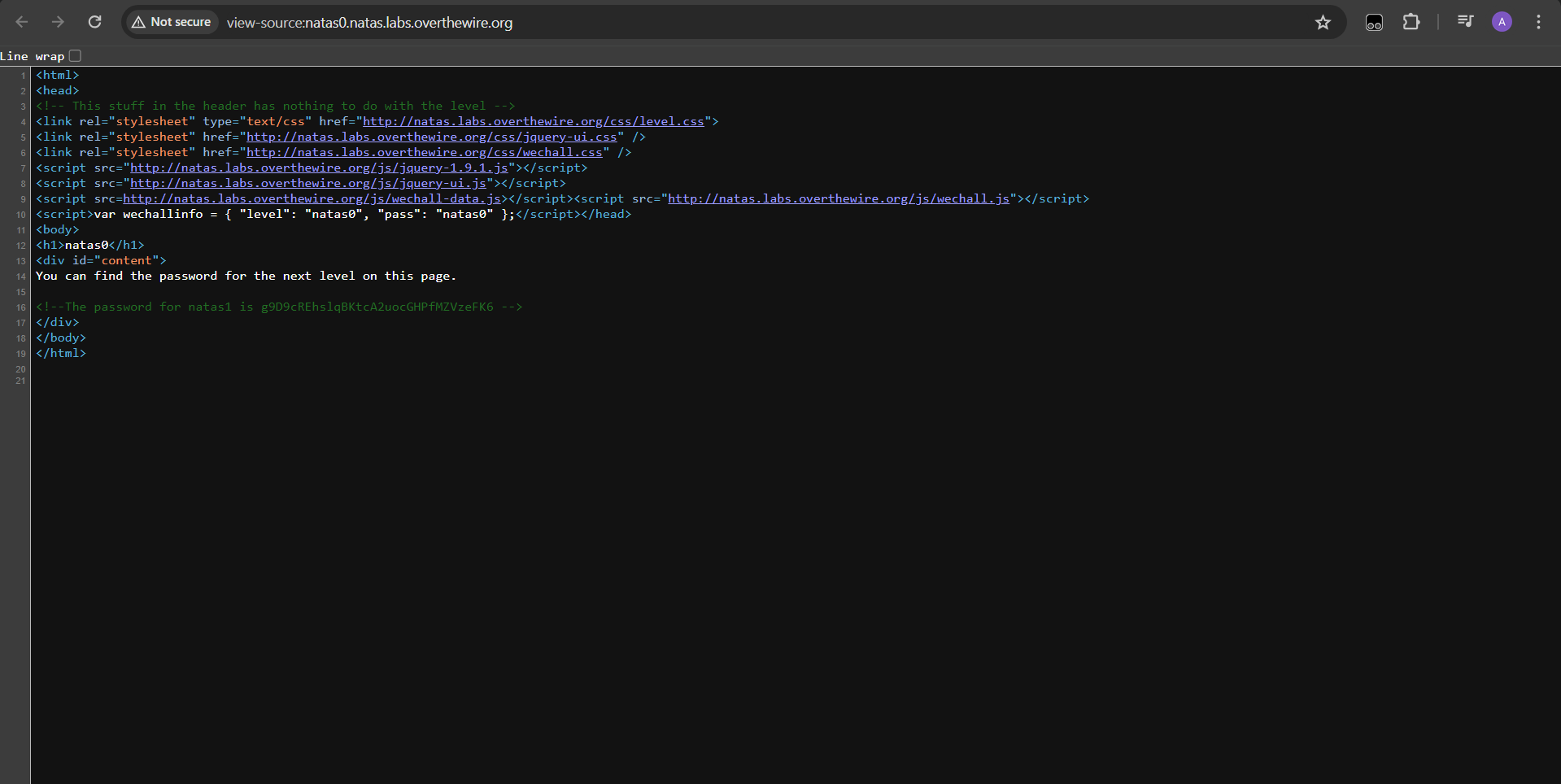
**SIG CYBERSECURITY**

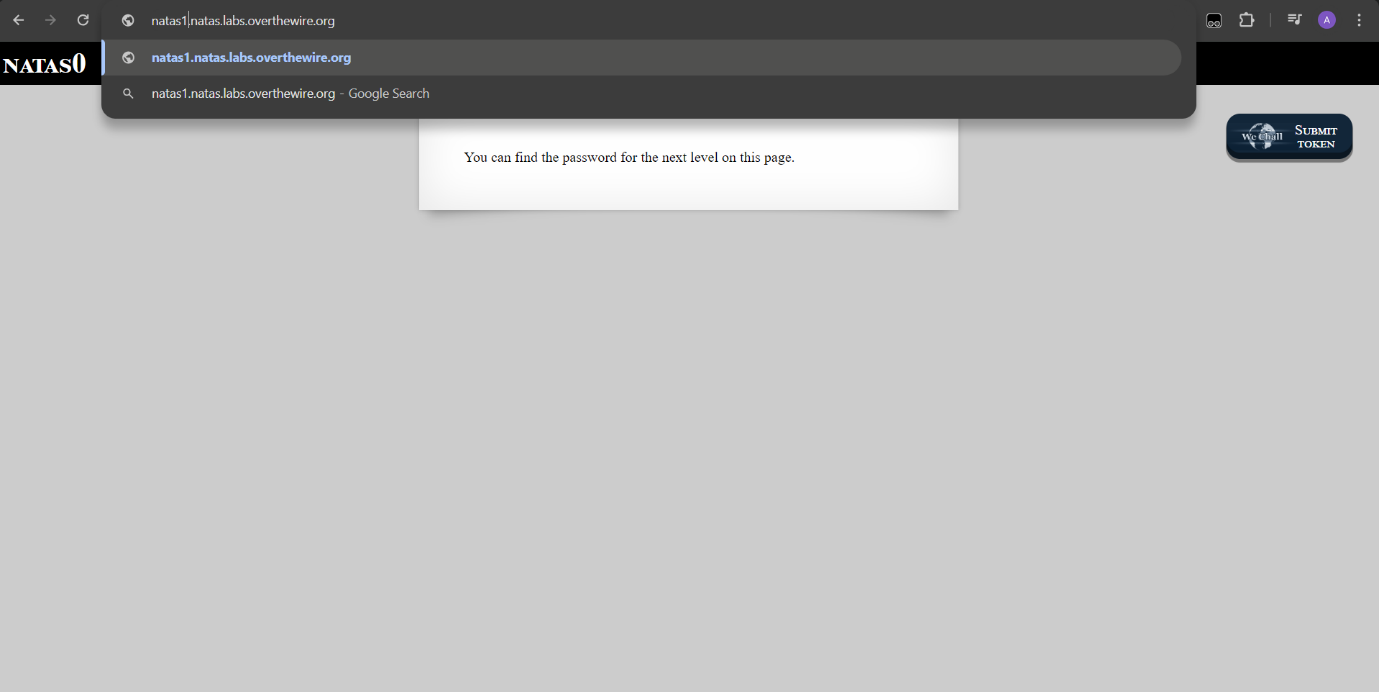
**NATAS wargame solving: by Arjun T**

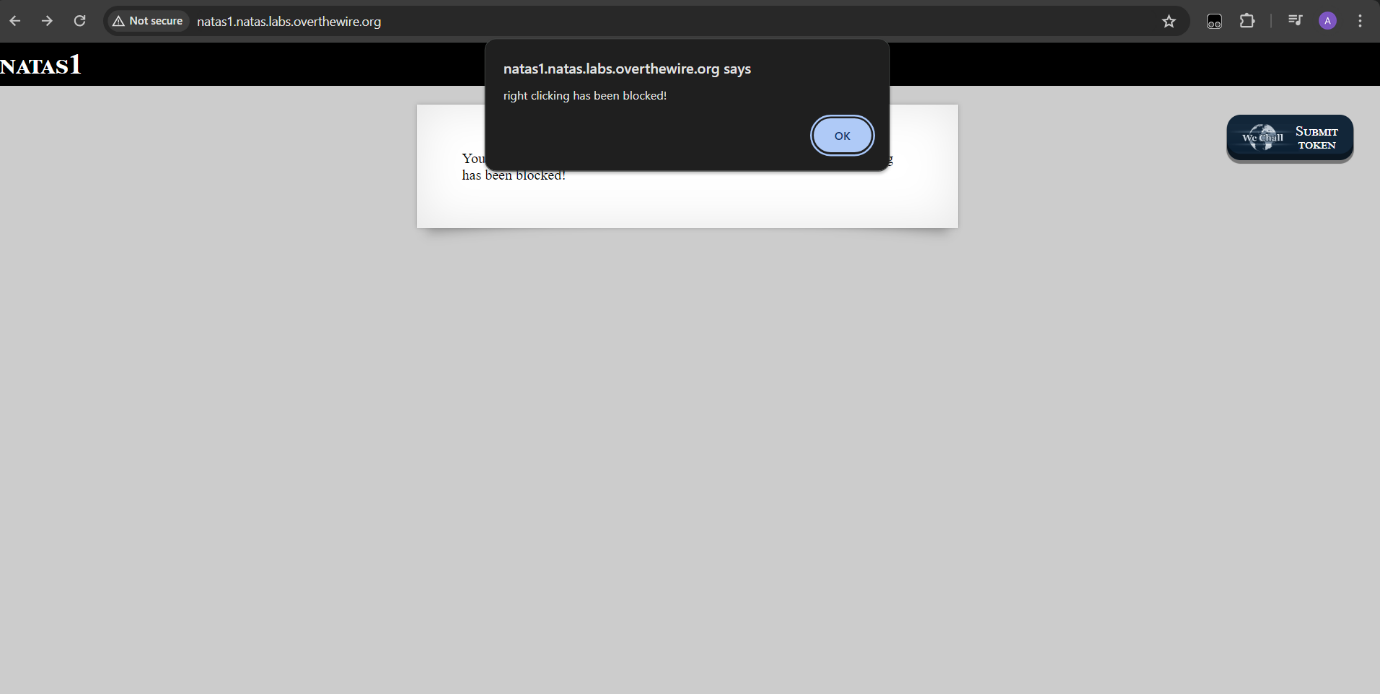
**Natas0**

****

by entering the page source, we get the password for natas1.

