

NATAS Write up

Level 0 → 1

- View the page source and the password is given under div content tag for level 1

```
→ ↻ ⓘ Not secure | view-source:ntas0.natas.labs.overthewire.org

<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://ntas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://ntas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://ntas.labs.overthewire.org/css/wechall.css" />
<script src="http://ntas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
<script src="http://ntas.labs.overthewire.org/js/jquery-ui.js"></script>
<script src="http://ntas.labs.overthewire.org/js/wechall-data.js"></script><script src="http://ntas.labs.overthewire.org/js/wechall.js"></script>
<script>var wechallinfo = { "level": "ntas0", "pass": "ntas0" };</script></head>
<body>
<h1>ntas0</h1>
<div id="content">
You can find the password for the next level on this page.

<!--The password for ntas1 is gtVrDuiDfck831PqWsLEZy5gyDz1clto -->
</div>
</body>
</html>
```

The password for ntas1 is gtVrDuiDfck831PqWsLEZy5gyDz1clto

Level 1 → 2

- This page does not allow us to right-click on the page but if you just use a shortcut you can still get to the next level.
- I choose to view source using control-u

```
← → ↻ ⓘ Not secure | view-source:ntas1.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://ntas.labs.overthewire.org/css/level.css">
5 <link rel="stylesheet" href="http://ntas.labs.overthewire.org/css/jquery-ui.css" />
6 <link rel="stylesheet" href="http://ntas.labs.overthewire.org/css/wechall.css" />
7 <script src="http://ntas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
8 <script src="http://ntas.labs.overthewire.org/js/jquery-ui.js"></script>
9 <script src="http://ntas.labs.overthewire.org/js/wechall-data.js"></script><script src="http://ntas.labs.overthewire.org/js/wechall.js"></script>
10 <script>var wechallinfo = { "level": "ntas1", "pass": "gtVrDuiDfck831PqWsLEZy5gyDz1clto" };</script></head>
11 <body oncontextmenu="javascript:alert('right clicking has been blocked!');return false;">
12 <h1>ntas1</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 ntas2 is ZluruAthQk7Q2MqmDeTiUij2ZvWy2mBi -->
18 </div>
19 </body>
20 </html>
21
22
```

The password for ntas2 is ZluruAthQk7Q2MqmDeTiUij2ZvWy2mBi

Level 2 → 3

- This page i went straight into the source code which revealed that image exists on the webpage and it stored in files folder

```
← → ↻ ⓘ Not secure | view-source:natas2.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": "natas2", "pass": "ZluruAthQk7Q2MqmDeTiUij2ZvWY2mBi" };</script></head>
11 <body>
12 <h1>natas2</h1>
13 <div id="content">
14 There is nothing on this page
15 
16 </div>
17 </body></html>
18
```

- Next I choose to go to the URL and append to add /files, this resulted in showing a users.txt file also, as seen below

```
← → ↻ ⓘ Not secure | natas2.natas.labs.overthewire.org/files/
```

Index of /files

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 pixel.png	2016-12-15 16:07	303	
 users.txt	2016-12-20 05:15	145	

Apache/2.4.10 (Debian) Server at natas2.natas.labs.overthewire.org Port 80

- I opened the users.txt file and the password was contained within the text document.

```
← → ↻ ⓘ Not secure | natas2.natas.labs.overthewire.org/files/users.txt
```

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

natas3:sJIJNW6ucpu6HPZ1ZAchaDtwd7oGrD14

Level 3 → 4

- I first headed to the source which revealed a hint stating that Not even Google will find it this time. I had then assumed that this has to do with the robots.txt web crawler websites have to allow Google and other search engines to index websites for the internet

← → ↻ ⓘ Not secure | natas3.natas.labs.overthewire.org/robots.txt

User-agent: *
Disallow: /s3cr3t/

- Within i had then searched up the disallow agent, to see what is contained within that file within the webpage, which opened a file that contained users.txt and again that users.txt contained the password for level 4.

