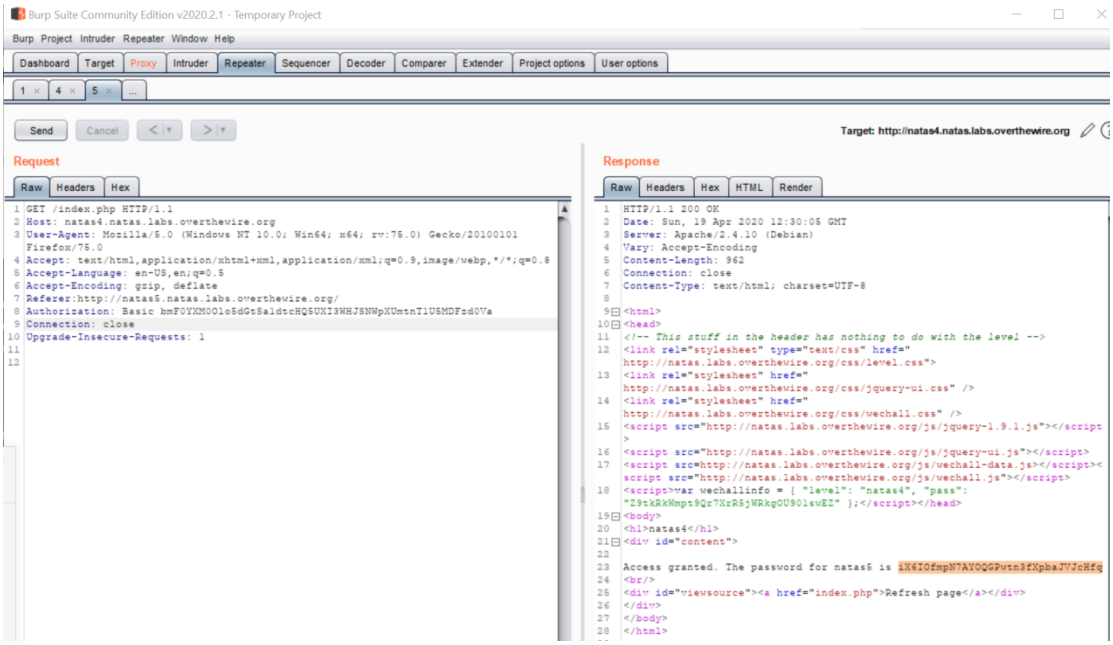


The password for natas4 is 【Z9tkRkWmpt9Qr7XrR5jWRkgOU901swEZ】

Time:~40 mins

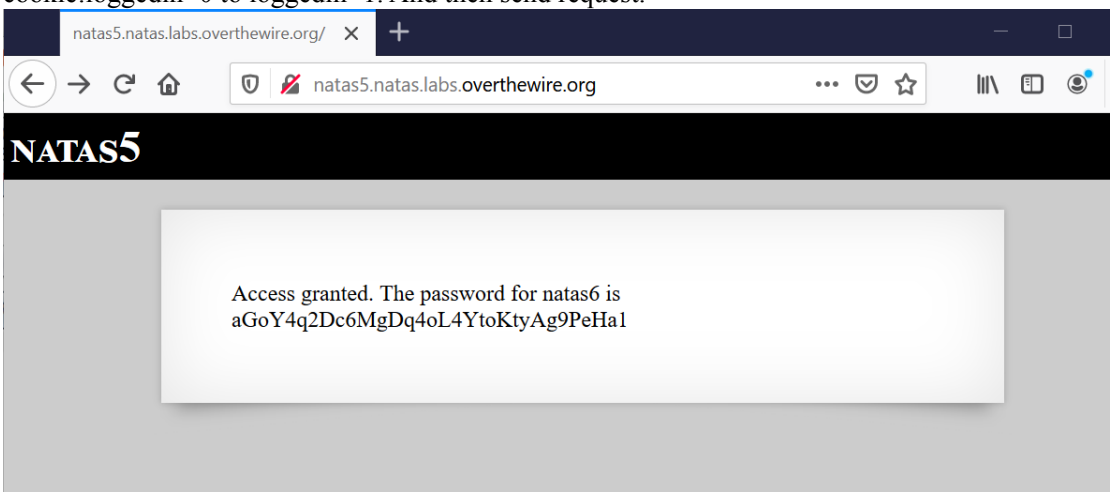
Level 3 --> Level 4
This one is a little bit challenge for me. I need to think about How to trick the server that we come from natas5? It take me a long time to learn about referer, which is part of the HTTP request header. When the browser sends a request to the web server, the referer will tell the server which web page I came from. So i need to change the referer in order to trick the website.I open the

webpage in firefox, and then connecting to burp suite. Then I use burp to intercept the packet. And then change referer to http://natas5.natas.labs.overthewire.org/.