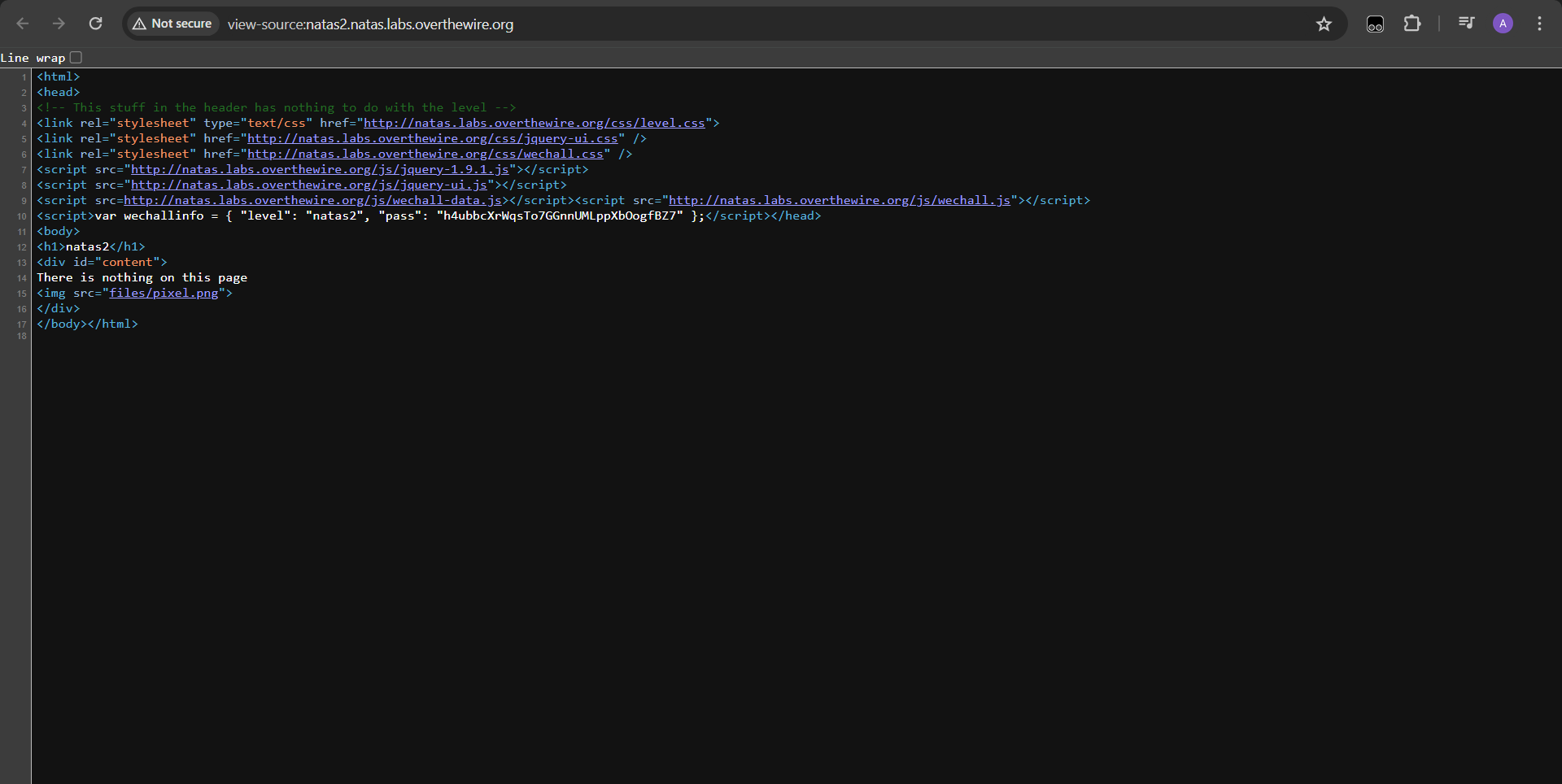
**Natas1**



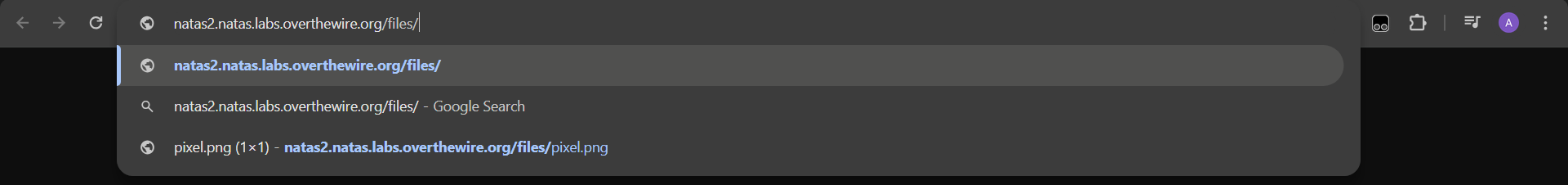


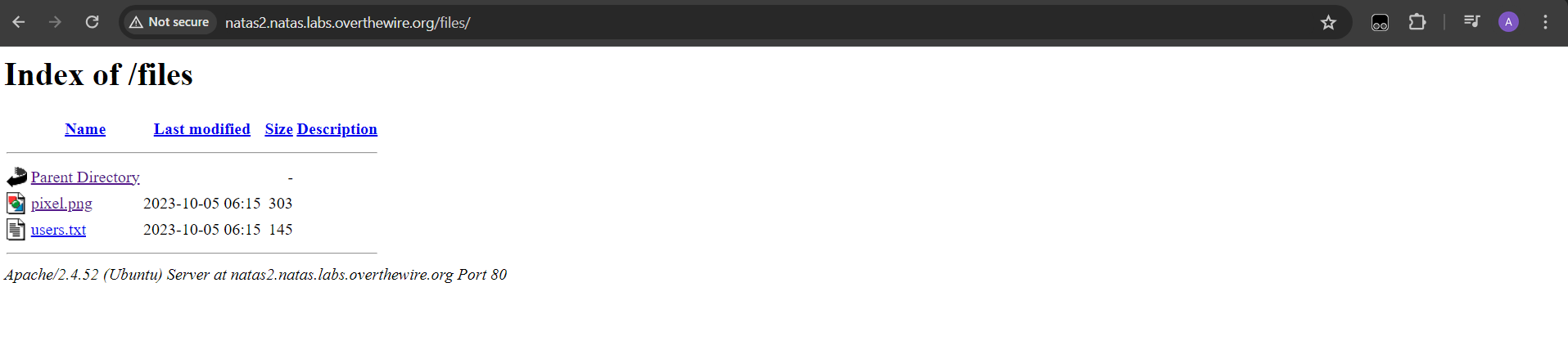
We can’t right click on this page, so I used keyboard shortcut ctrl + u to view source code to get the password for natas2

