Sri Lanka Institute of Information
BSc Honors in Information Technology
Specializing in Cyber Security

IE2012 - Systems and Network Programming

Walkthrough of Natas

IT22083678
SAHAN H P T

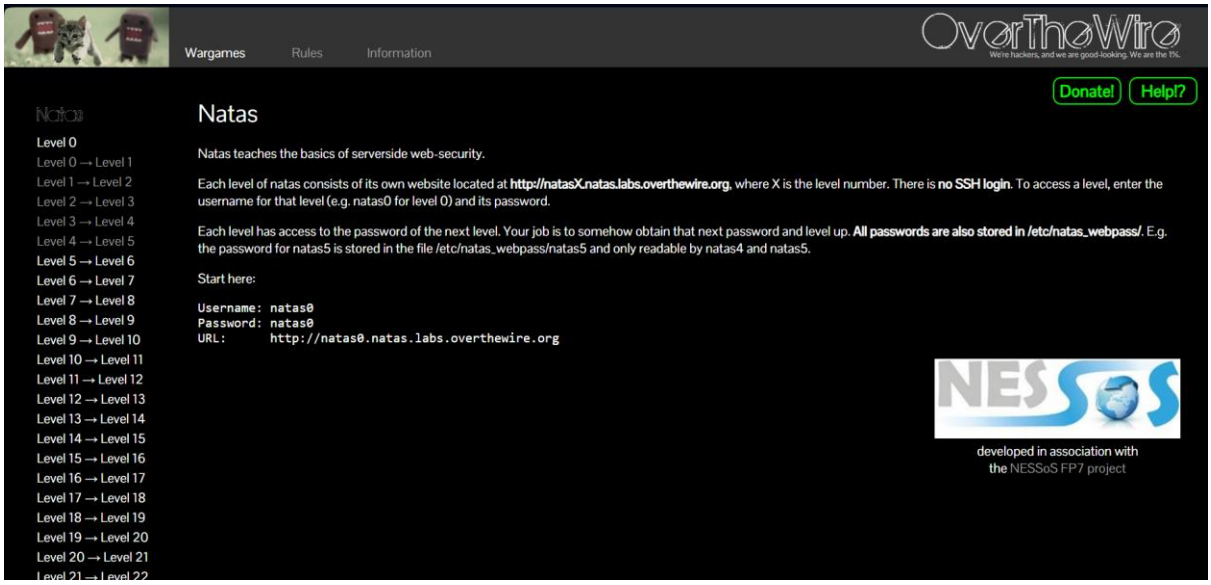
Introduction To The Topic

The “Walkthrough of Natas” topic includes a thorough investigation into the field of security on the internet, made possible by the fascinating puzzles offered y OverTheWire “Natas” series. The security of web-based applications is a top priority in a world driven by internet access. For those looking to strengthen their awareness of the evolving web security environment, this program probes the core of cybersecurity, analyzing vulnerabilities that reflect real-world events. The importance of strong security cannot be emphasized in the modern digital environment, where the internet is deeply woven into every facet of our personal and professional lives.

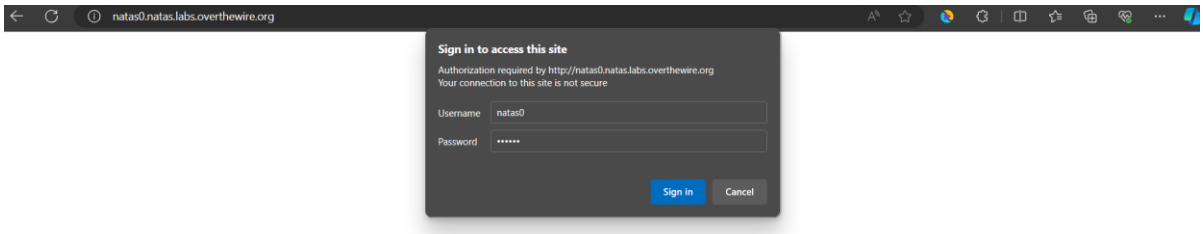
The “Walkthrough of Natas” acts as a learning tool, directing users across the maze of web vulnerabilities while promoting a natural understanding of fundamental security concepts. With this background, the “Natas” tasks become an instructional powerhouse, allowing students to navigate actual vulnerabilities in a safe setting. The "Walkthrough of Natas” is built around precisely prepared walkthroughs that explain how to complete each challenge. These walkthroughs resemble novels that are gradually revealed, with each stage revealing a different aspect of web security. This project’s primary goal is to go beyond theoretical concepts by giving users hands-on experiences that are representative of real-world situations. Advanced vulnerabilities, such as SQL injection, cross-site scripting, authentication bypass, and more are explained in the walkthroughs. Participants gain practical understanding of these security vulnerabilities’ mechanisms and potential effects by dissecting these flaws in detail.

Natas0 ->Natas1

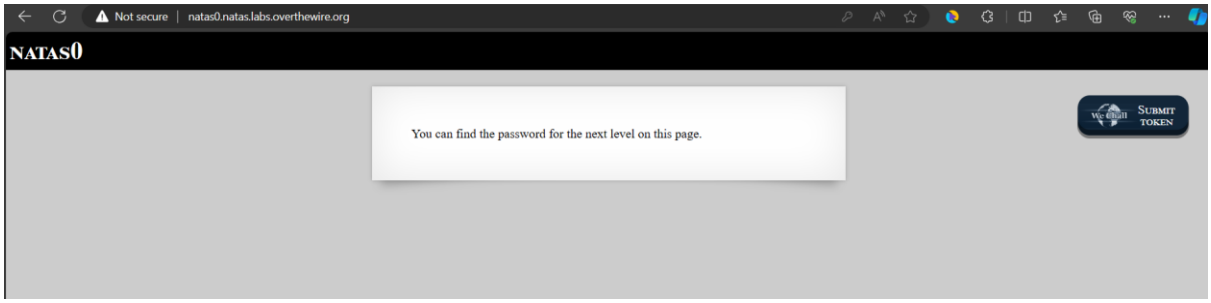
At the initial level of Natas, they give us proper instructions on how to proceed with this. And the username and password of the zero level are also given.



Go to the link they provided by them and provide the username and password.

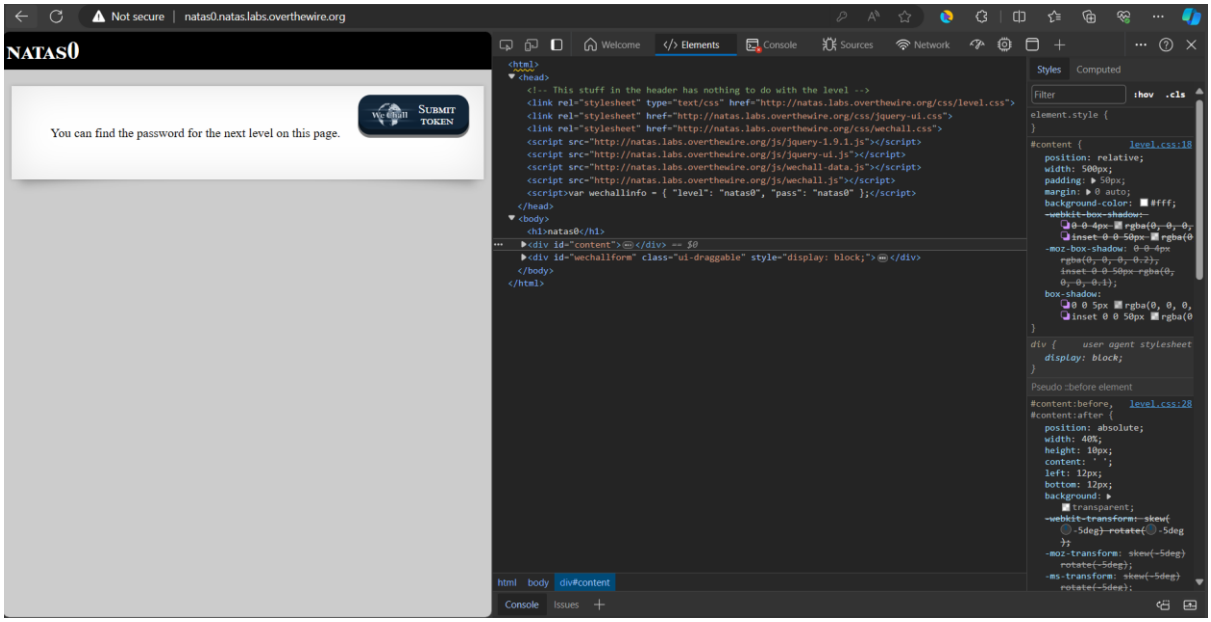


When we give it, we will get a message.

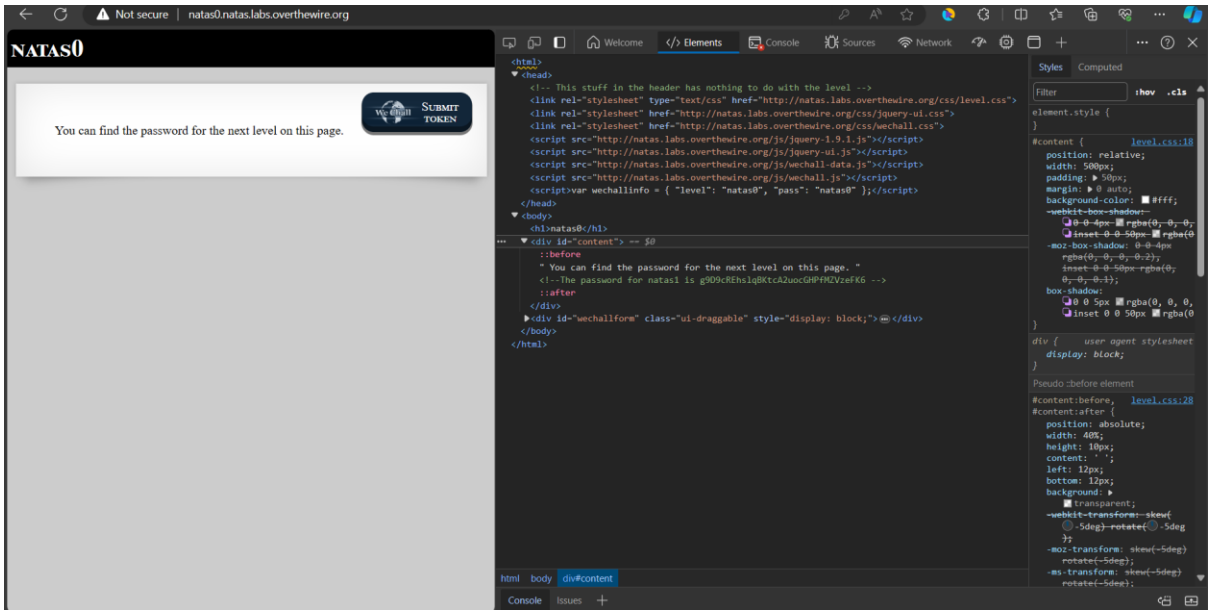


Now we need to find the password related to the next step from this page.

Open the inspect and go to inspector to try to find the password.

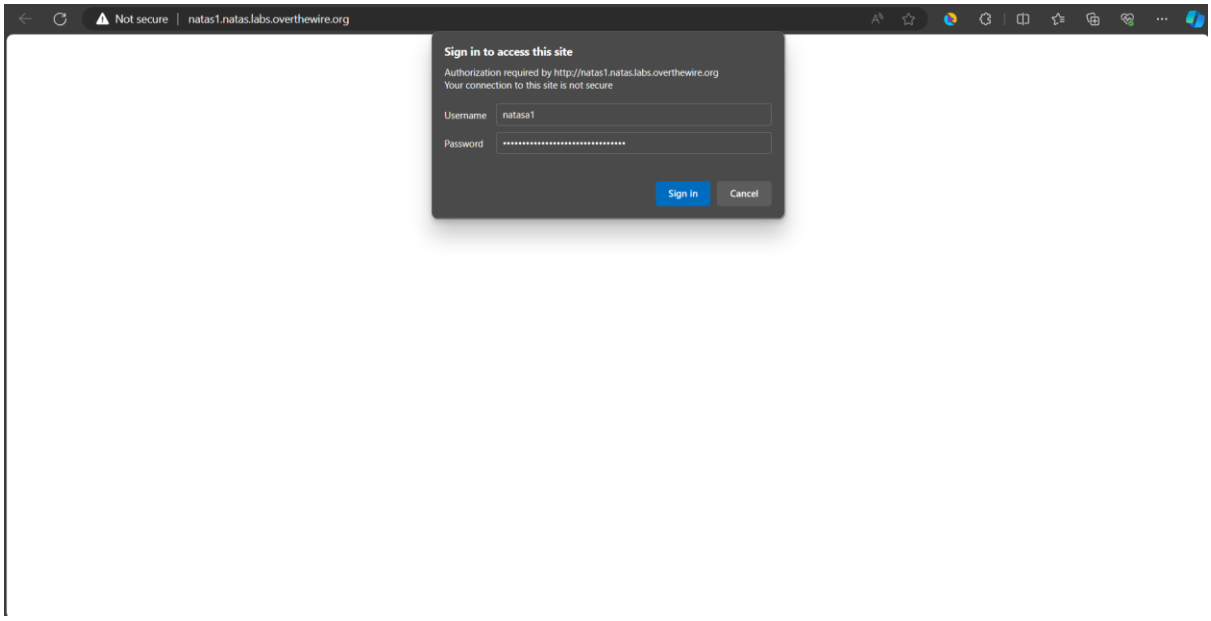


We can see the password of the 1st level into the inspector.