← → ↻ ⓘ Not secure | natas3.natas.labs.overthewire.org/s3cr3t/

Index of /s3cr3t

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<hr/>			
 Parent Directory		-	
 users.txt	2016-12-20 05:15	40	

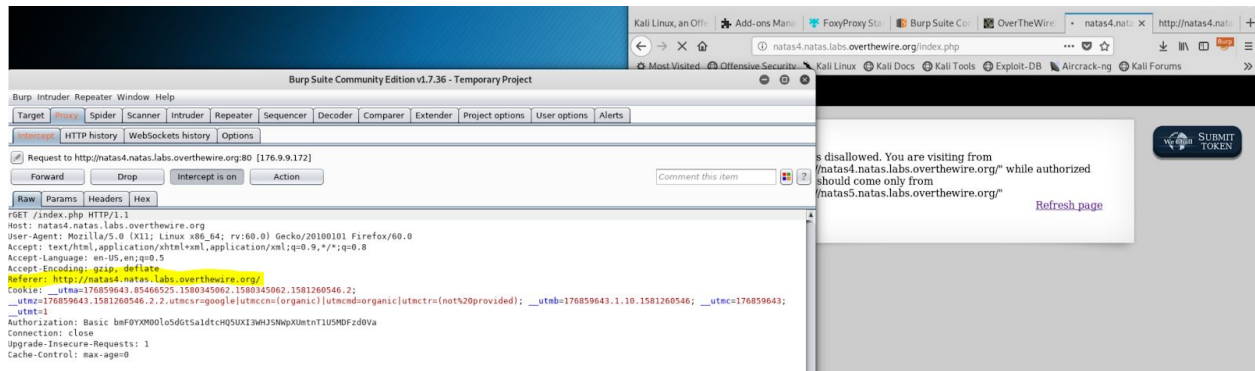
Apache/2.4.10 (Debian) Server at natas3.natas.labs.overthewire.org Port 80

natas4:Z9tkRkWmpt9Qr7XrR5jWRkgOU901swEZ

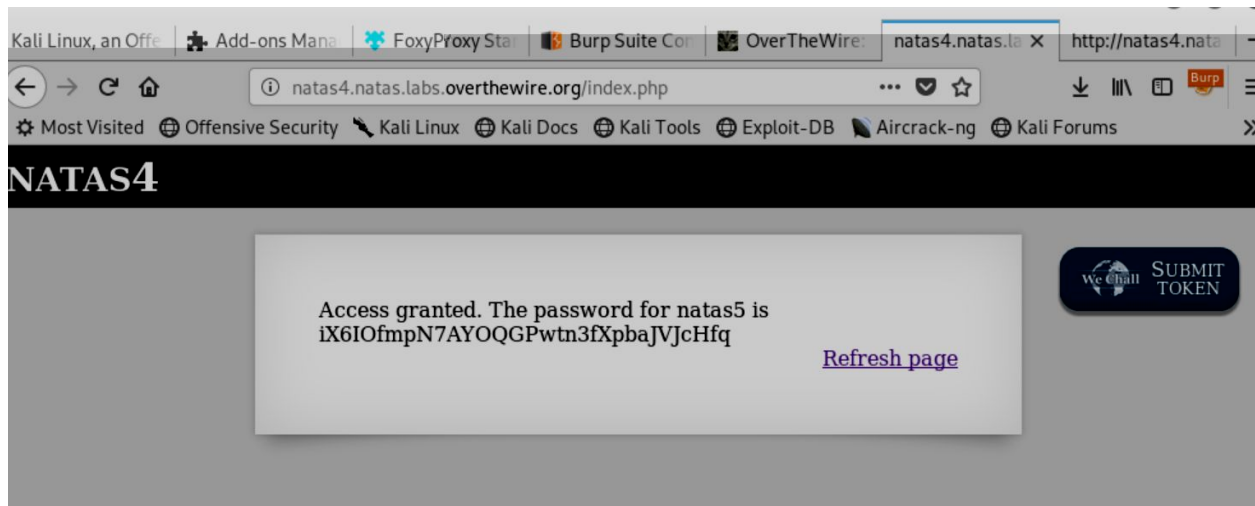
Level 4 → 5

For this level I had to change to use Kali as i needed to inspect packets using burp suite

- The first thing was to start up burp suite (note i changed to use Maz implementation of burp proxy using an add on)
- At first the header seemed fine, but once I clicked on refresh the raw intercept showed me a referrer, as shown down below



- I just changed the referer to be natas5 and forwarded the packet, this then gave me the password on a new page as displayed below



natas5 is iX6IOfmpN7AYOQGPwtn3fXpba4

Level 5 → 6

Tip: Turn off anti virus shield and if you don't it won't let you on to natas 5

- Just change the user cookie parameter to 1 instead of 0 to make it true.

Level 6 → 7

- Go to the /include/secret file that was provided in the source code
- Input that into the natas 6 secret prompt given and the webpage changes and give out the password