**Natas lvl2**



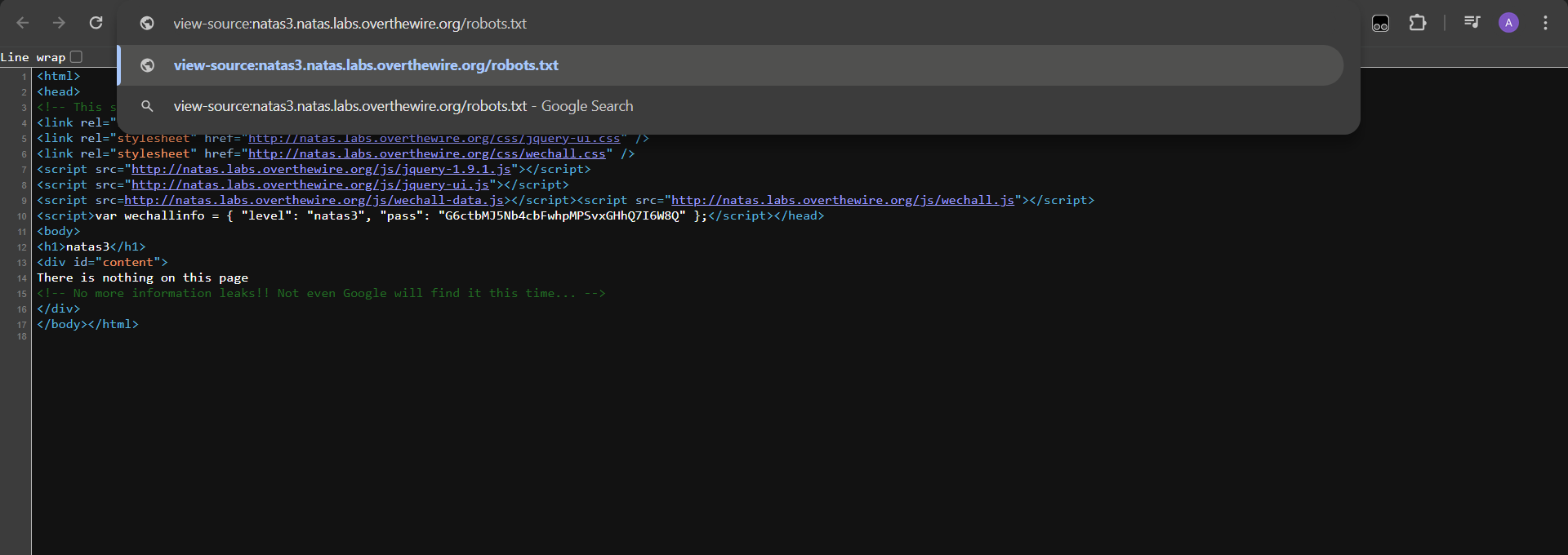
We can see a 1x1 png file here, so if we go the file directory, we could get something.



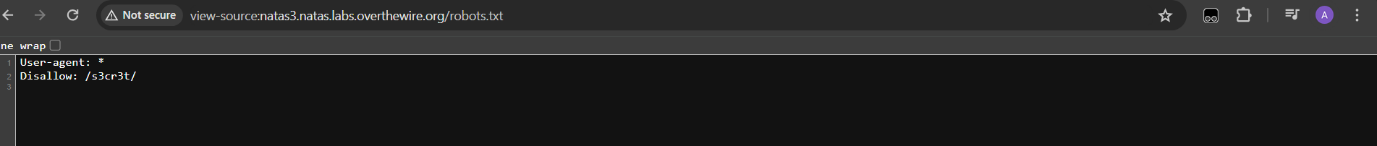


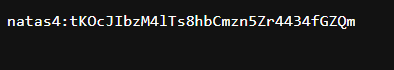
when we look inside user.txt file, we have the password for natas3 right there.

**Natas lvl3**



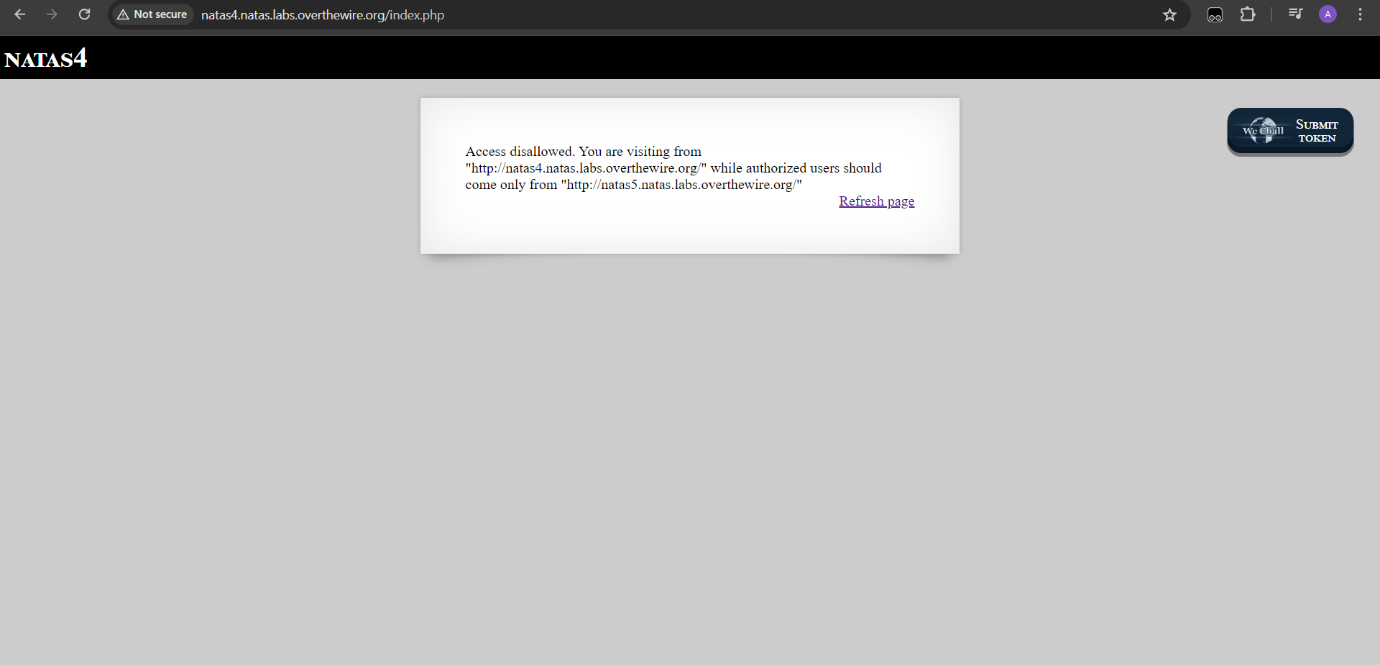
Here we can see, there is nothing and we are blocked use some file, so if we go the /robots.txt , we could see which file is hidden from us.