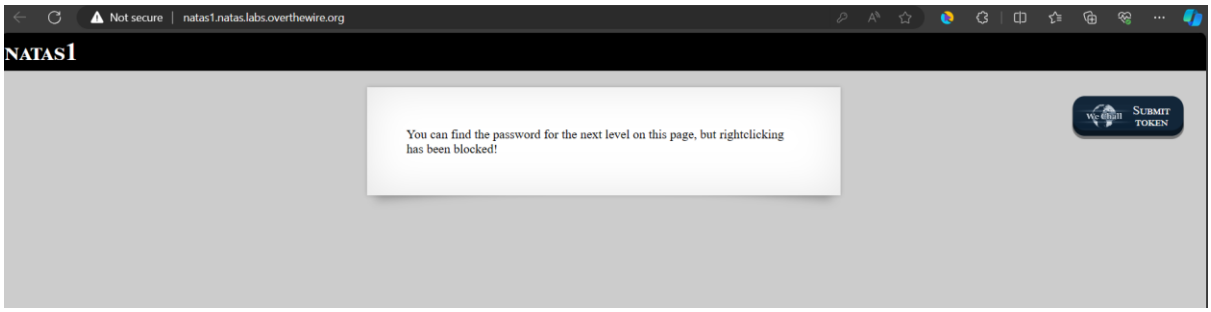


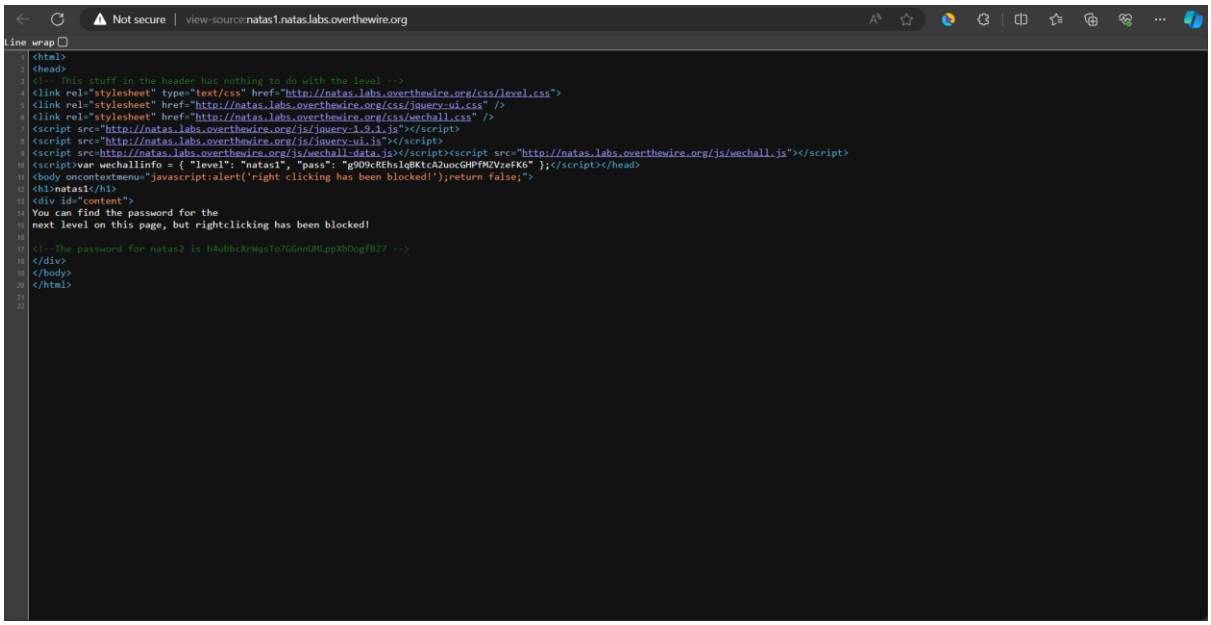
Natas1-> Natas2

Now change the link to one instead of zero and go to Natas1. Give the username natas1 and the password found in the previous level.



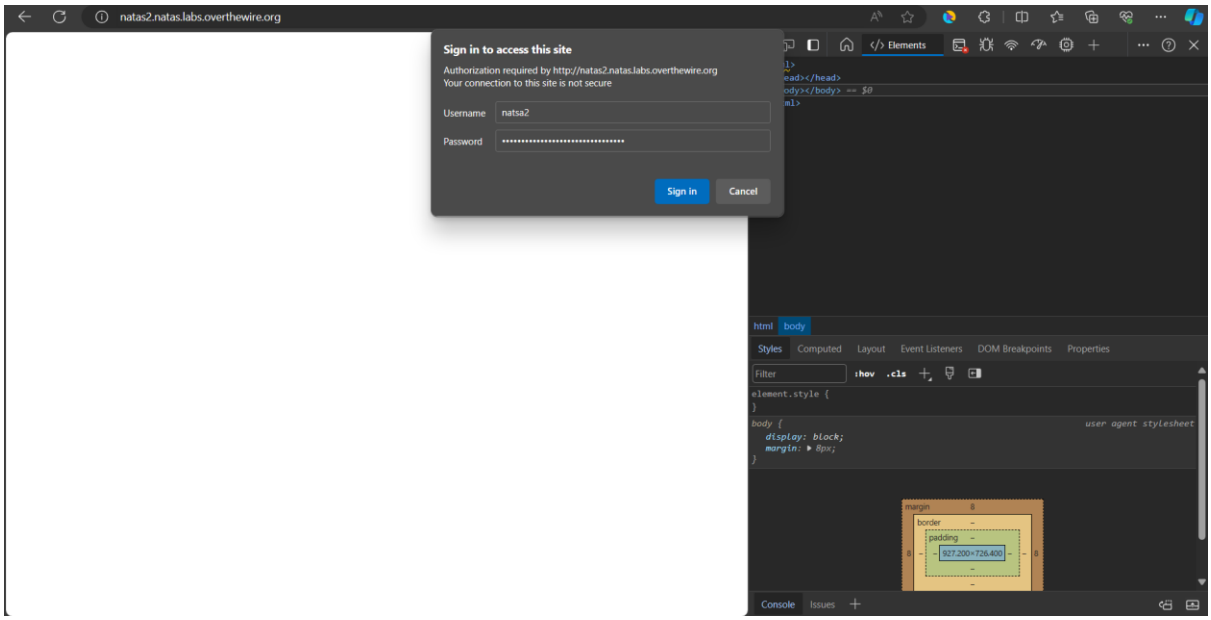
When we give a username and password, we can see a message on the webpage.



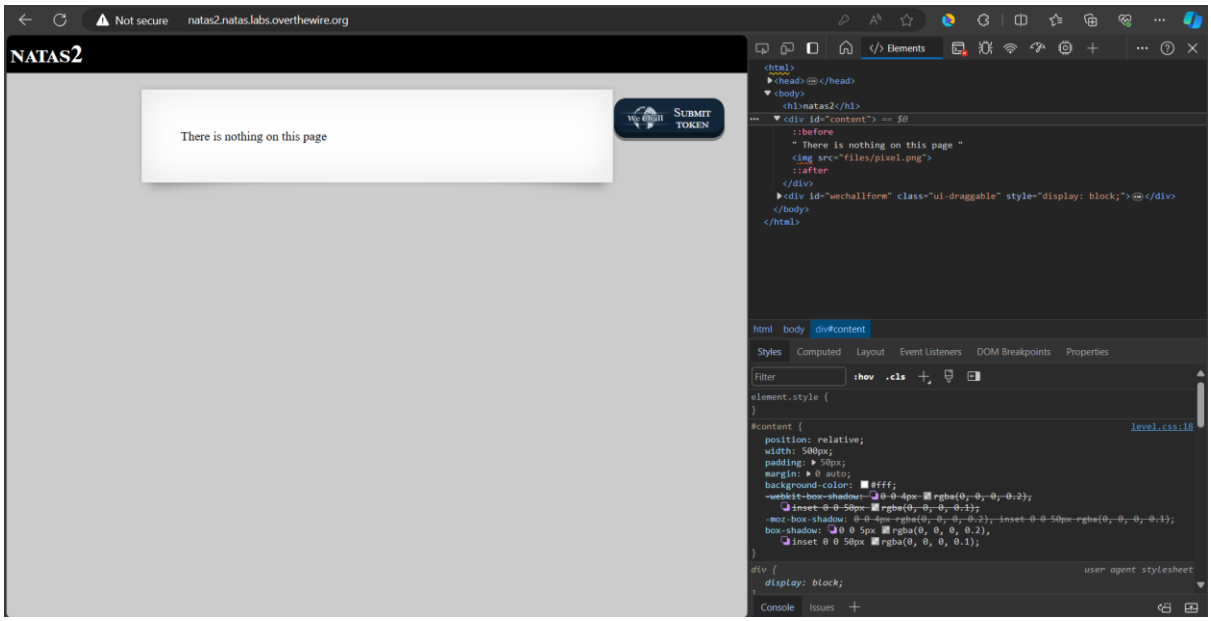


Natas2-> Natas3

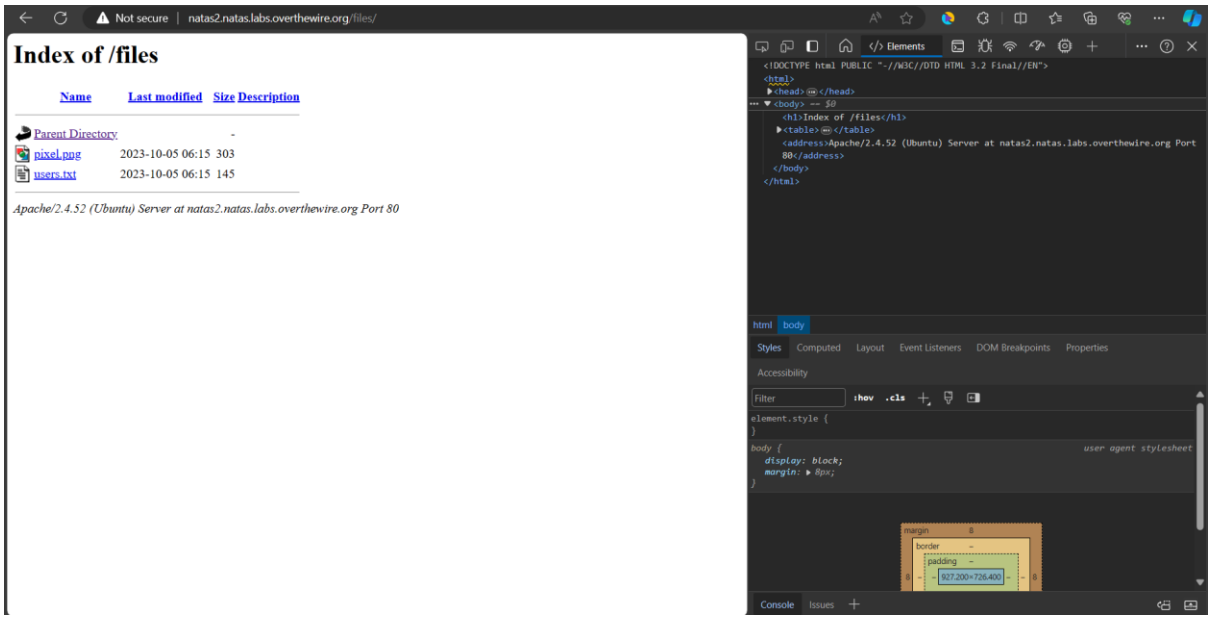
Change the link to two instead of one and go to Natas2. Give the username natas2 and the password found in the previous level.



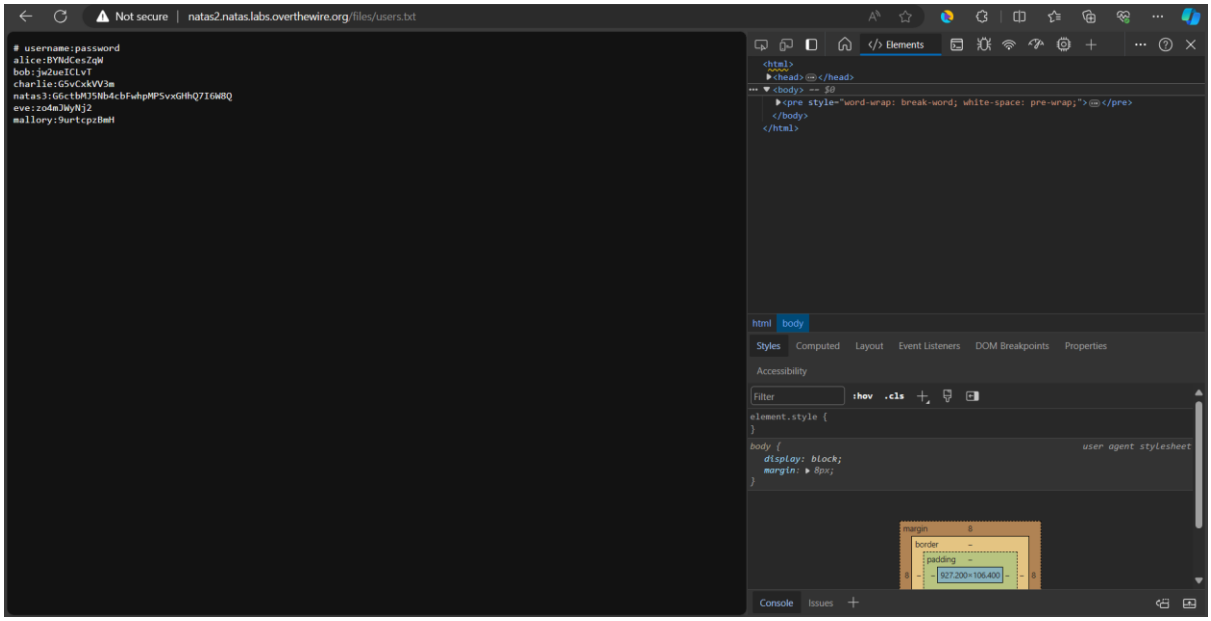
They display “There is nothing on this page”. So next-level password is not on this page.