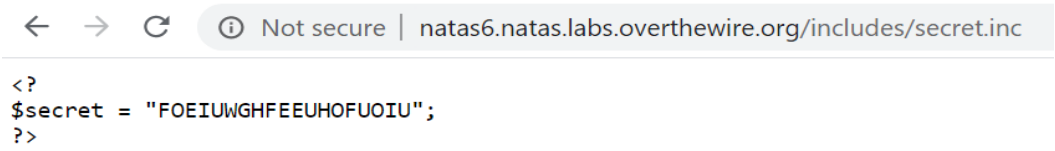
Access granted. The password for natas5 is【iX6IOfmpN7AYOQGPwtn3fXpbaJVJcHfq】
Time:~3 hours

Level 4 --> Level 5
Similar with last one. Trick the website we logged in. Use burp suite and then change cookie:loggedin=0 to loggedin=1. And then send request.



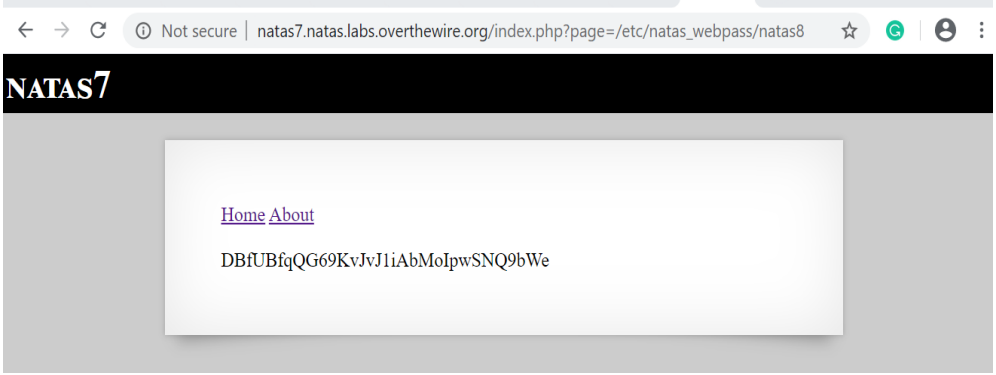
Access granted. The password for natas6 【aGoY4q2Dc6MgDq4oL4YtoKtyAg9PeHa1】
Time:~30 mins

Level 5 --> Level 6
In the source code it looks like that the secret hide under “includes/secret.inc”
Let’s check it out
http://natas6.natas.labs.overthewire.org/includes/secret.inc



After input the secret "FOEIUWGHFEEUHOFUOIU". I get the password for natas7 is 【7z3hEENjQtflzgnT29q7wAvMNfZdh0i9】
Time:~30 Mins

Level 6 --> Level 7
After click "Home" and "About", I didn't get anything
So go to the source page, I see a hint.
Let's try
http://natas7.natas.labs.overthewire.org/index.php?page=/etc/natas_webpass/natas8
Then I get



The password for natas8 is 【DBfUBfqQG69KvJvJ1iAbMoIpwSNQ9bWe】

Time:~30 Mins

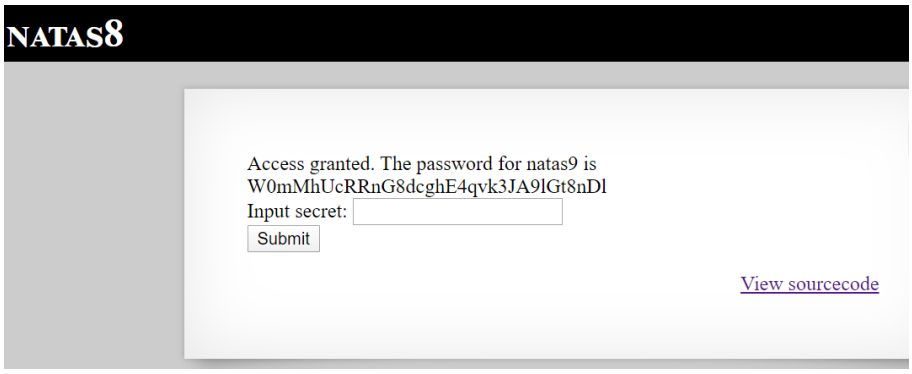
Level 7 --> Level 8
I see there is a "encodedSecret" in source code.
We might need to decoded the secret. Through the given function, to decode the secret, we need to base64 decoding it and then reversed, then convert it back to binary.

```
<?php
echo base64_decode(strrev(hex2bin('3d3d516343746d4d6d6c315669563362')));
```