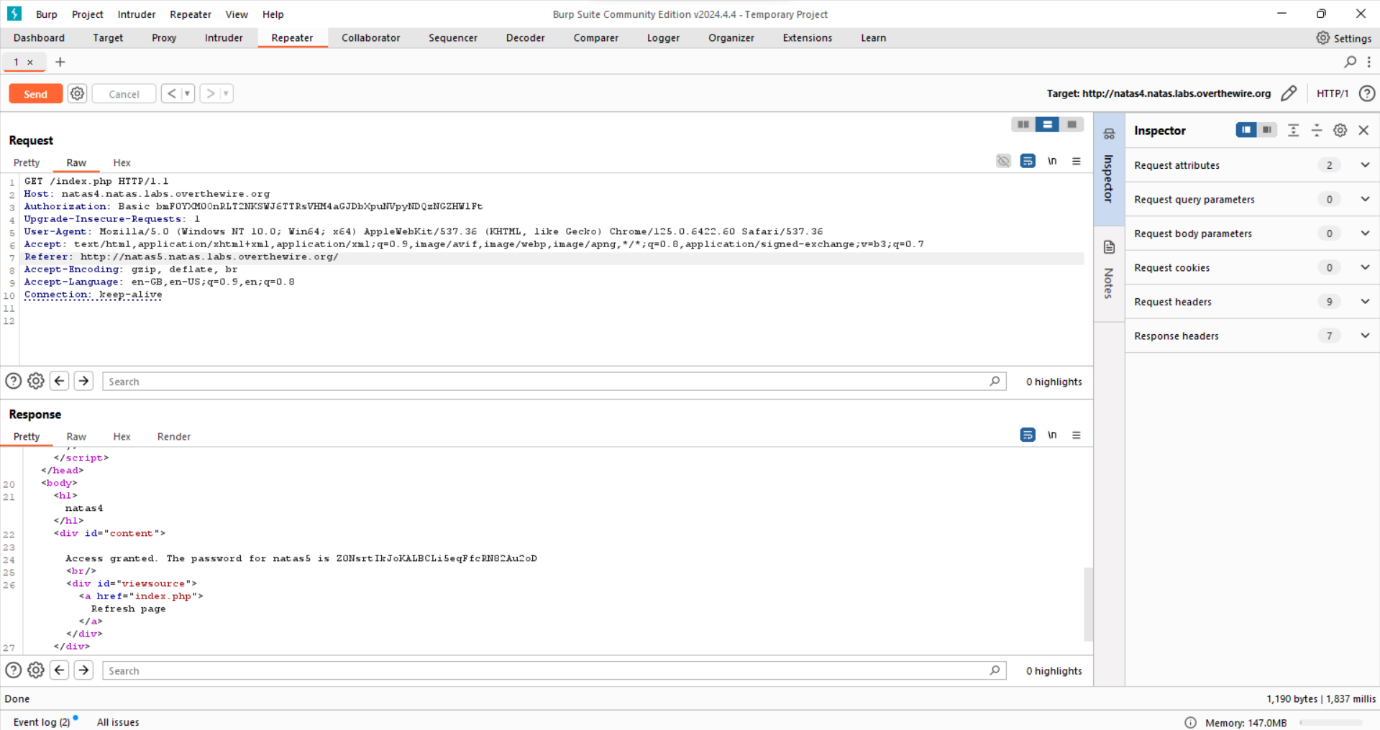
we will get the password for next lvl from given directory.

**Natas lvl4**

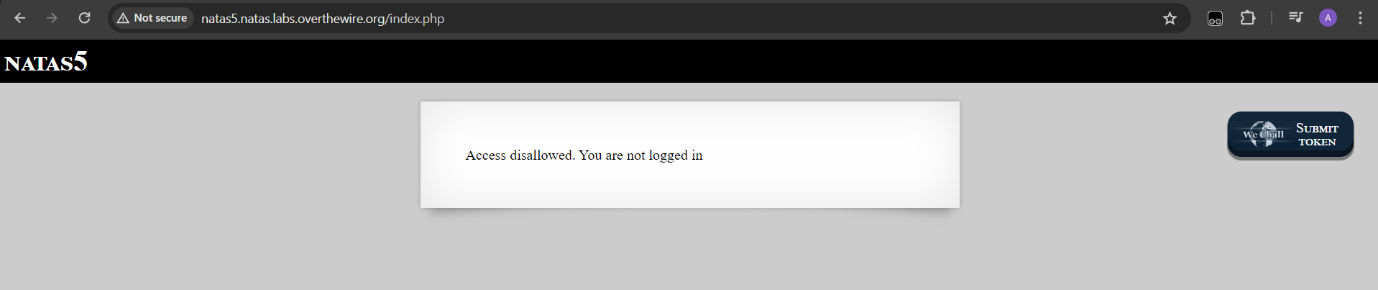
****

Every browser has a thing called referrer. If we are using a site that holds a link to another site, definitely the other site knows where you are coming from and we need to intercept that request and change the referrer

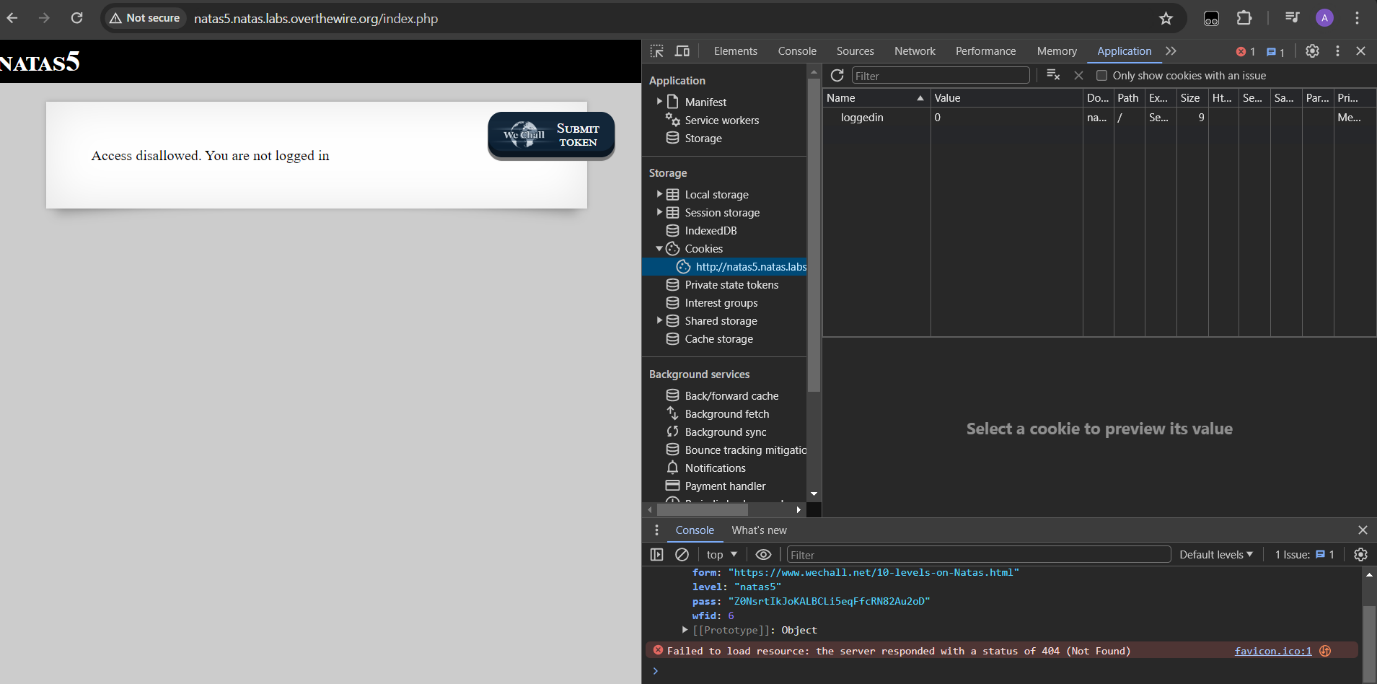
So here we are using burb suite to tackle that