Try to find the password using the /files page. Now we can see the users.txt file go inside it.

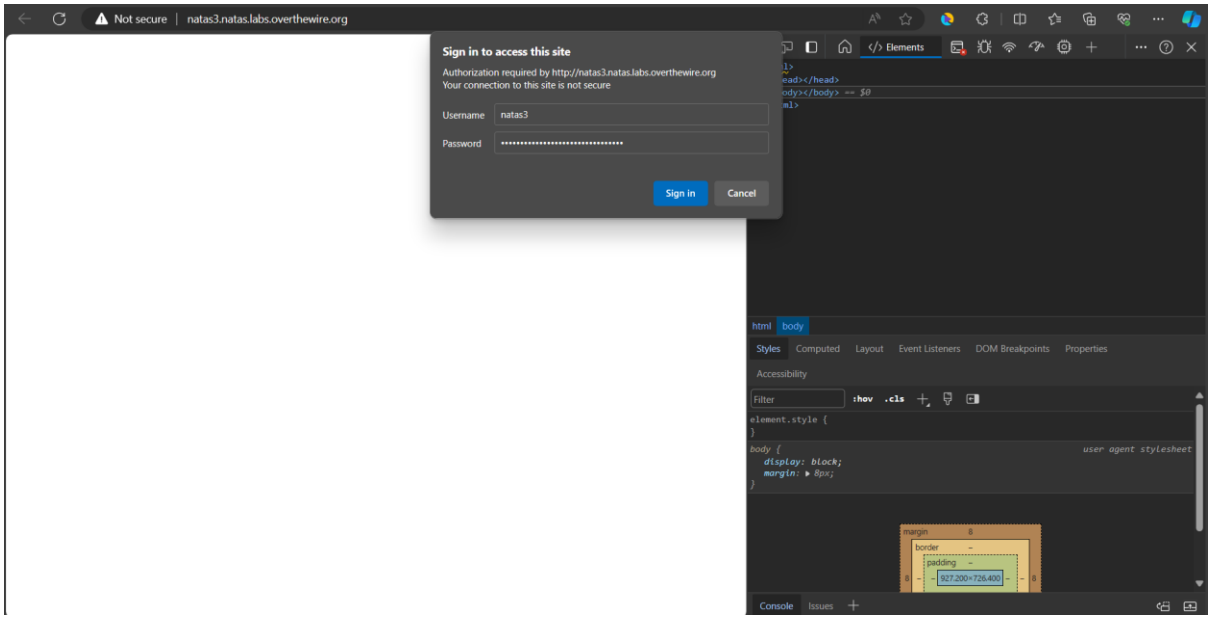


We can see the password now.

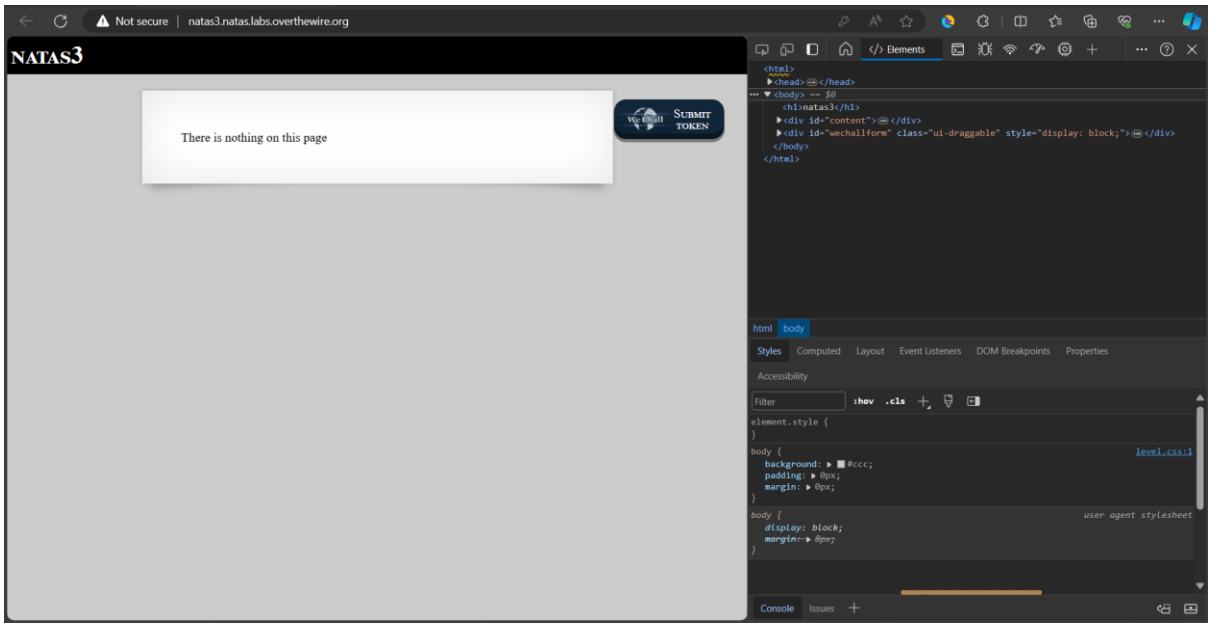


Natas3 -> Natas4

Go to the 3rd level using the found username and the password.

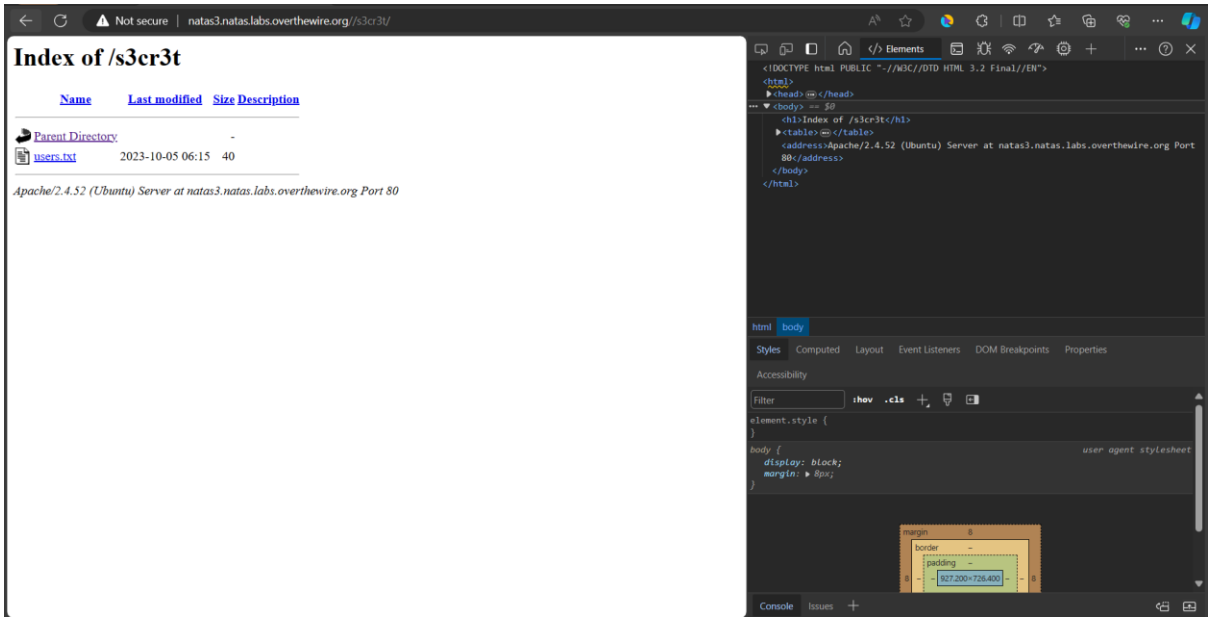


Go to the inspector first. We can see a hint.

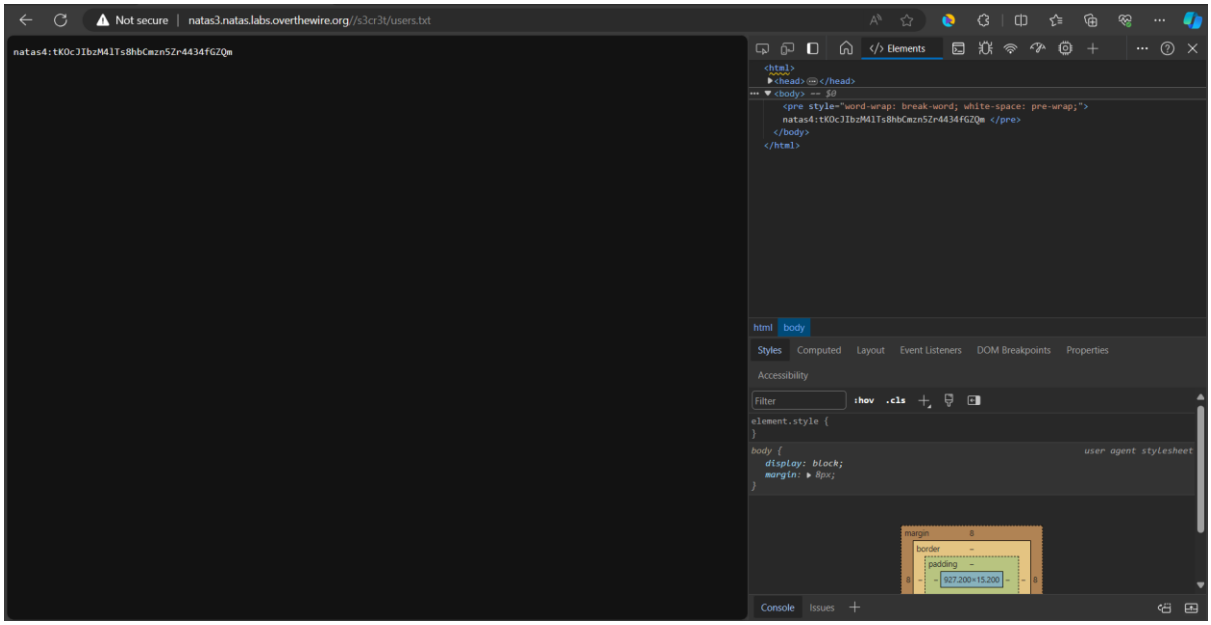


Go to the robots.txt website and find some hints. It mentioned a part of a link.

When we go to that link we can see the users.txt file.

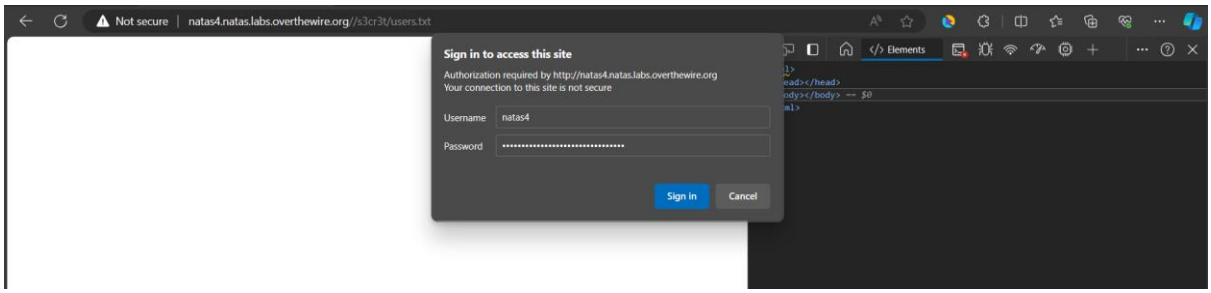


Go inside the users.txt file and find the password of natas4.

