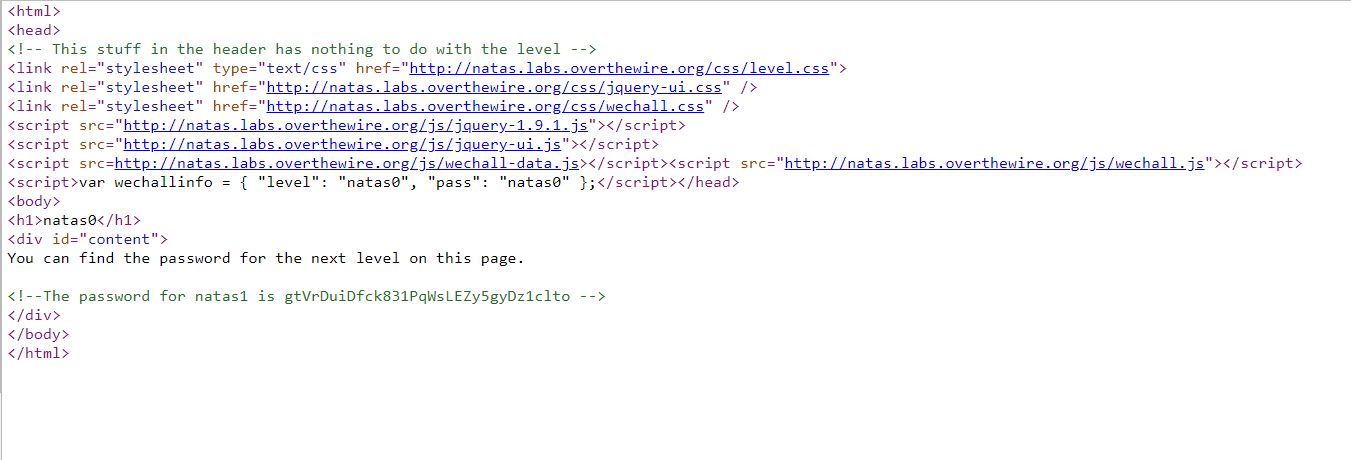
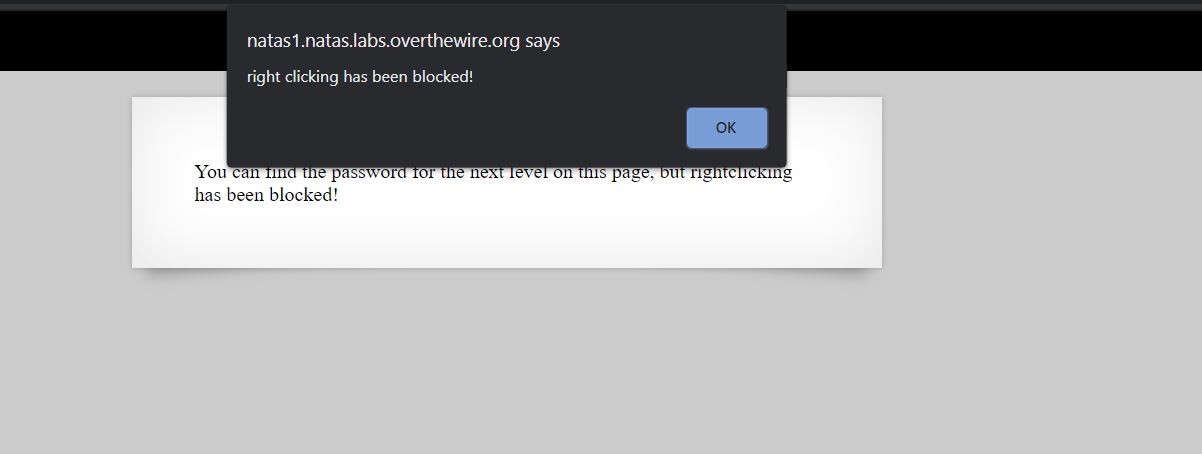
**Natas:**

For level 1 I just had to view the source code for the website and I got the password for the next level in the source code which was commented in the code below!!!