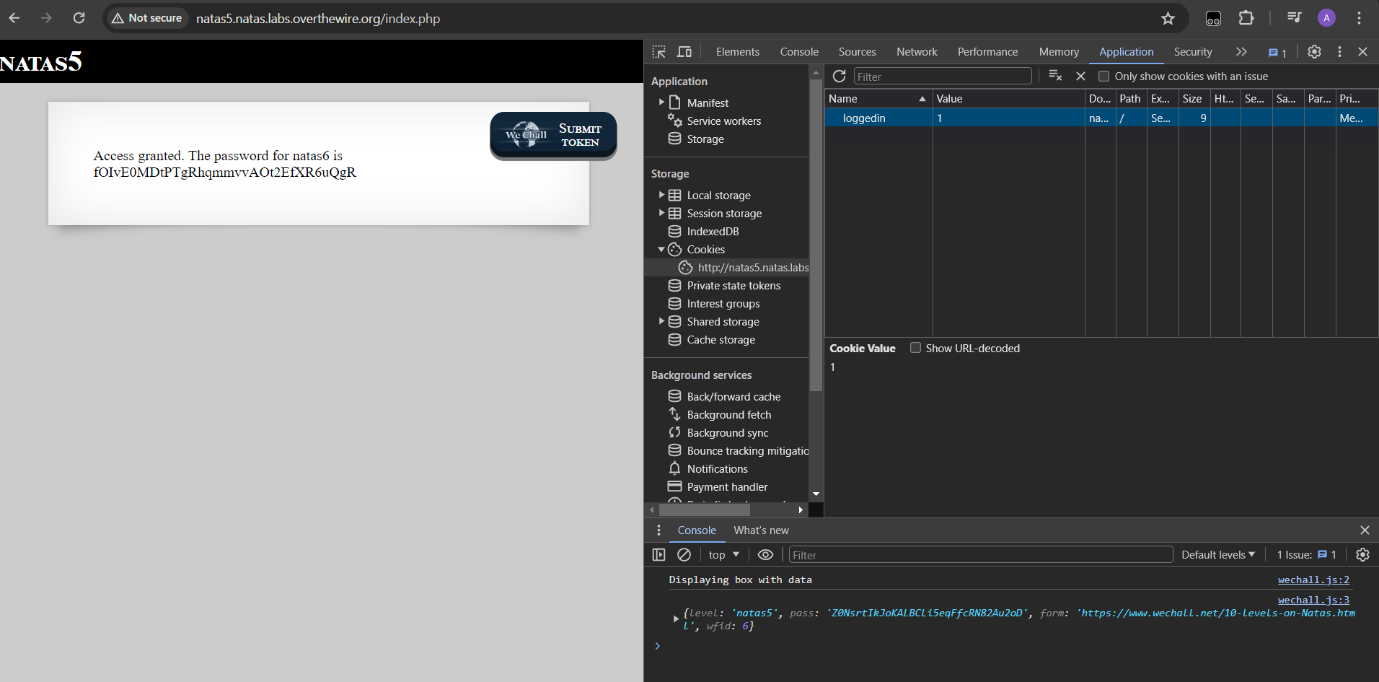
**Natas lvl 5**



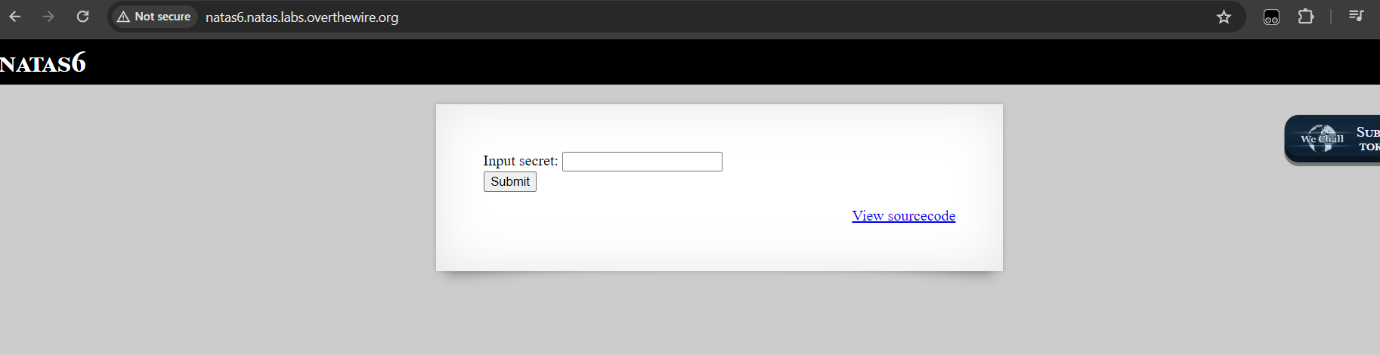
When we inspect the page, we can see that this page has cookies that says “logged in”…so we look into the application tab and we can see this



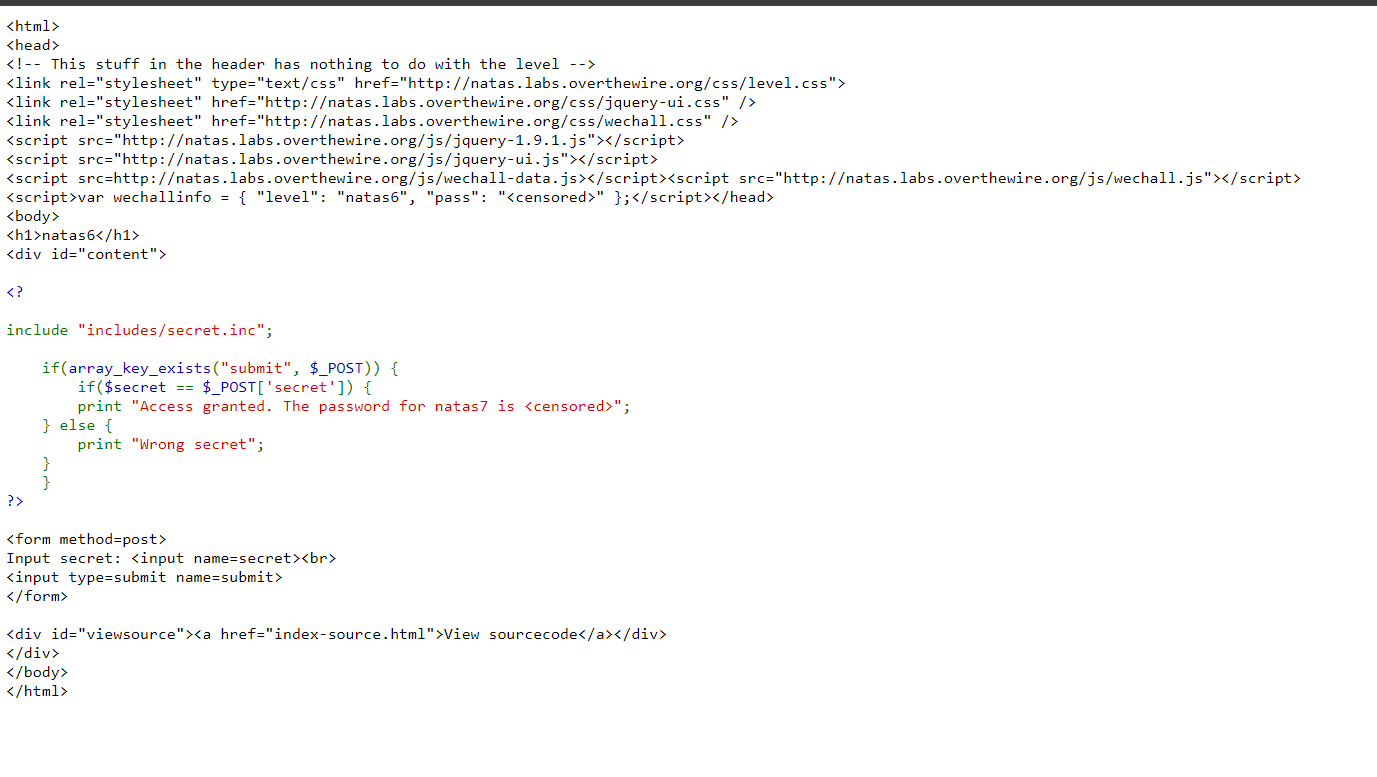
If we change the value from 0 to 1 and hit refresh , we get the password for Natas lvl6



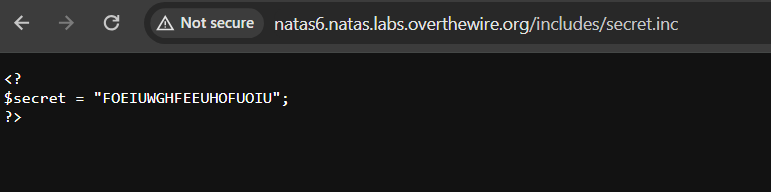
**Natas lvl6**



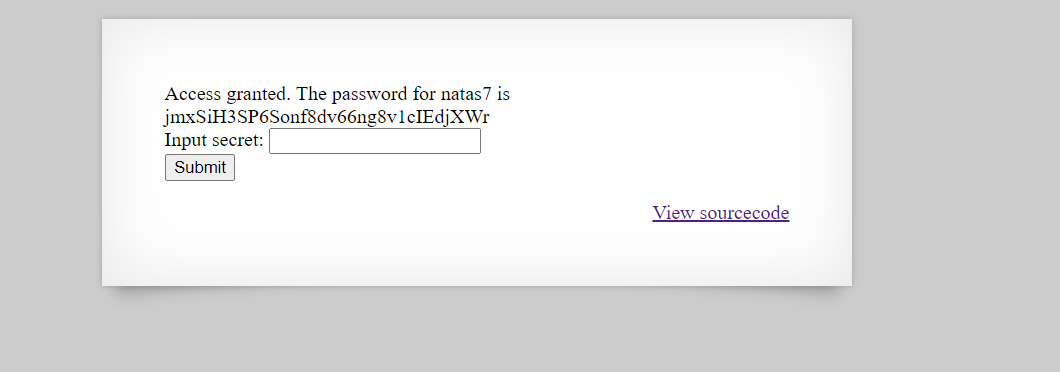
This is the source code that we get:



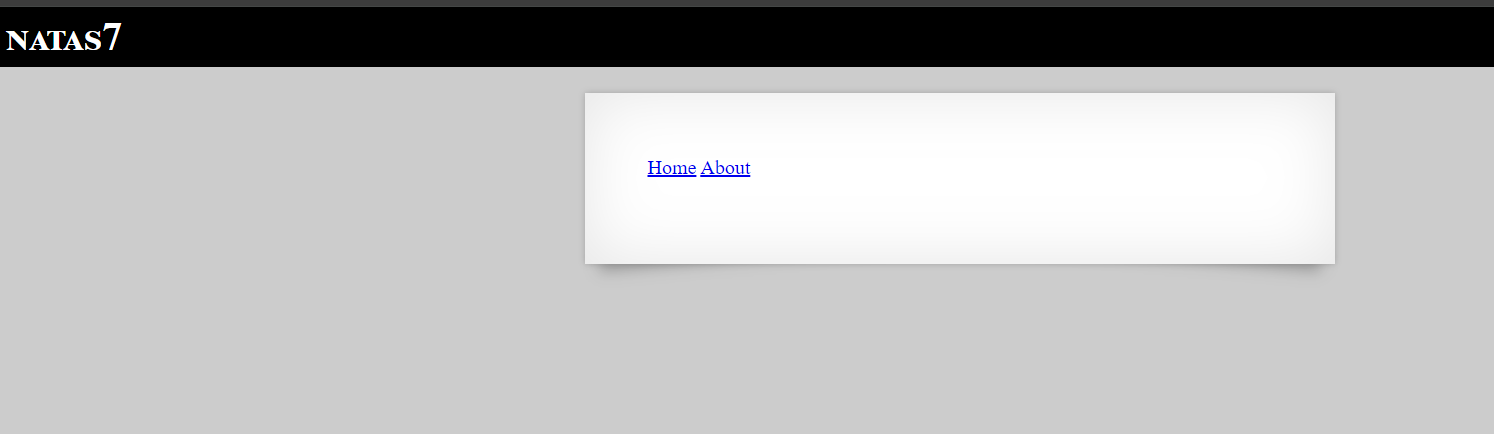
So we if look at here , it says: “includes/secret.inc”; what it means is inside this path , there is something inside it.