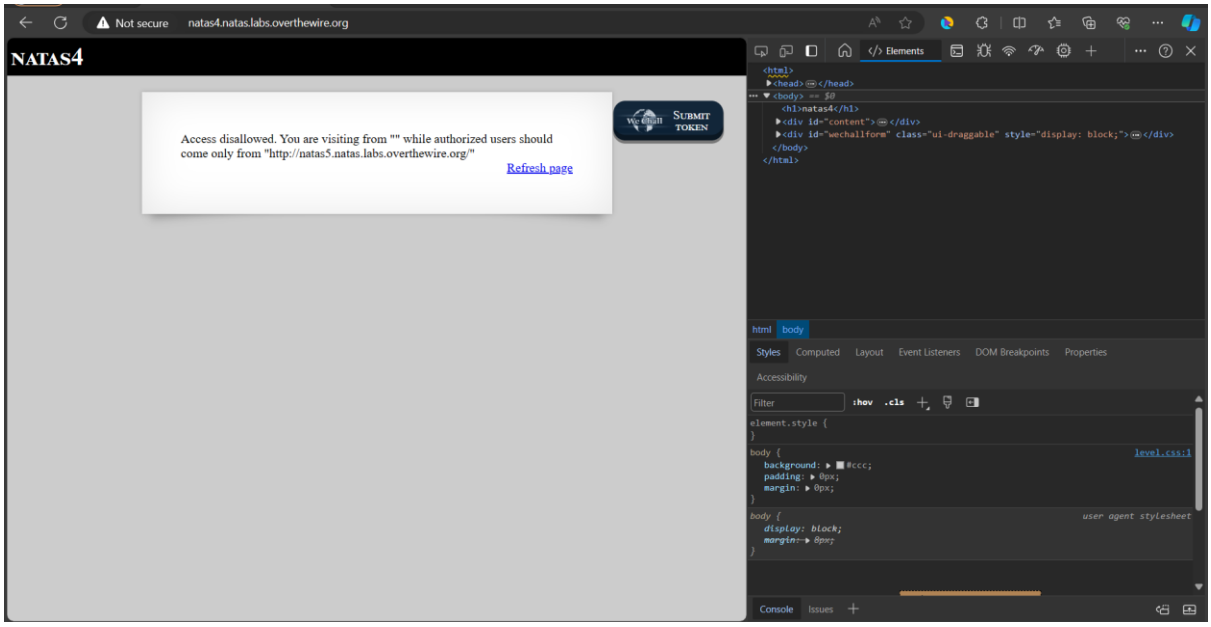


Natas4 -> Natas5

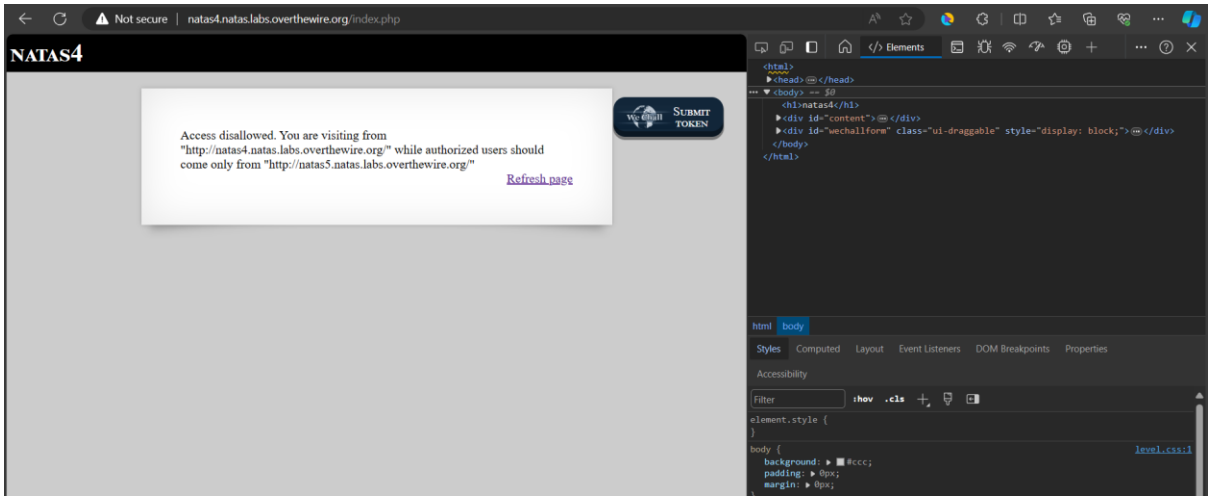
Log into the Natas4 using the password and the username.



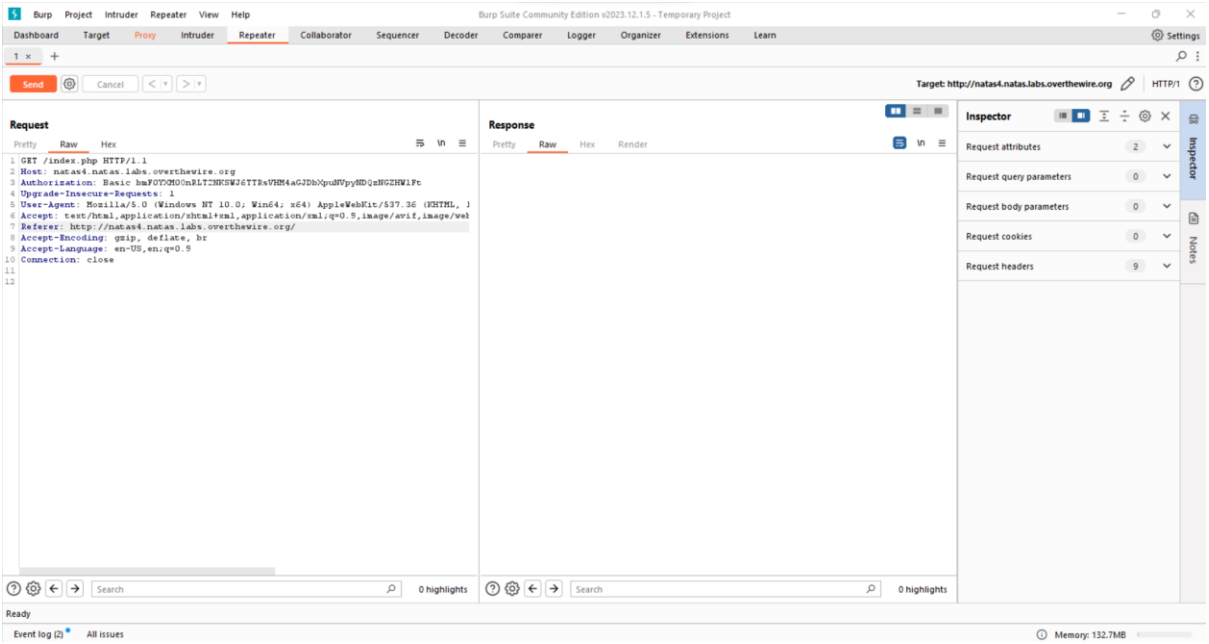
Now it displays a message to refresh the page.



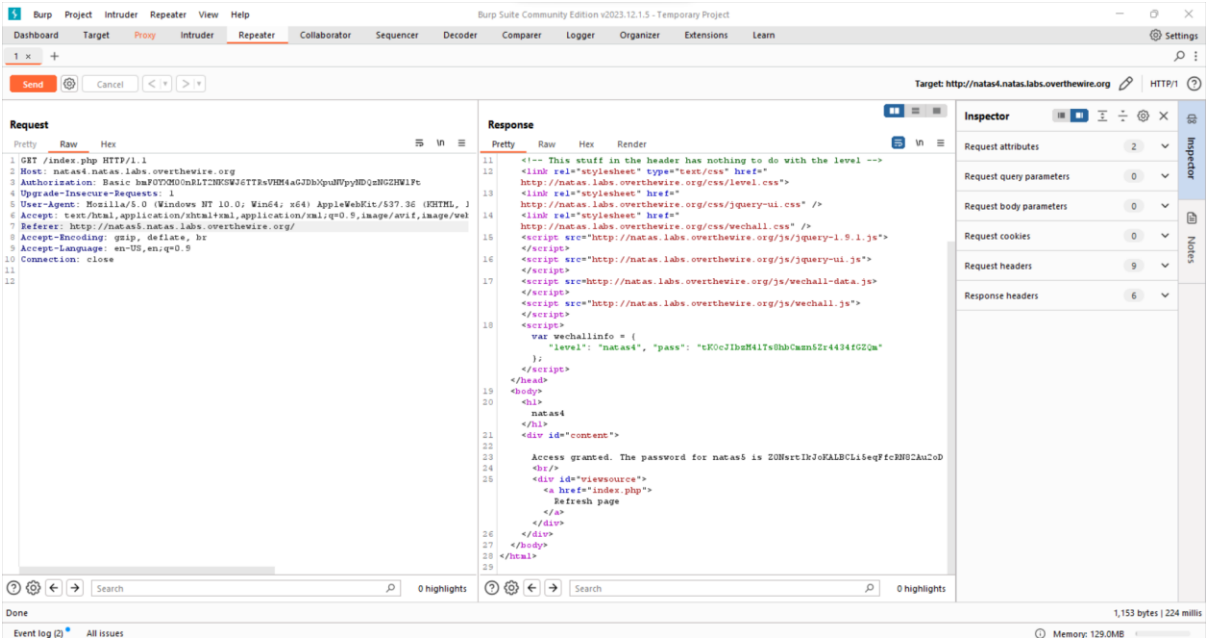
When we refresh the page, again displays the message “Access disallowed”.



Open the burp suite software and open the browser with it. Go to the proxy on burp suite.

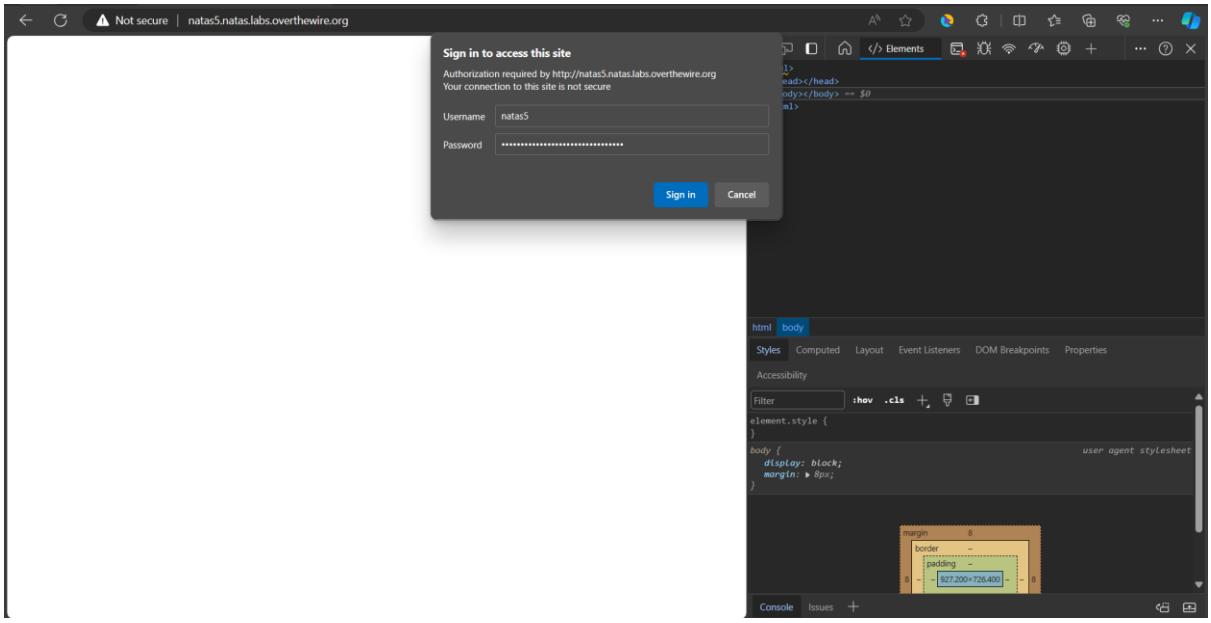


Send a request to the repeater. Change the referrer from natas4 to natas5 and send the request. Now we can see the password and access granted message on the response.