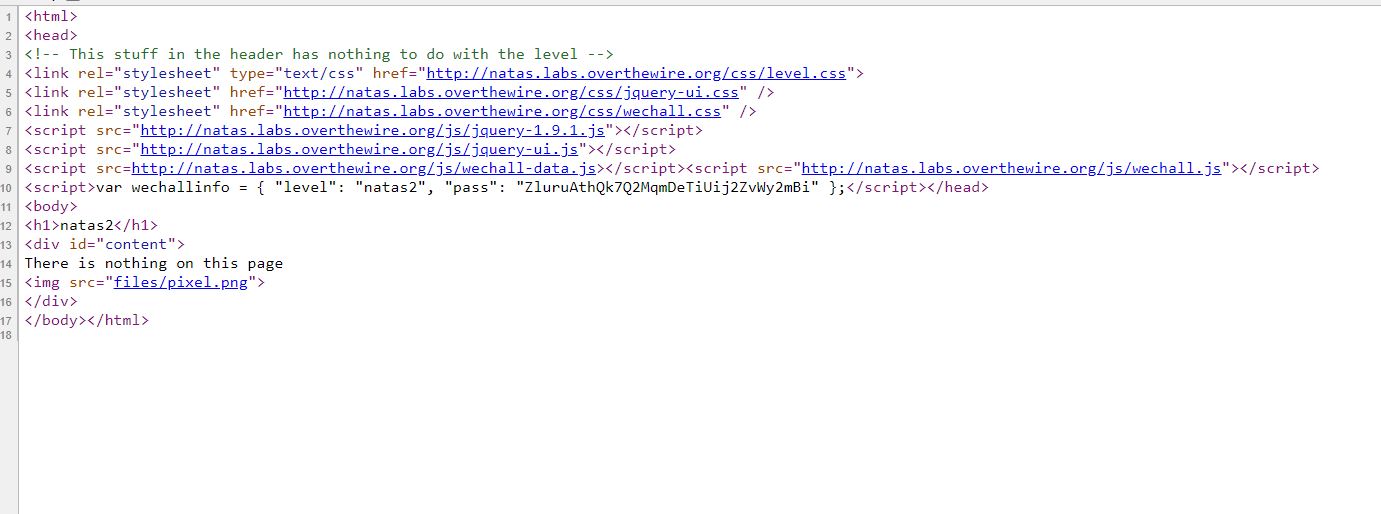


For level 2, the right-click was blocked on the page so for this level, I just used the shortcut for opening the source code which is "Ctrl + U" and BOOM I got the password for the next level as a comment in the code.





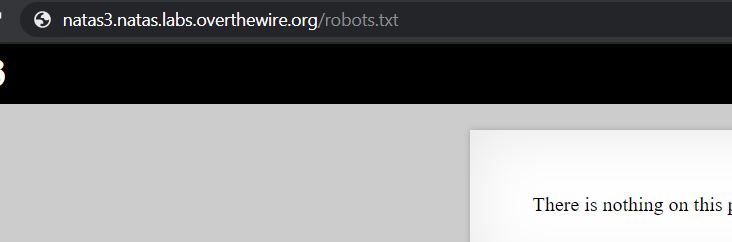
For level 2 it's said there is nothing on this page so I looked at the source code and there was a link to an image clicking on the image it took me to page with the URL "http://natas2.natas.labs.overthewire.org/files/pixel.png" so I tried to check what's the files and there was a file called user.txt going to that file I found the password for the next level.