Run Code

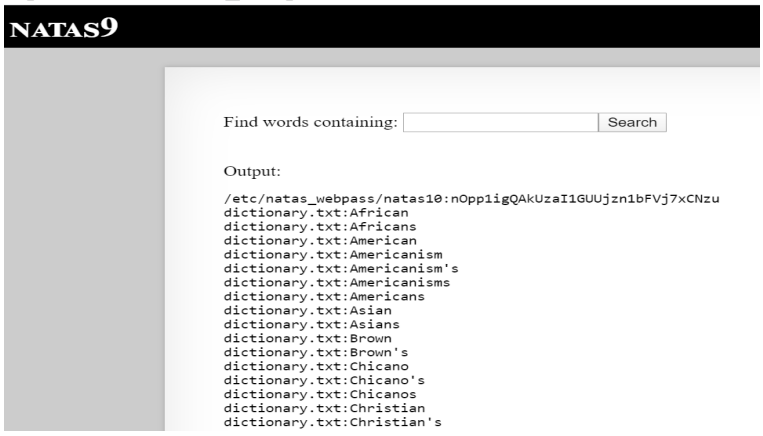
```
oubWYf2kBq
```

Then I get “oubWYf2kBq”



After input it. The password for natas9 is 【W0mMhUcRRnG8dcghE4qvk3JA9lGt8nDl】
Time:~ 1.5 hours

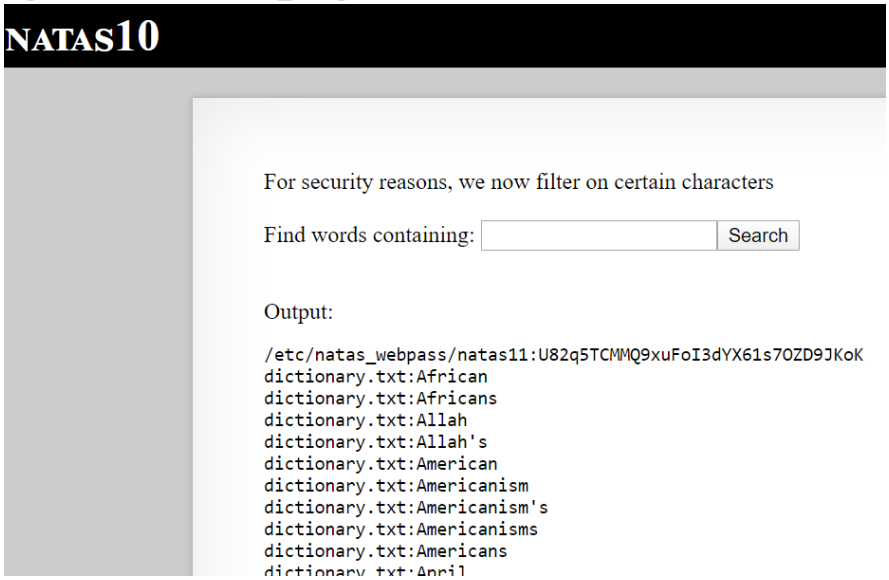
Level 8 --> Level 9
After reading the source code, we know that needle submits the parameters through the get request. If it is not empty, it will be taken to "grep -i $ key dictionary.txt" for execution. So the code allows us to find words in the dictionary.txt file. I first type “\ n” to see what is in this txt. A lot of things are returned, but we have to find what we need. In level 7, the passcode is located in / etc / natas_webpass. So I tried “\ n / etc / natas_webpass / natas10”
Input：\n /etc/natas_webpass/natas10



I get the password for natas10 is 【nOpp1igQAkUzaI1GUUjzn1bFVj7xCNzu】
Time:~ 2 hours

Level 9 --> Level 10
This is very similar to the previous one, I try “ \ n / etc / natas_webpass / natas11” firstly . But I didn't see what I wanted. Then the sentence says filter on certain characters, and the code state that “; | &” are illegal character. So I try “[a-z] / etc / natas_webpass / natas11” next. (case does not matter)

Input：[a-z] / etc / natas_webpass / natas11



I get the password for natas11 is 【U82q5TCMMQ9xuFoI3dYX61s7OZD9JKoK】

Time:~30 mins