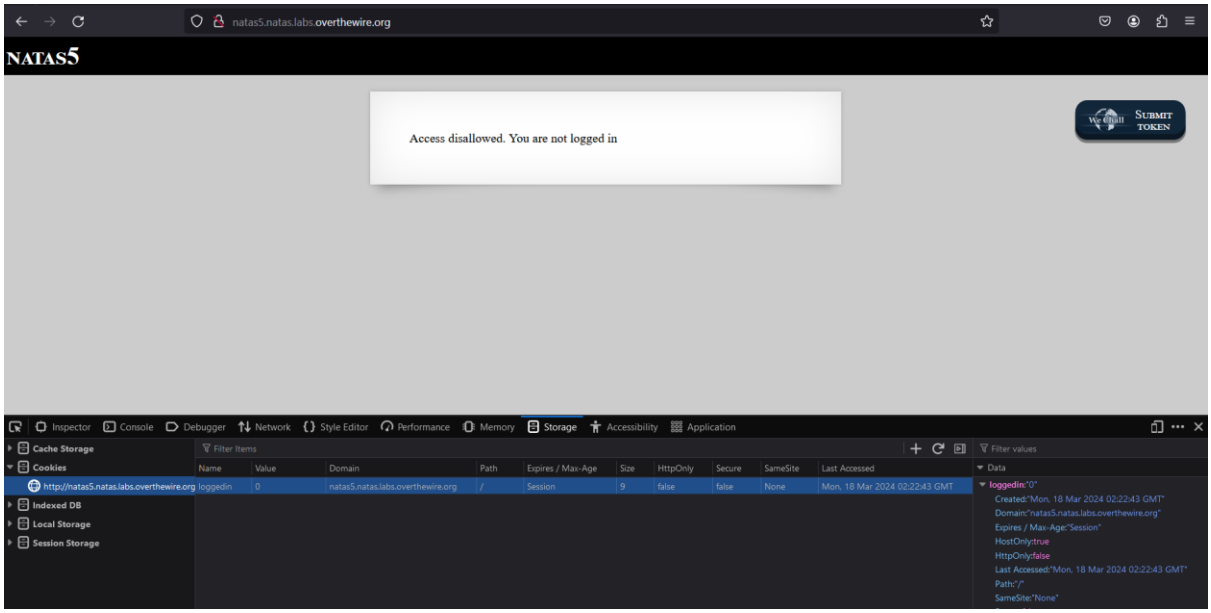


Natas5 -> Natas6

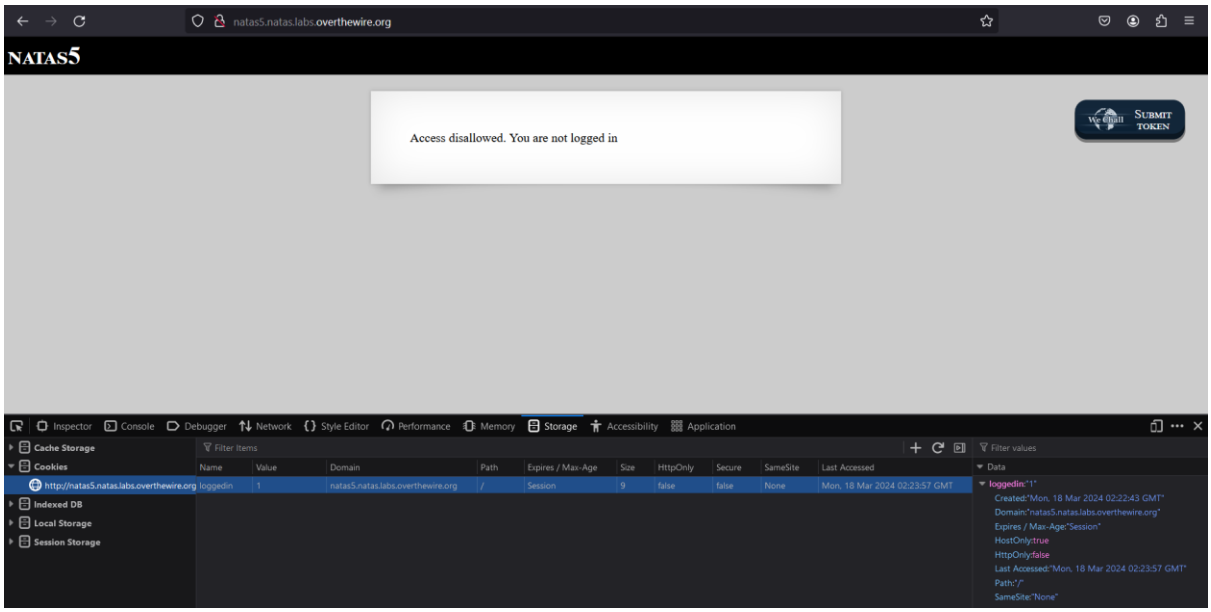
Go to Natas5 using the username and password.



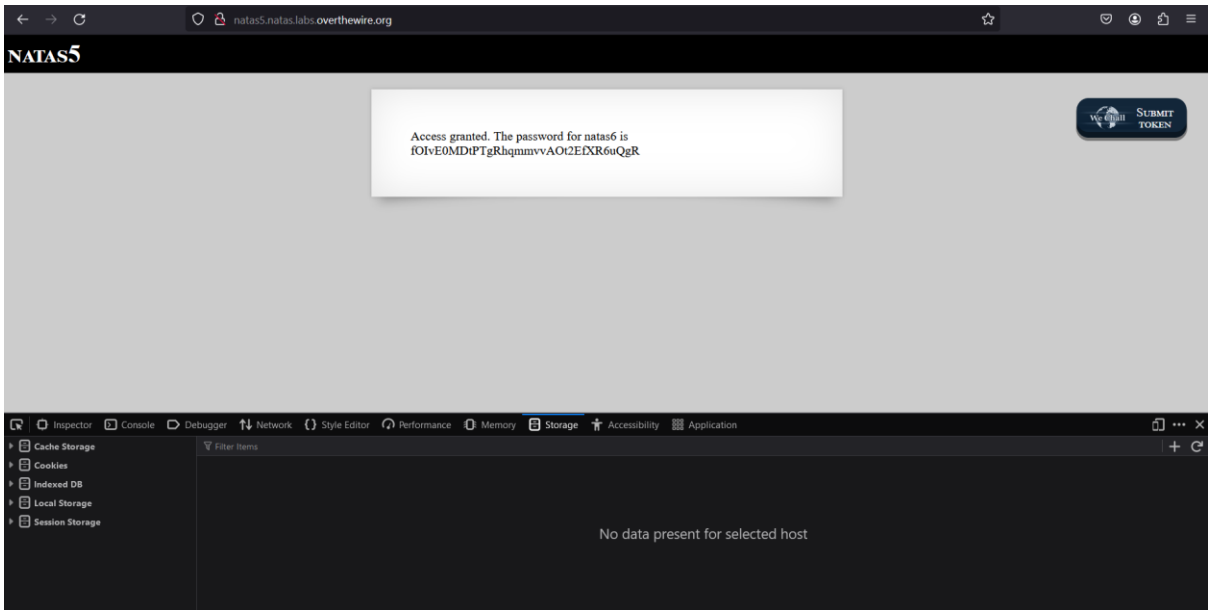
We can see the display message. Open inspect and go to the Cookies.



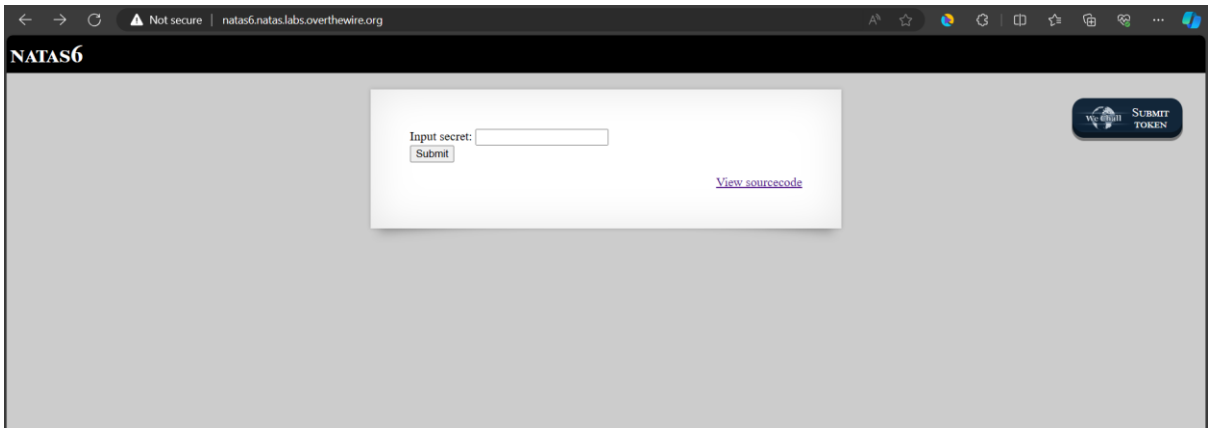
We can see that there are 0 loggedin. Change it to 1.



Refresh the page and get the natas6 password.

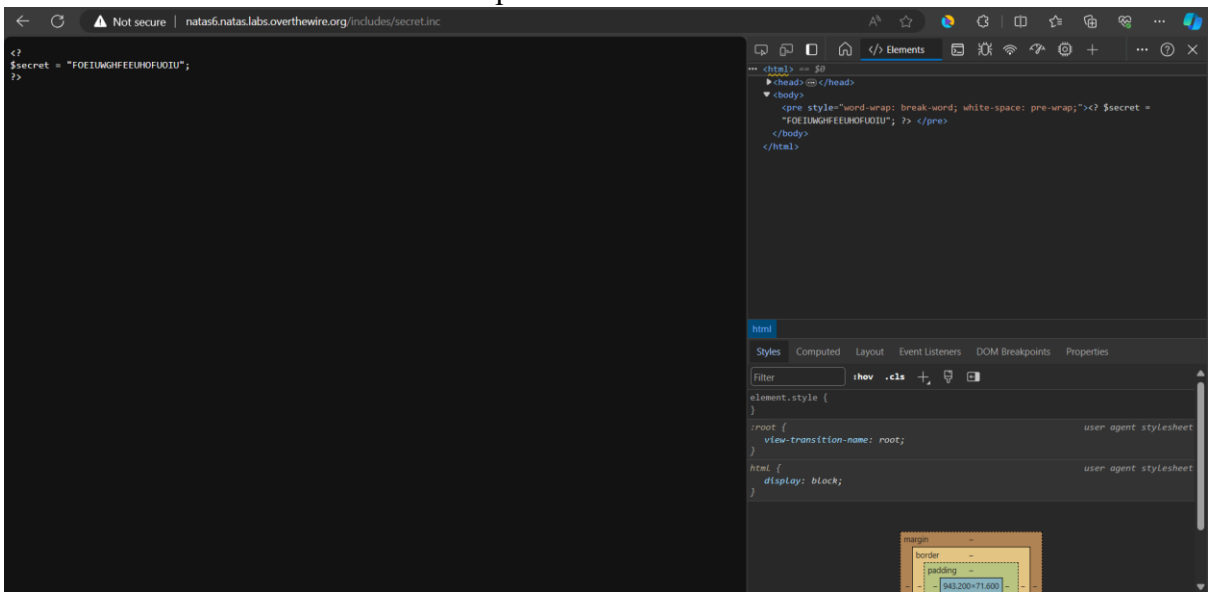


Natas6 -> Natas7

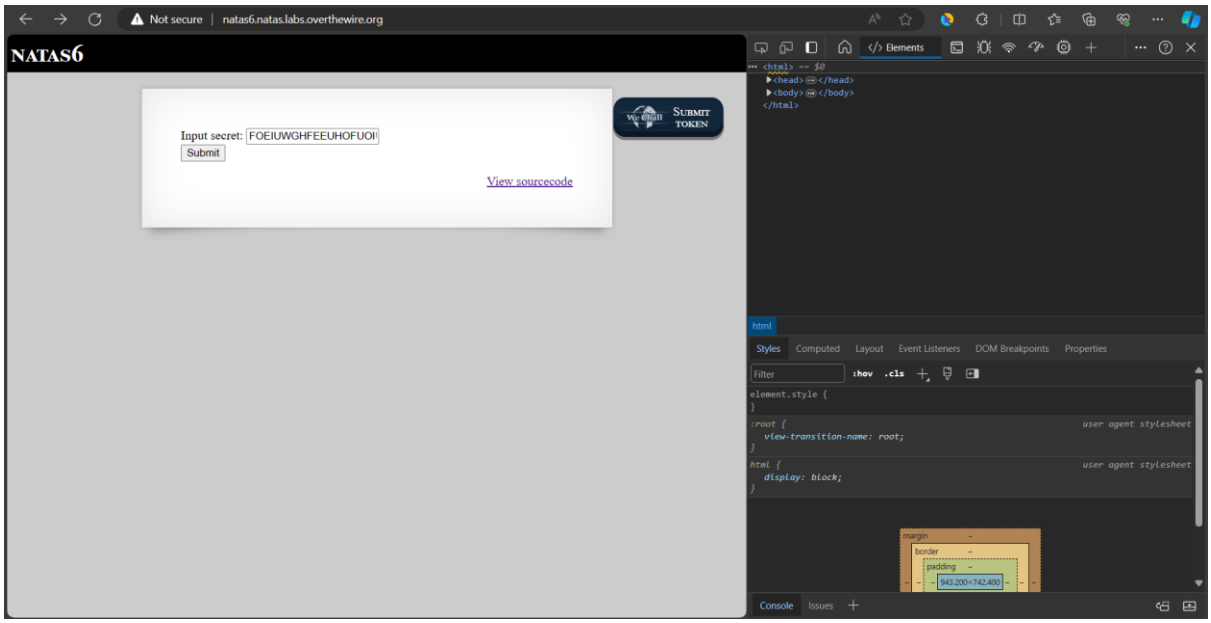


Go to Natas6 and view the source code that they gave. Find the hint.

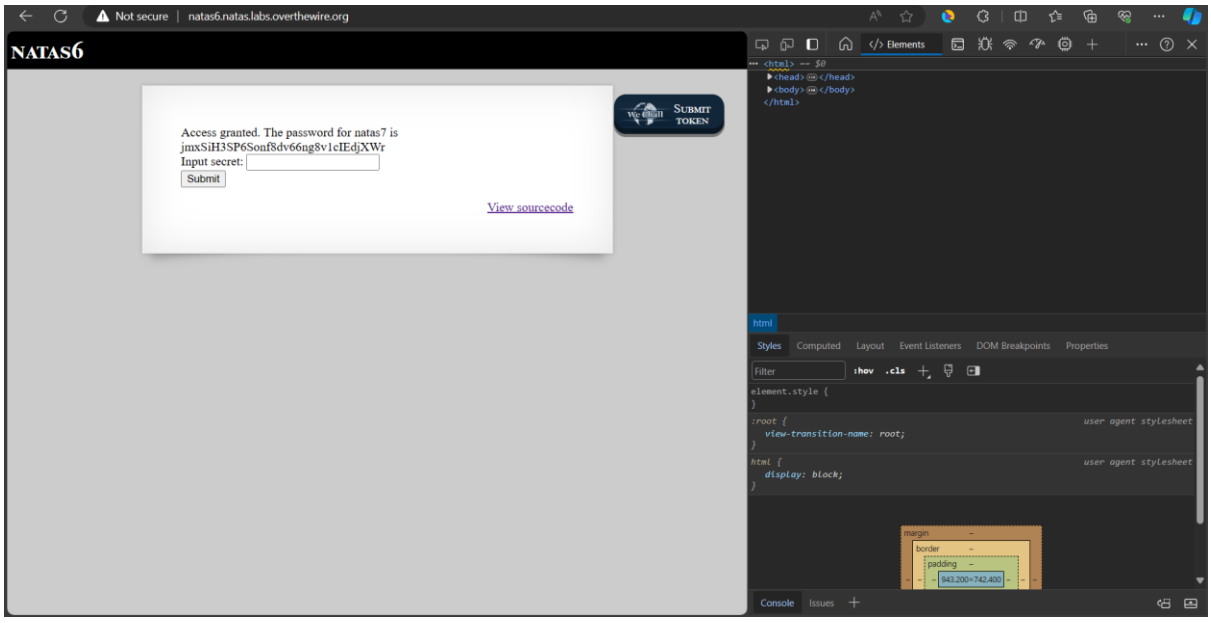
Go to “includes/secret.inc” and find input secret text.