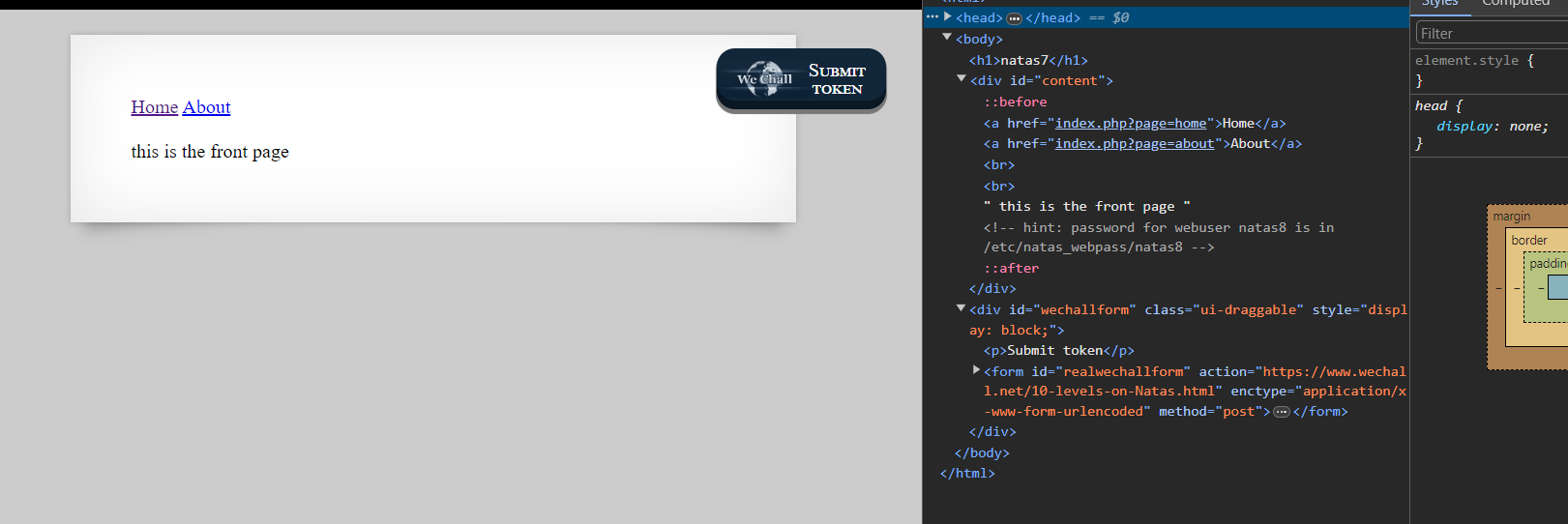
Basically, this is the input secret

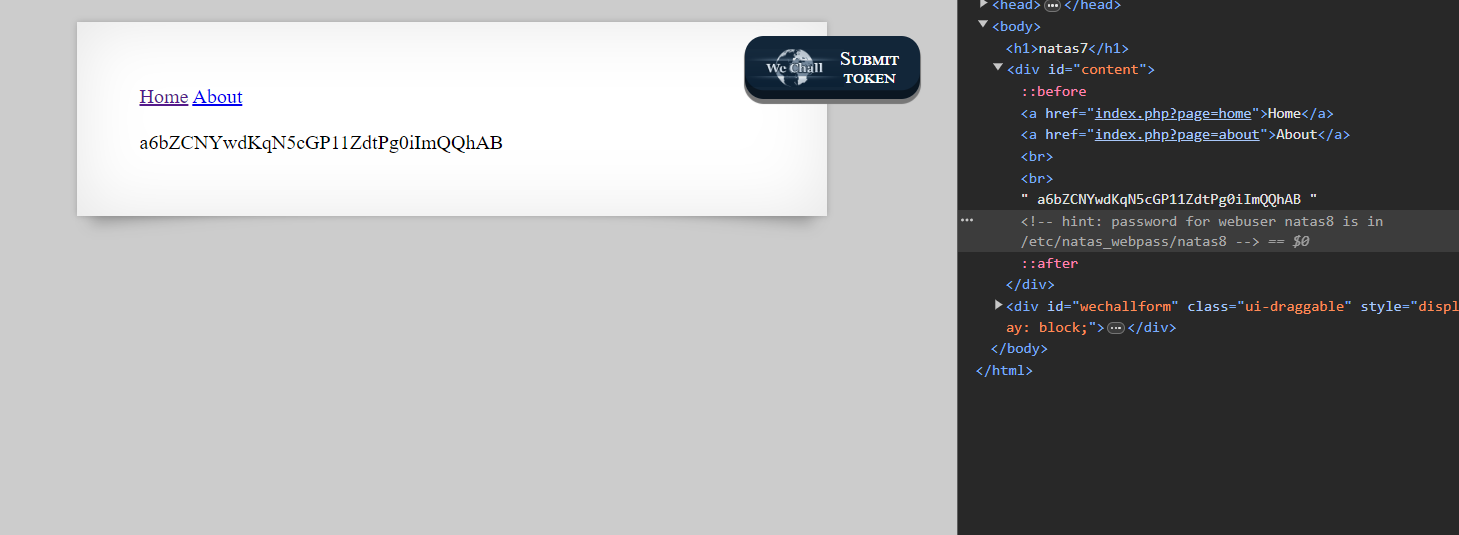


**Natas lvl7**

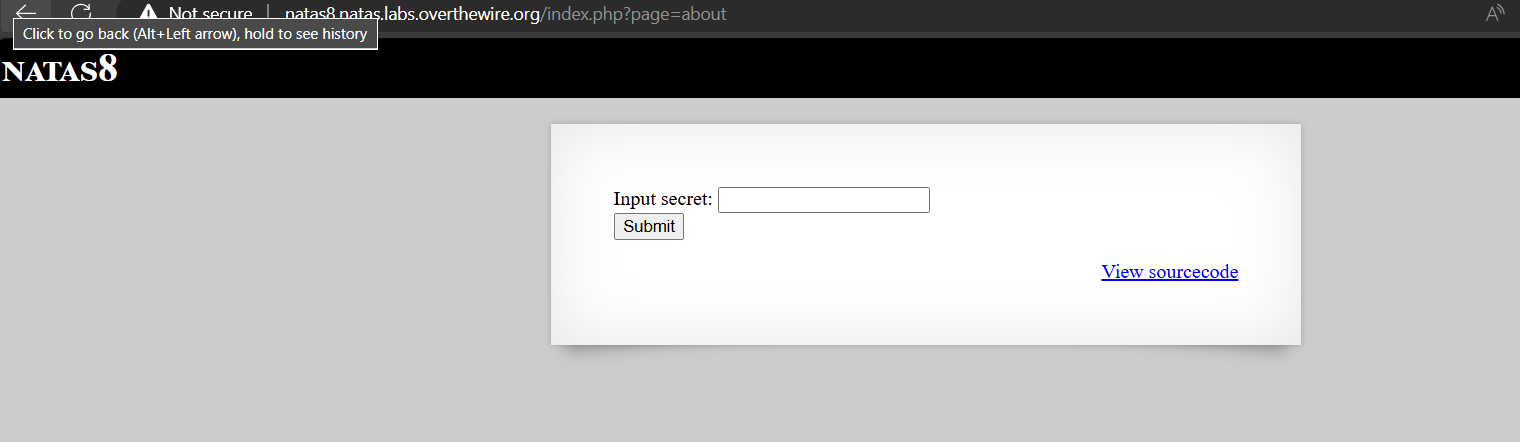


If we inspect the page, we could see a hint in the elements code



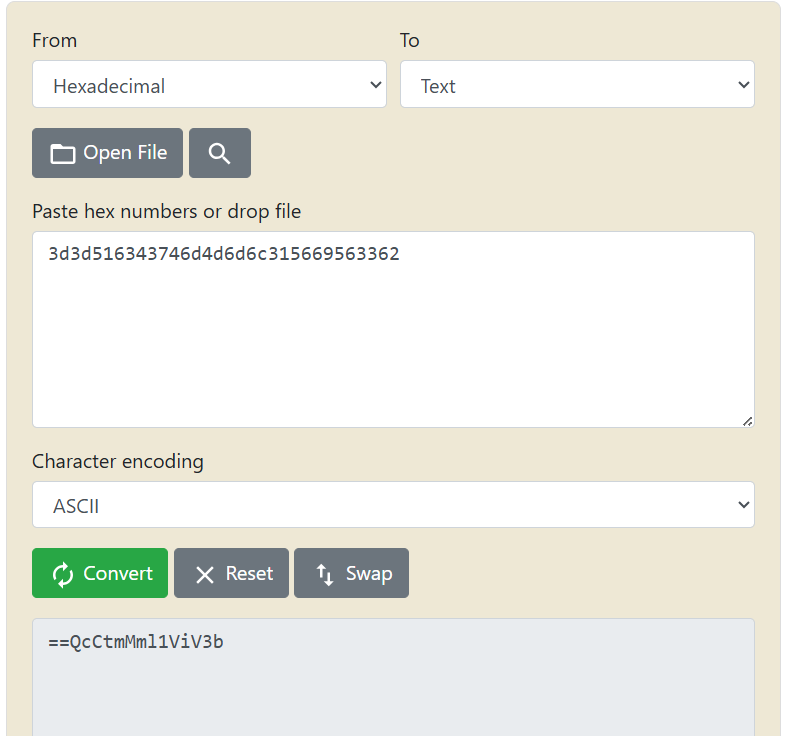
So instead of going to home directory, when we go to /etc/natas\_webpass/natas8 we will get the password

**Natas lvl8**

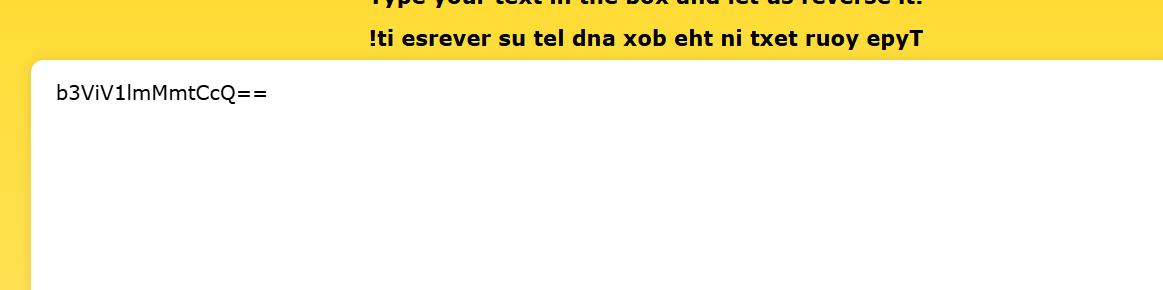
****

****

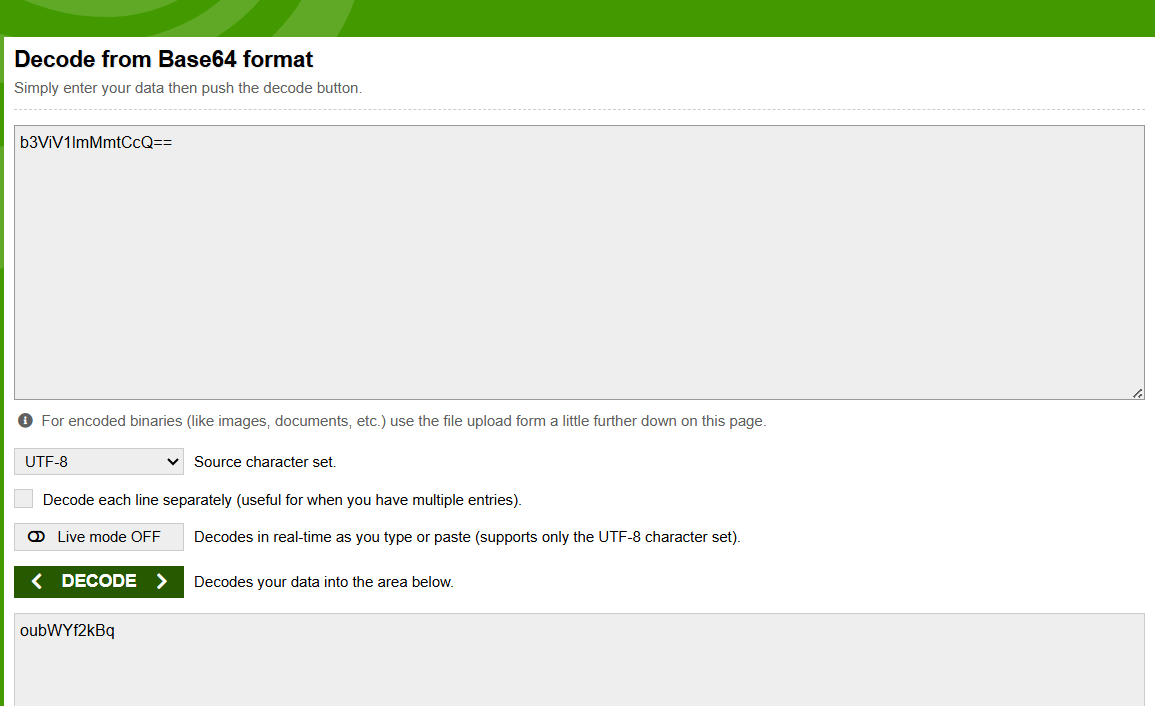
Here we can see an encoded secret and it is undergone a series of function .so if we do the reverse of those functions, we could get something here