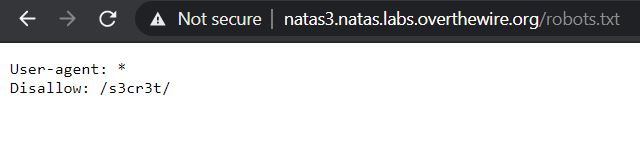


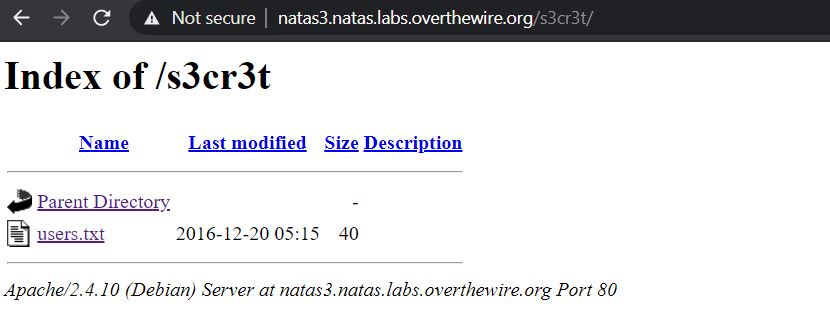




For level 3, I looked at the source code, but this time there was nothing in the source but a comment saying that "This time, not even google can find us", I was sure this is some type of a hint so I tried to look at the robots.txt for the website "Robots.txt" is used for the search crawlers to know which page and file can be accessed from the website, so looking at the robots.txt I found a Disallow directory and I tried to open it and there was file in it called user.txt and after opening that file I got the password for next level.