Input it to the query.

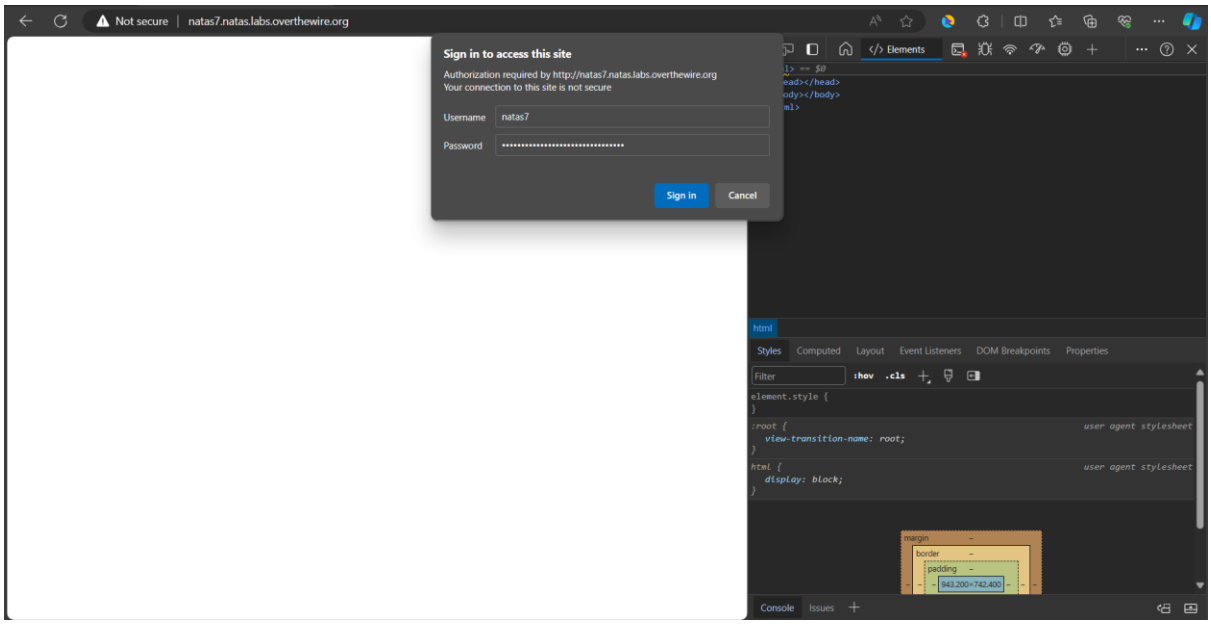


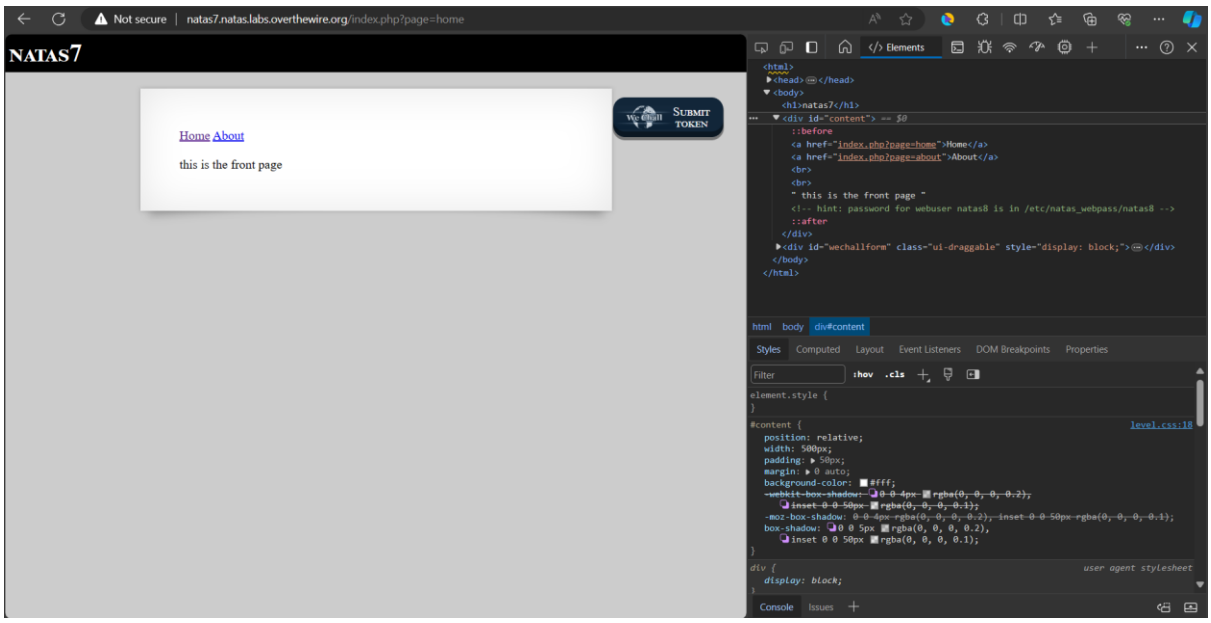
Now we can see the Natas7 password.



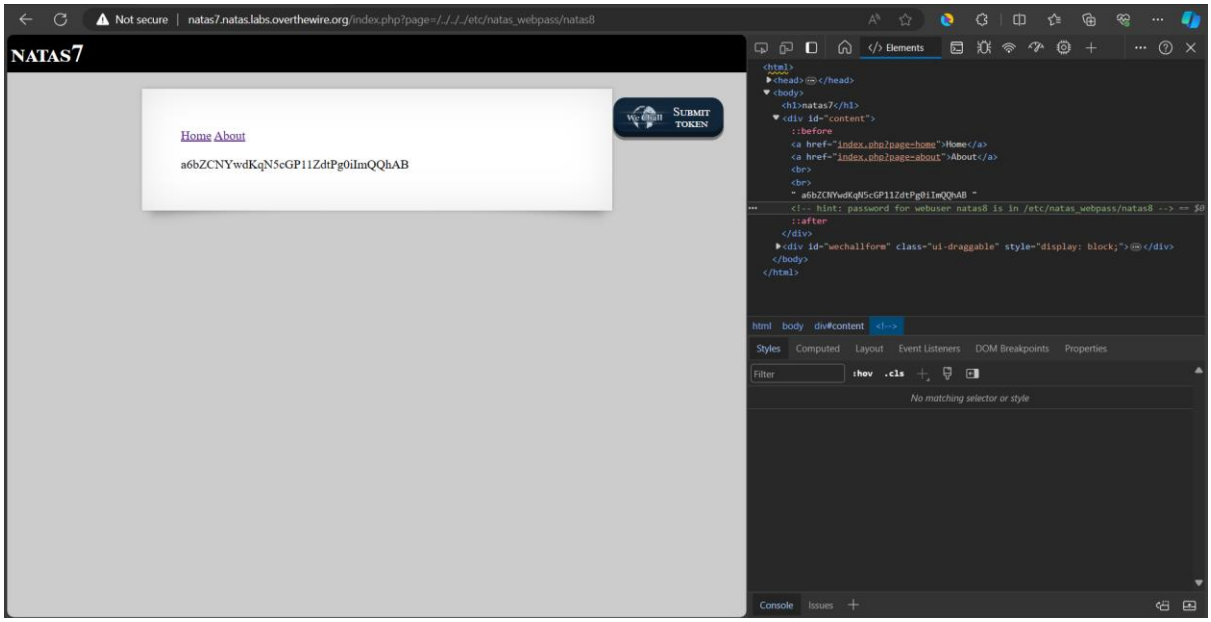
Natas7 - > Natas8

Go to Natas7 using the username and password". When we go to the webpage open inspector and find a hint link.