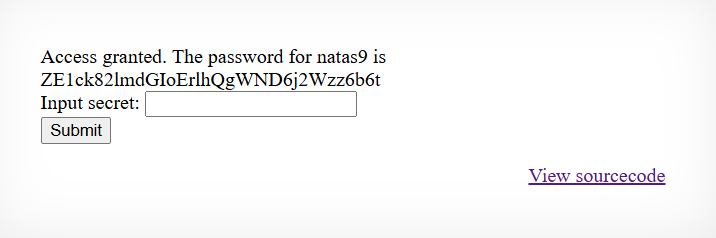
The given secret code seems to be in hexadecimal and that’s why we are converting them to ASCII



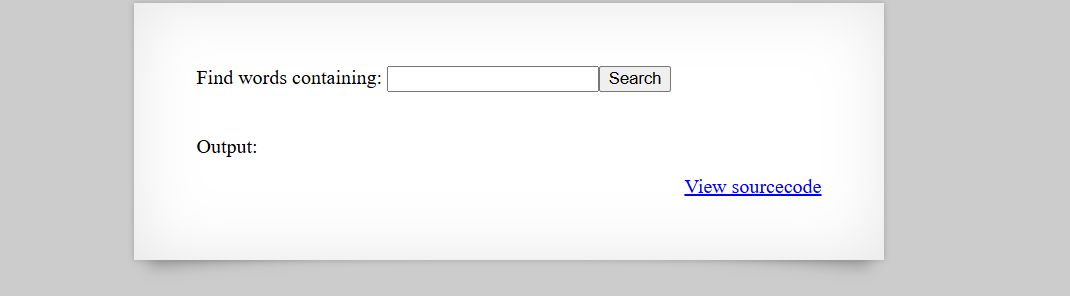
Now if we reverse the code, we get a base64 text. We know that it is base64 is because of the “==”



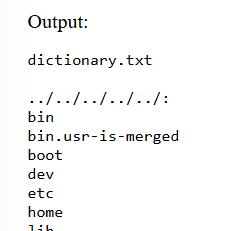
If we decode the code, we get something that looks like a secretcode.



**Natas lvl9**

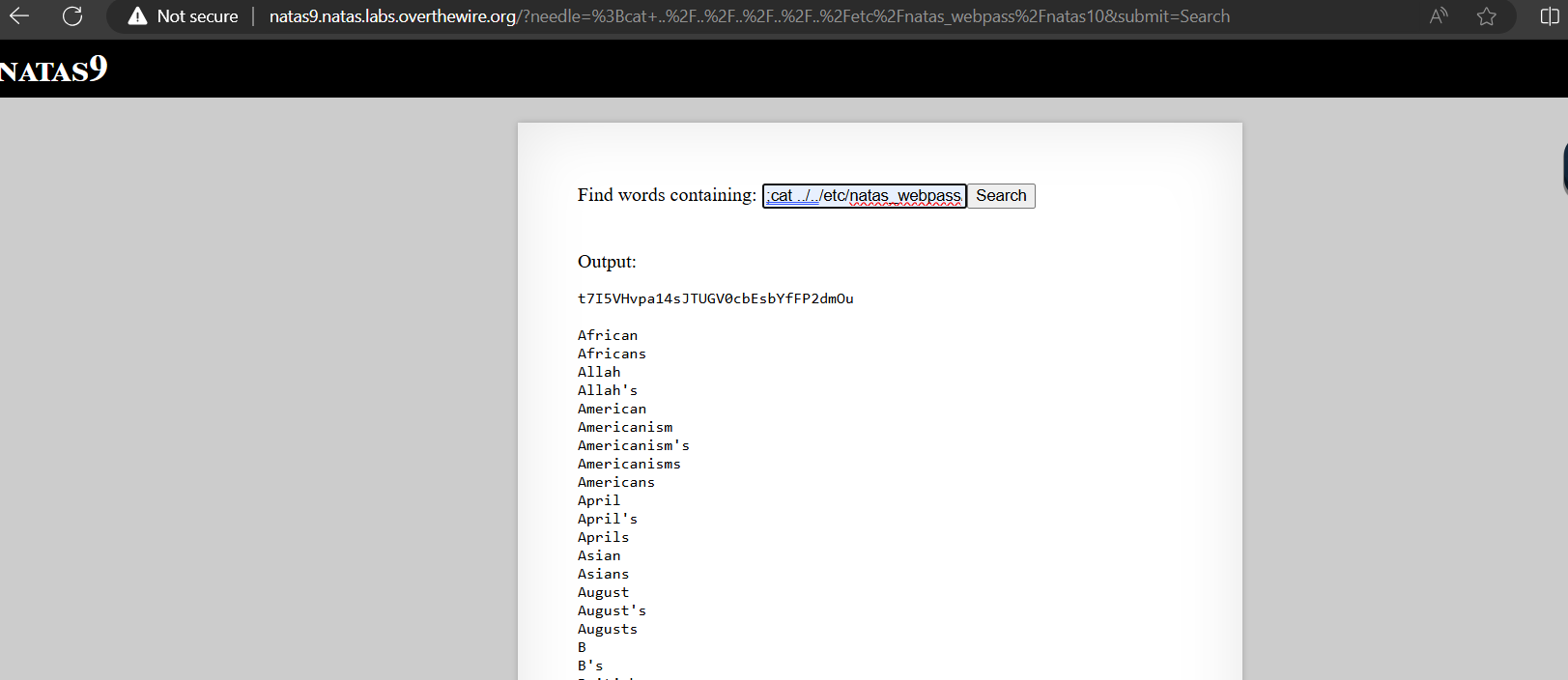
****

if we view the source code, we code see a function called passthru, what it does is it simply execute the command and give output.And to consider a sequential execution, we need to use “;” to before command.

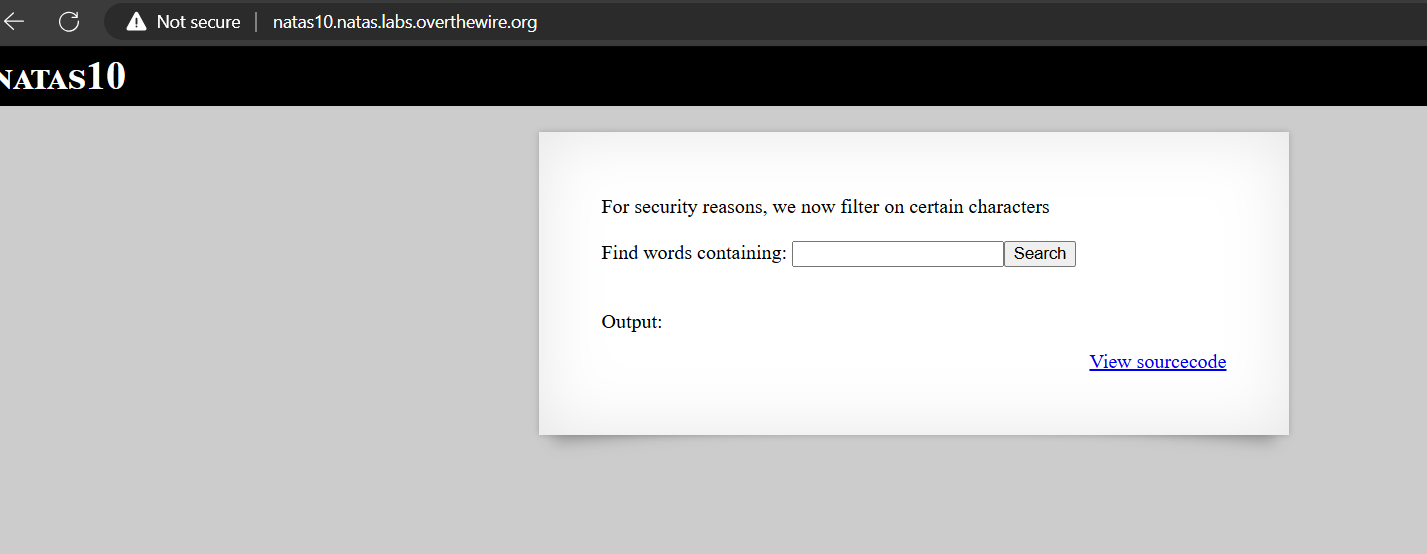


Lets consider that we are in a tree system and we need to go to the top directory, so we use ../ to reach top

And when we use cat command we could see what’s inside it



**Natas lvl10**





Here we can’t use ; or & but since grep can be used to find search different locations at a time , we simply bruteforce with different letters to find the passkey.

So it will be inform “keyletter /etc/natas\_webpass/natas11 and if the password contains the input letter we provided, it will print it out.