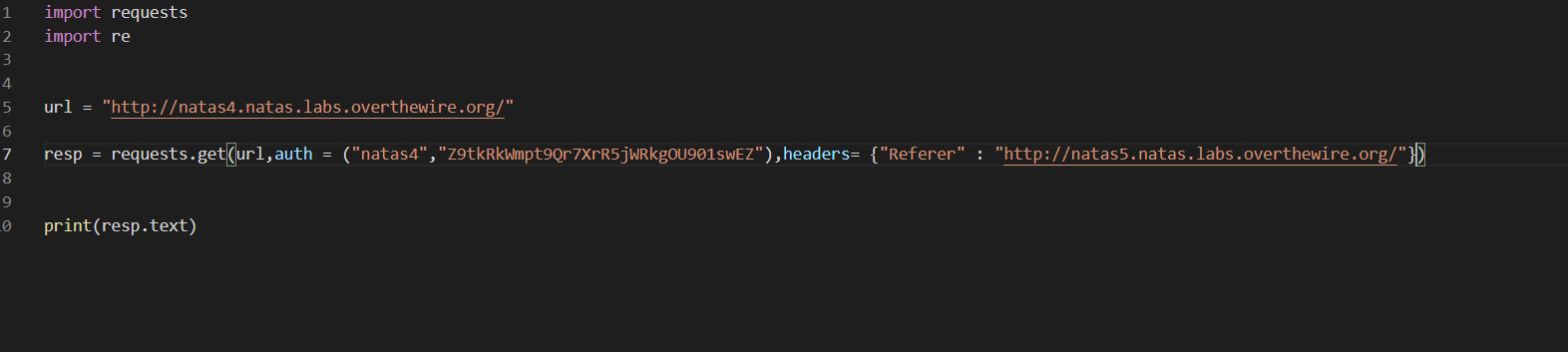


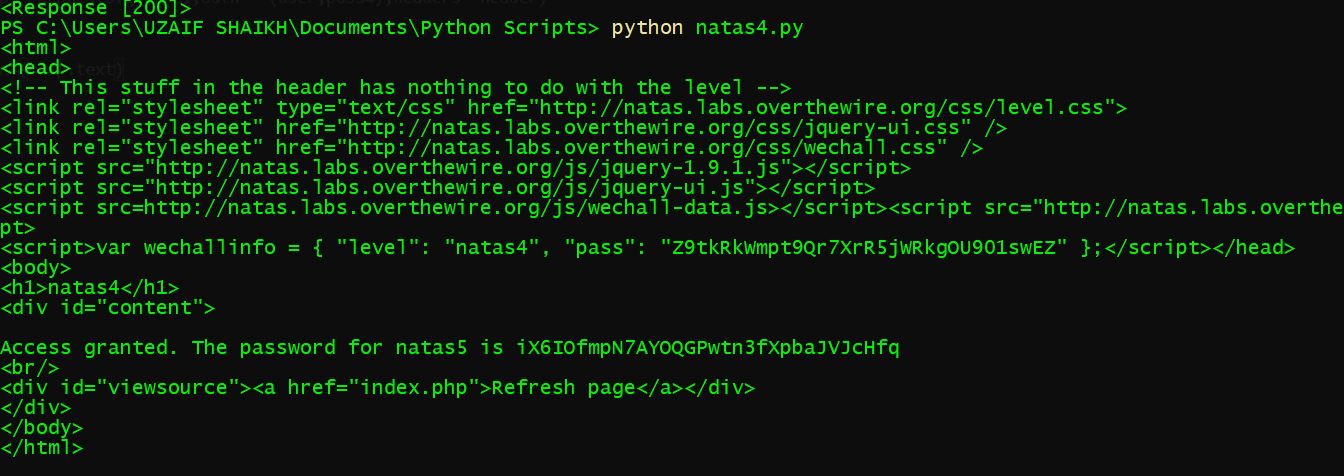






This level was really fun, for this level it said the coming request should come from natas5 in order to get the pass for natas5 so I had sent a get request for this one with the header as natas5 so I get the password for level 5, I wrote a simple python script which sent the get request and I just print the response, here "Referer" allow to identify where the user is coming from that's why I had to set this field as "natas5" and in the response I got the password for the level5. HELL YEAH!!!

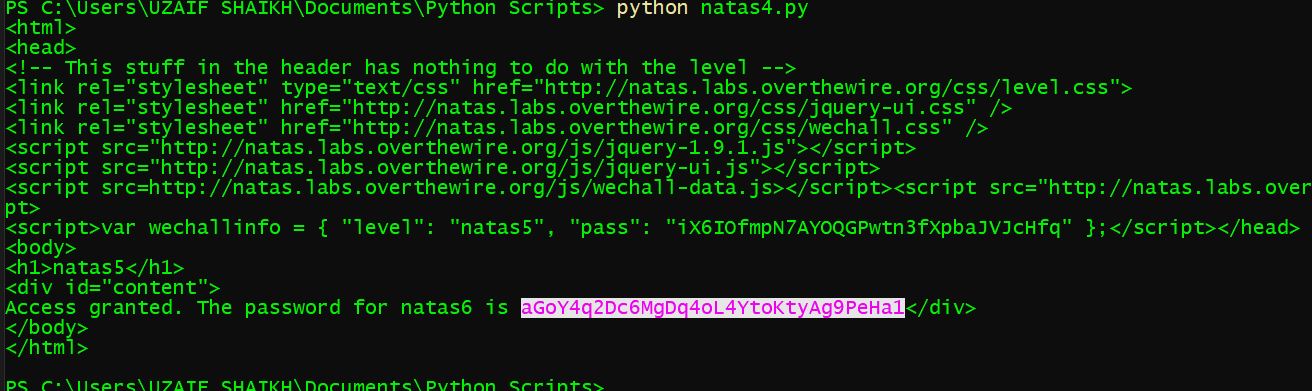




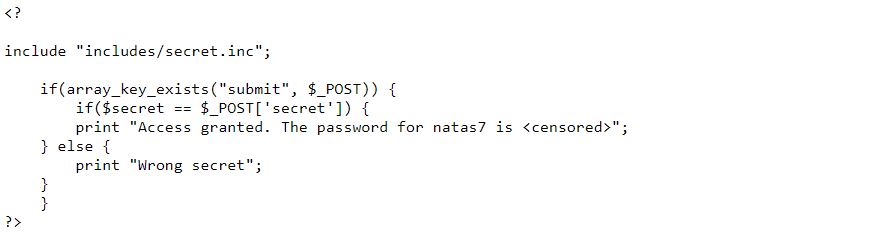
For This level, I was given that "Access disallowed. You are not logged in" so it had to do something with the session cookie so I looked at the cookie using the request.cookies in the same python script and found that the cookie had logged in is set as "0" so I had to change this to a "1" to get the next password. So I used the same python script but using the log in of natas5 and setting the cookies and "loggedin = 1".