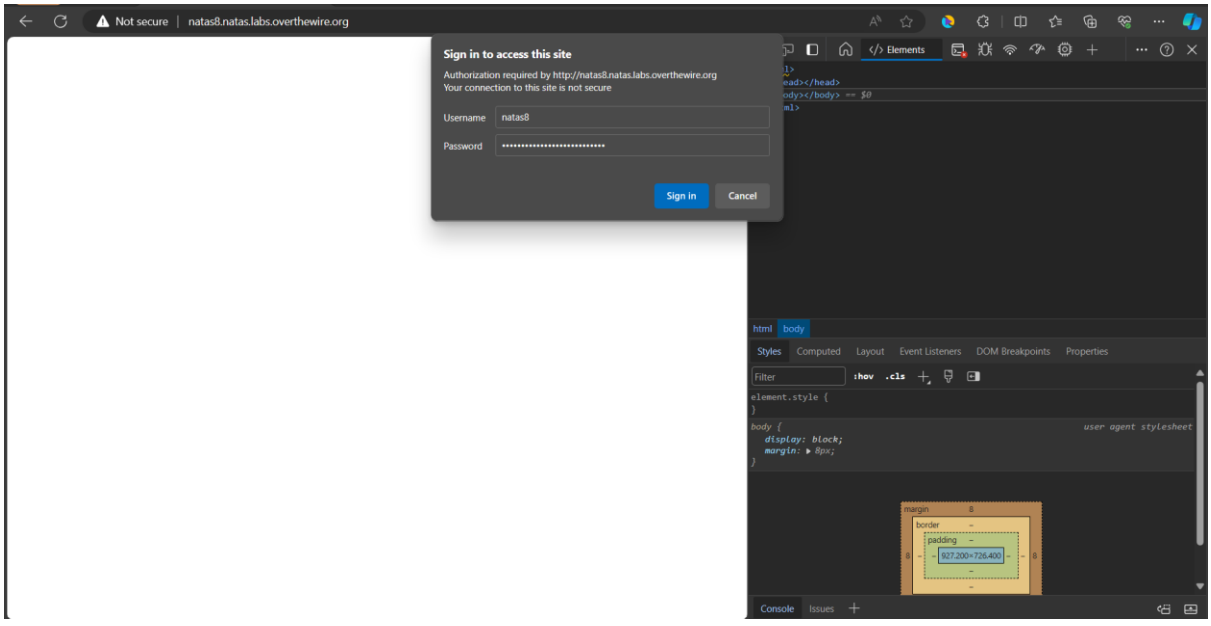


Go to that link. When we use that link correctly, we can get the password

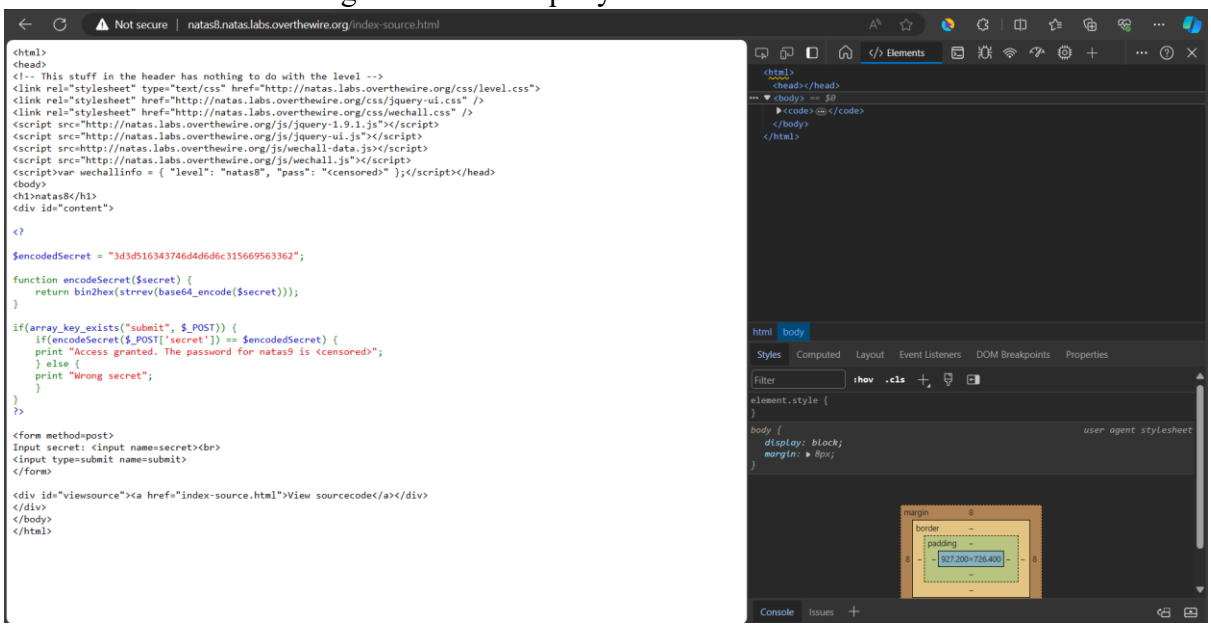


Natas8 -> Natas9

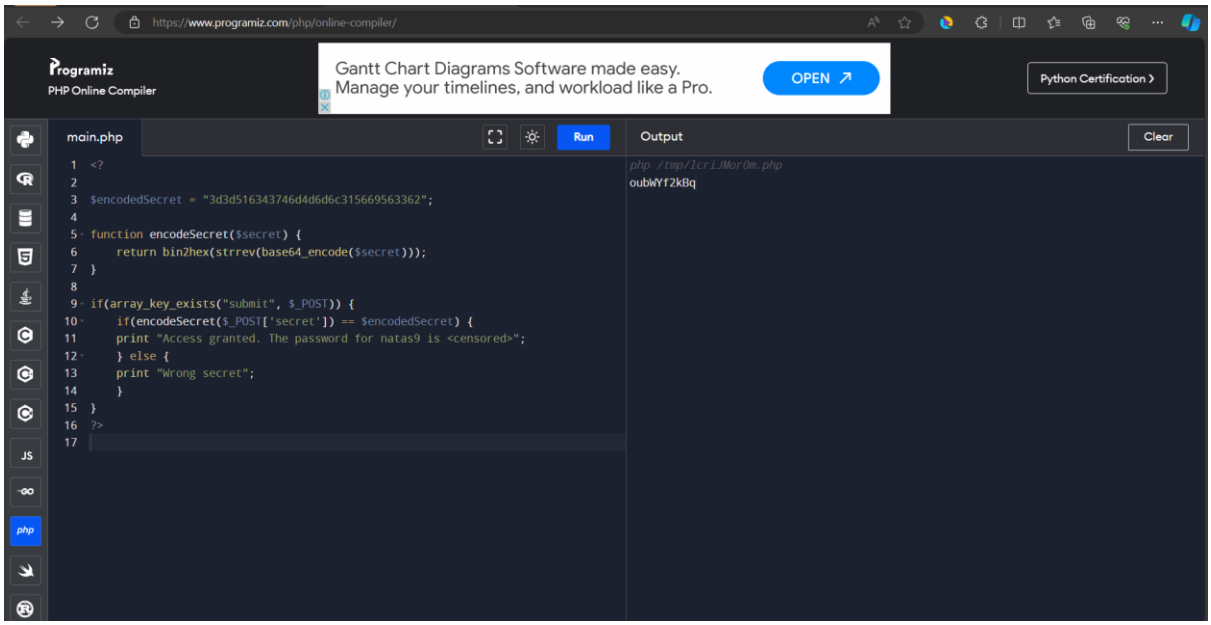
Initially go to the Natas8.



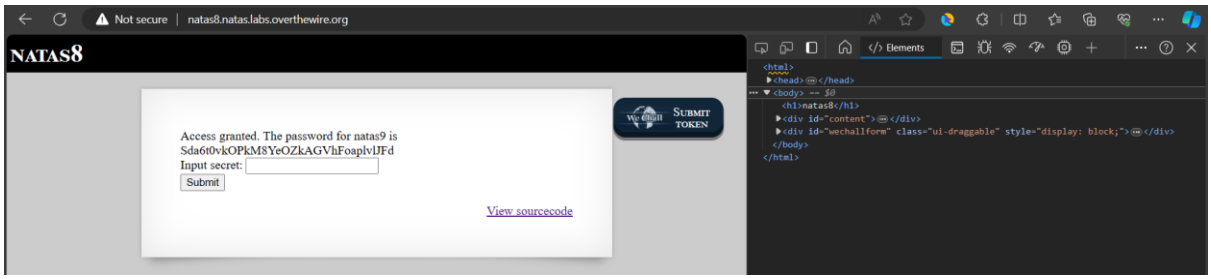
View the source code and get an encoded query.



Decoded that encoded query first.

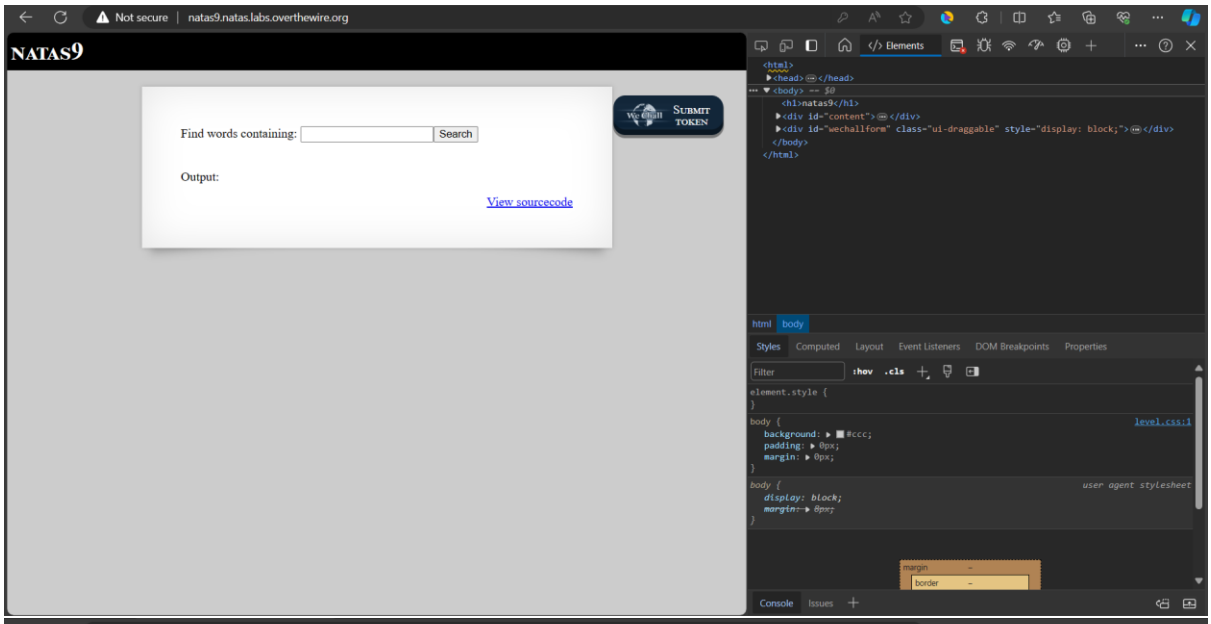


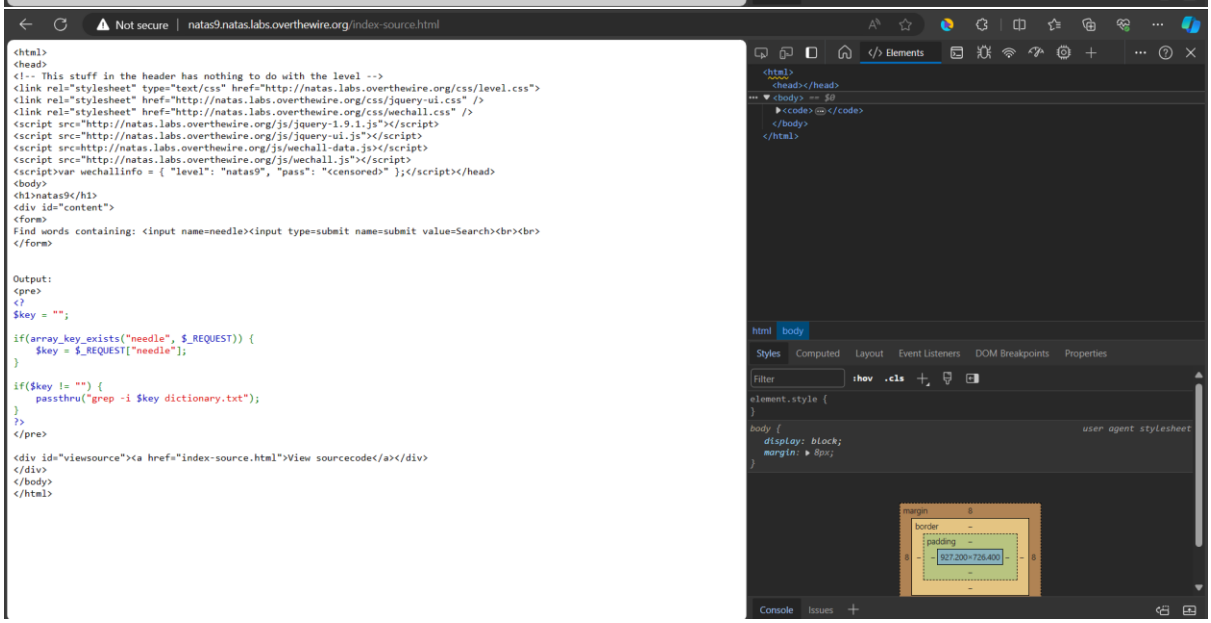
Submit the query using that decoded query and get the natas9 password.



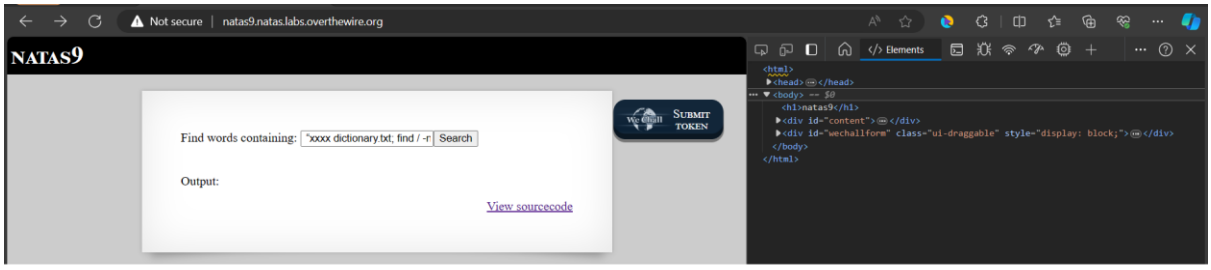
Natas9 -> Natas10

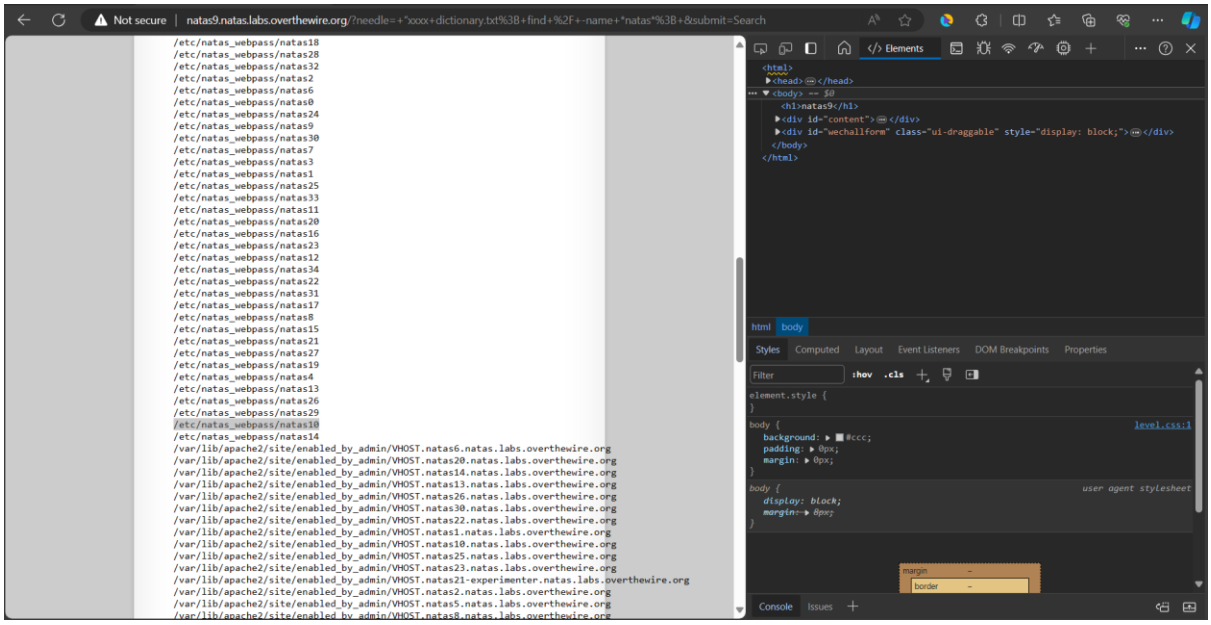
Go to Natas9 and view the source code. Find the hint.