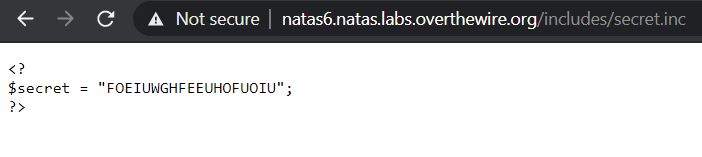


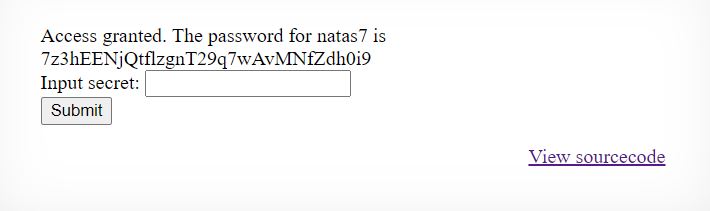




For Level 7, I had to give in an input secret in order to get the password for the next level, so looking at the source code given on the website it had a code that compares the input given to the secret and the code includes a file called "includes/secret.inc" when I opened the file I found the secret key and I got the password for the next level.

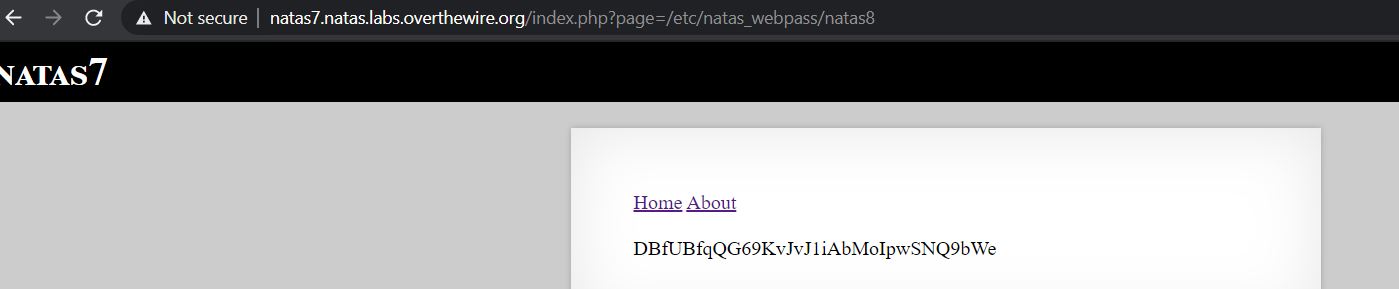




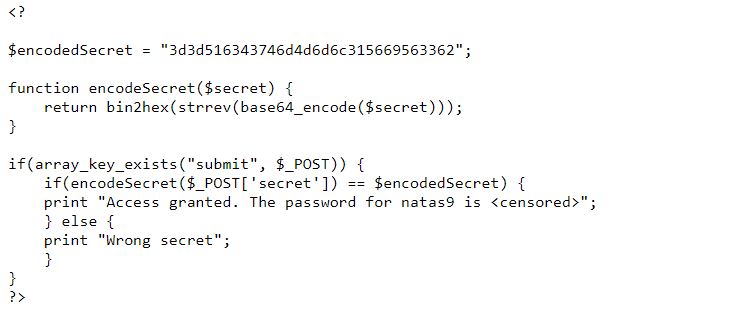


For Level 8, there were two links on the webpage one for home and the other was for about, looking at the source code of the two webpages it's that a hint that password level 8 is in /etc/natas\_webpass/natas8, so looking at the URL which was "natas7.natas.labs.overthewire.org/index.php?page=home" I was sure that address "/etc/natas\_webpass/natas8" was a page so I just replaced home with the address and got the password for the next level.

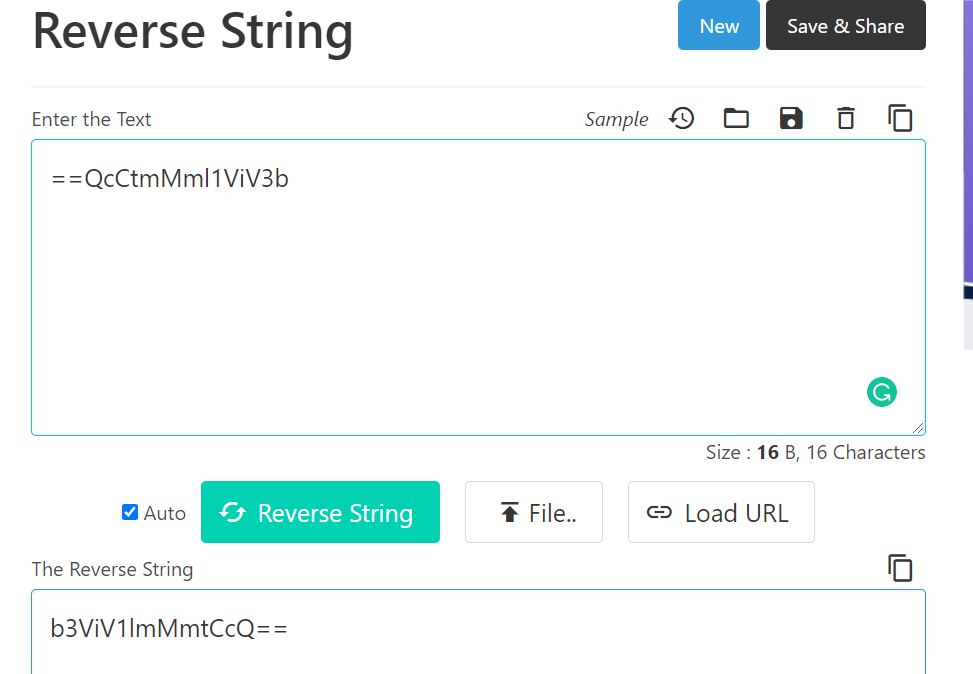


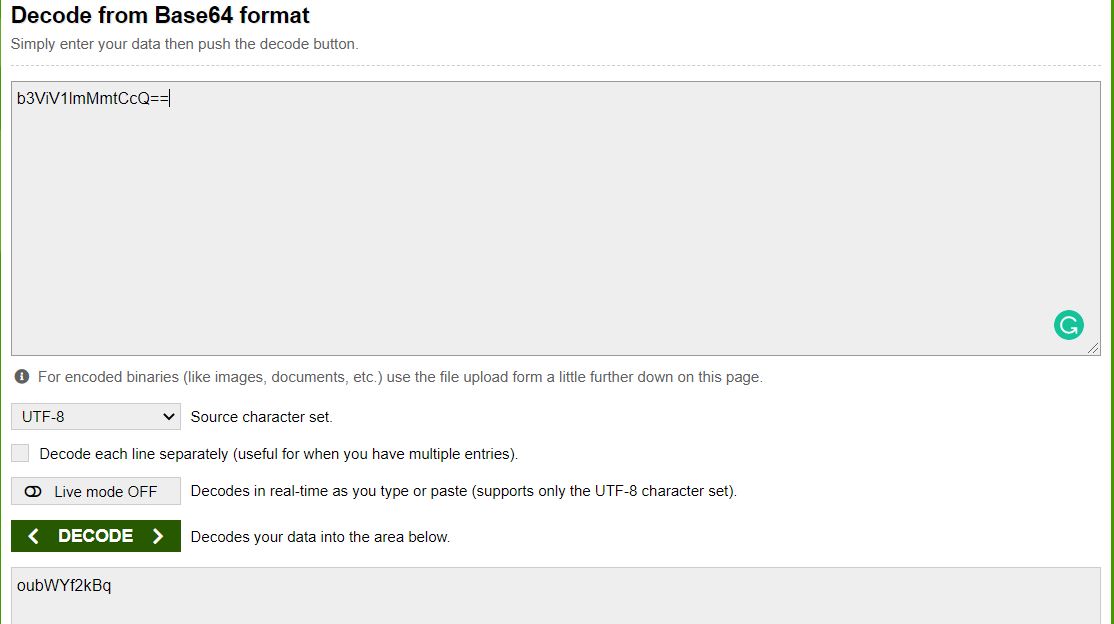


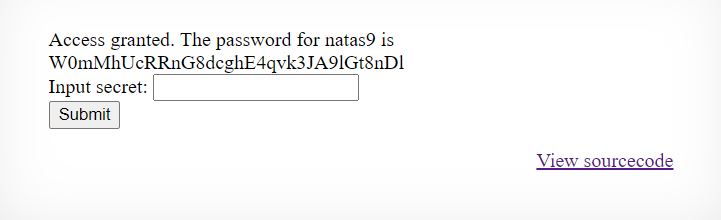
For This level, I had to find the secret again, so I looked at the source code and there I found the code of how they are comparing the secret with a encode secret key, so to decode the secret I followed the step in reverse order to the function was "bin2hex(strrev(base64encode(string)))" so first I converted the hex2bin and then reversed the string and use a base64 decoder to get the original secret!!



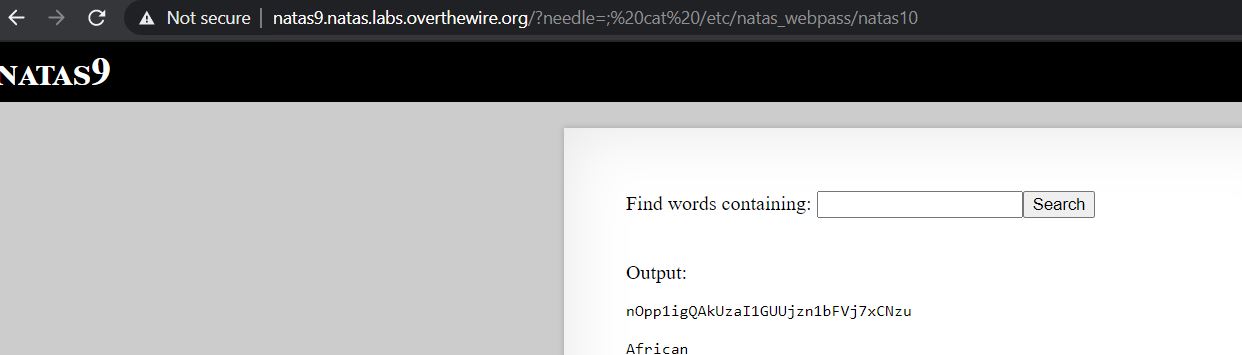








For level 10, I used a command injection as the website gave a search box that linked to a file called dictonary.txt so if the needle field was injected with a semi column following with a Linux command it will slipt out the output and in order to get the password I used the command "cat /etc/natas\_webpass/natas10".



For this level, some of the special characters were blocked from searching, but using the source code and the cheat sheet for command injection I found only three-character were blocked which are "&semi;", "|", and "&" but using the cheat sheet I figure out other ways of using the commands so I used "$ cat /etc/natas\_webpass/natas11" to get the pass for the next level.