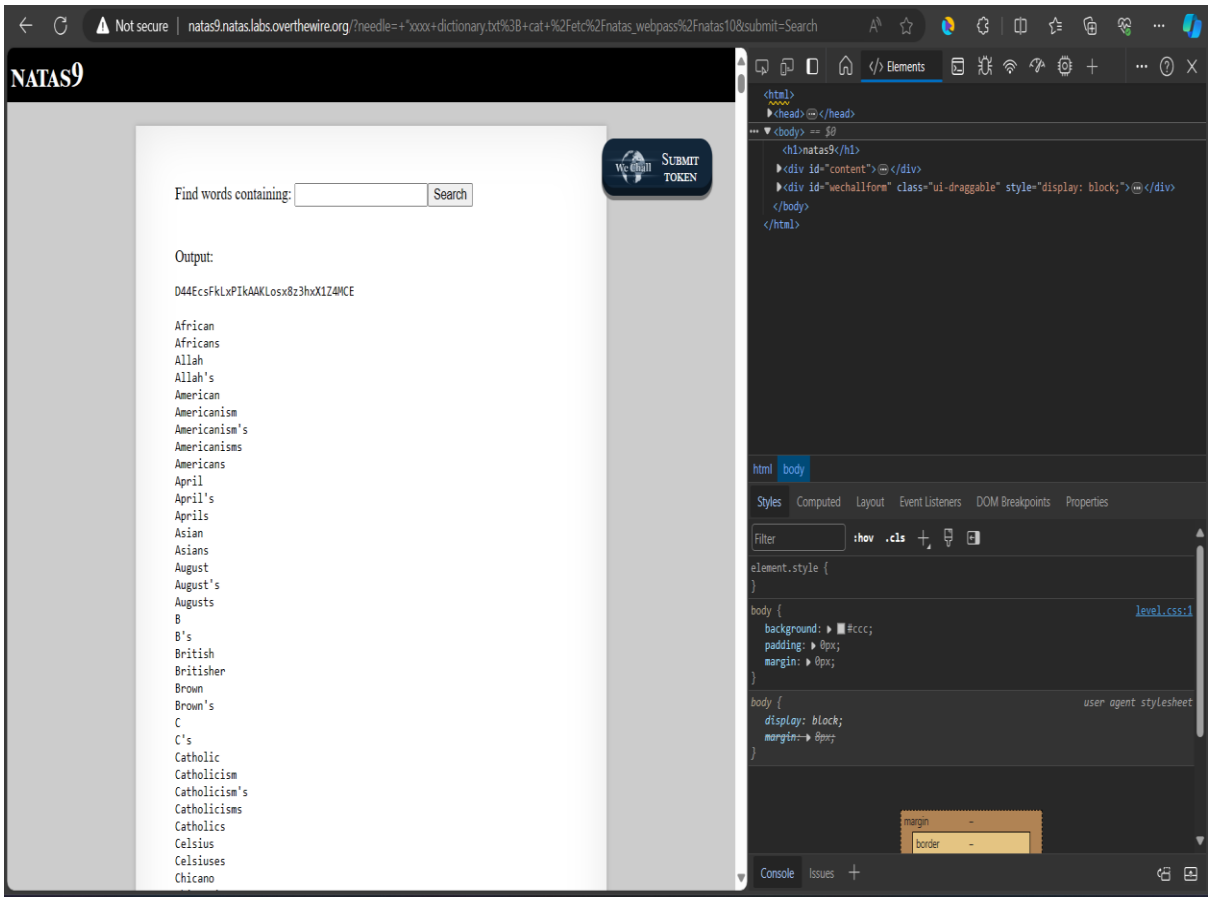


Find some words using “xxxx dictionary.txt; find / -name *natas*;



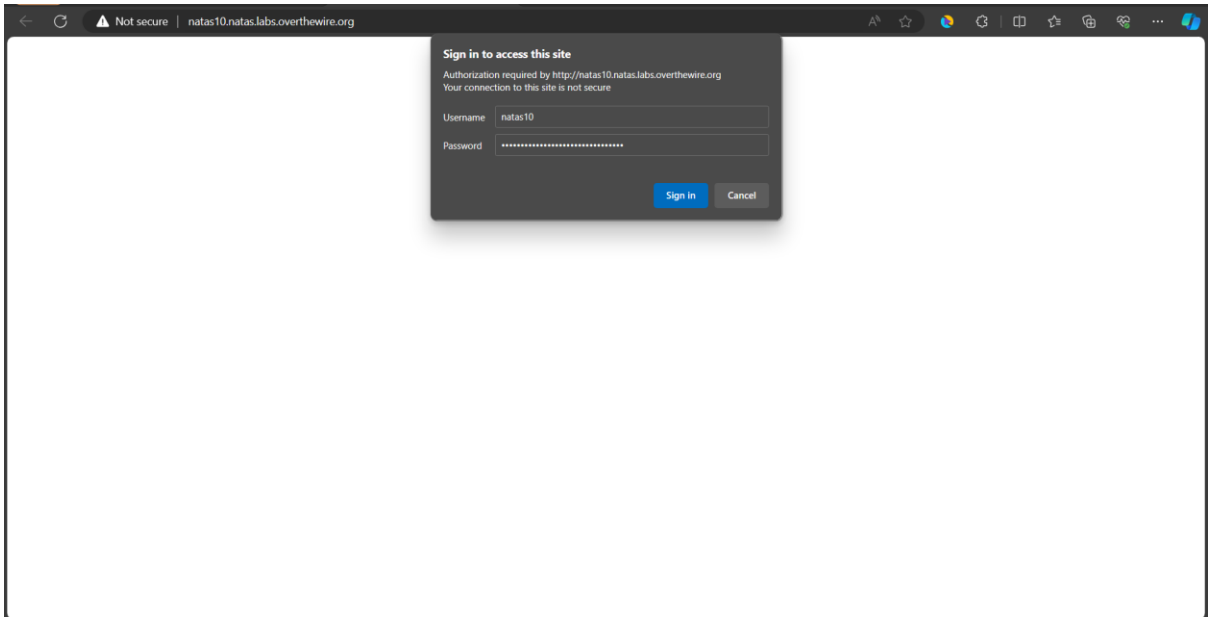


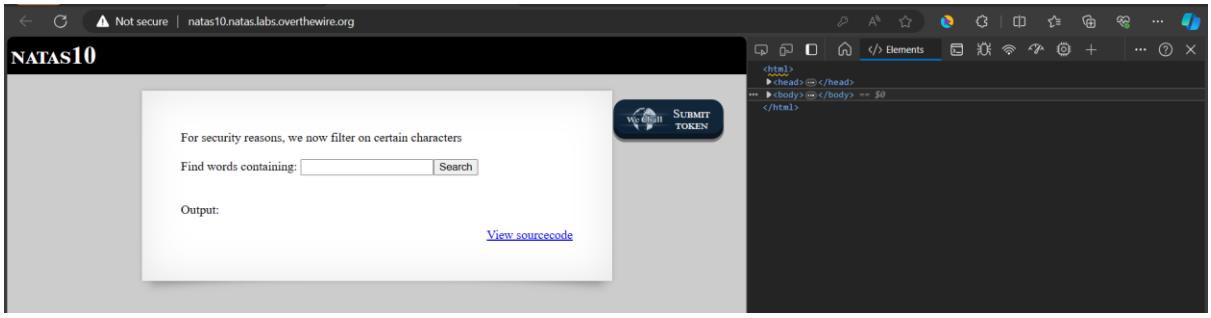
Using this "/etc/natas_webpass/natas10" we can find the password of Natas10.

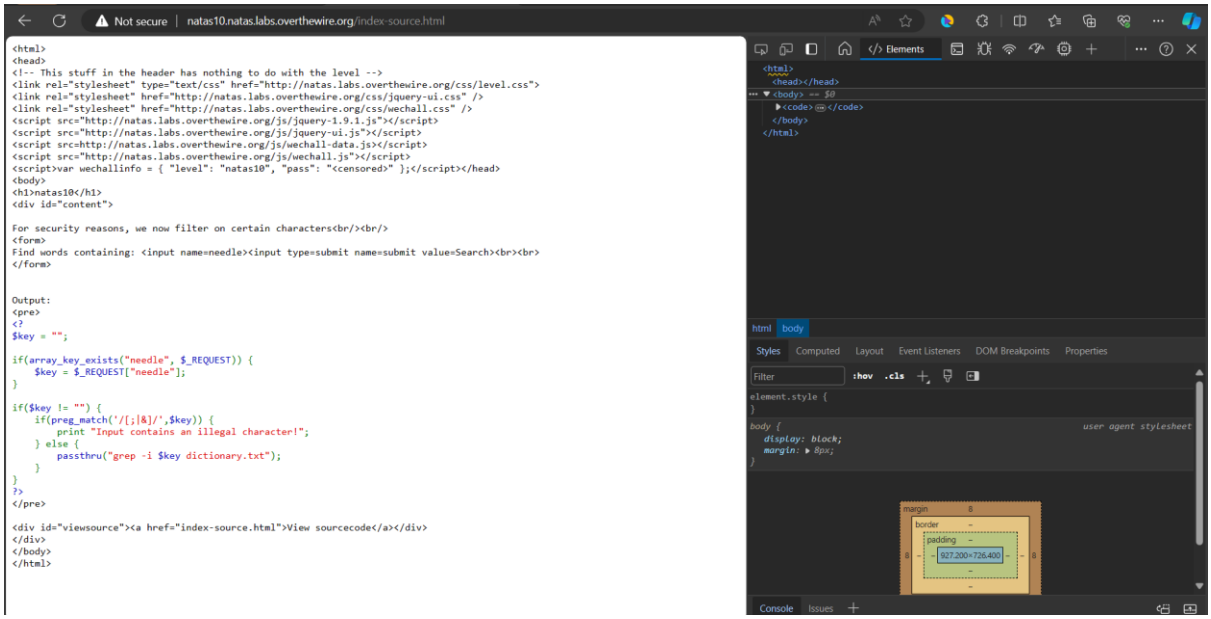


Natas10 -> Natas11

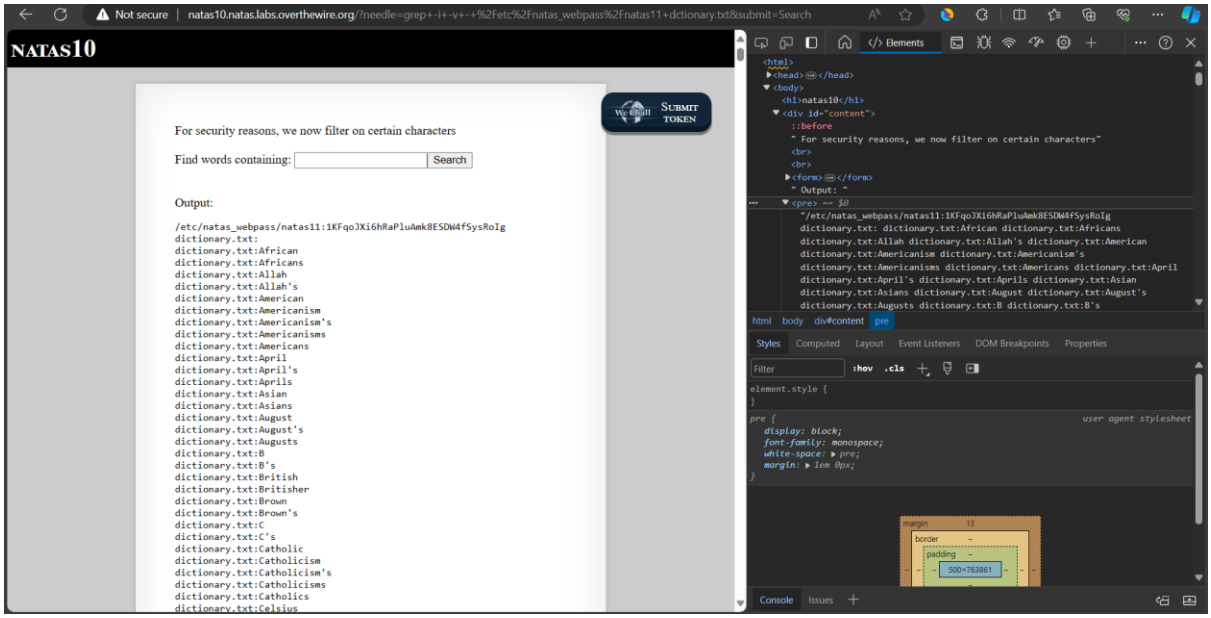
Go to Natas10 and view the source code





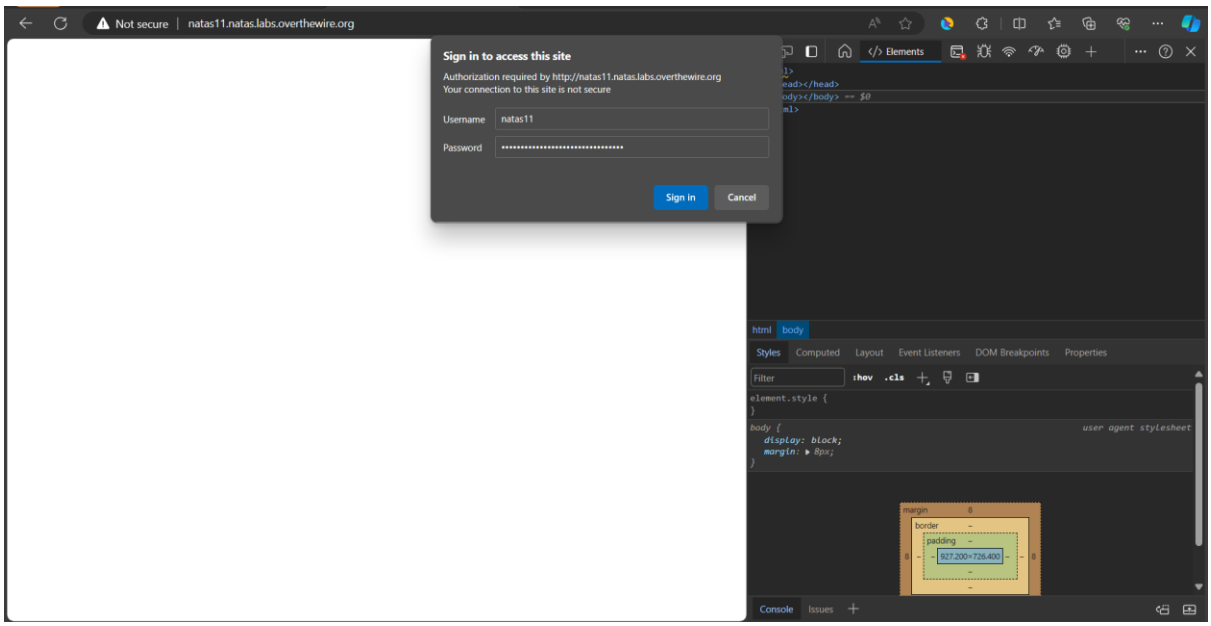


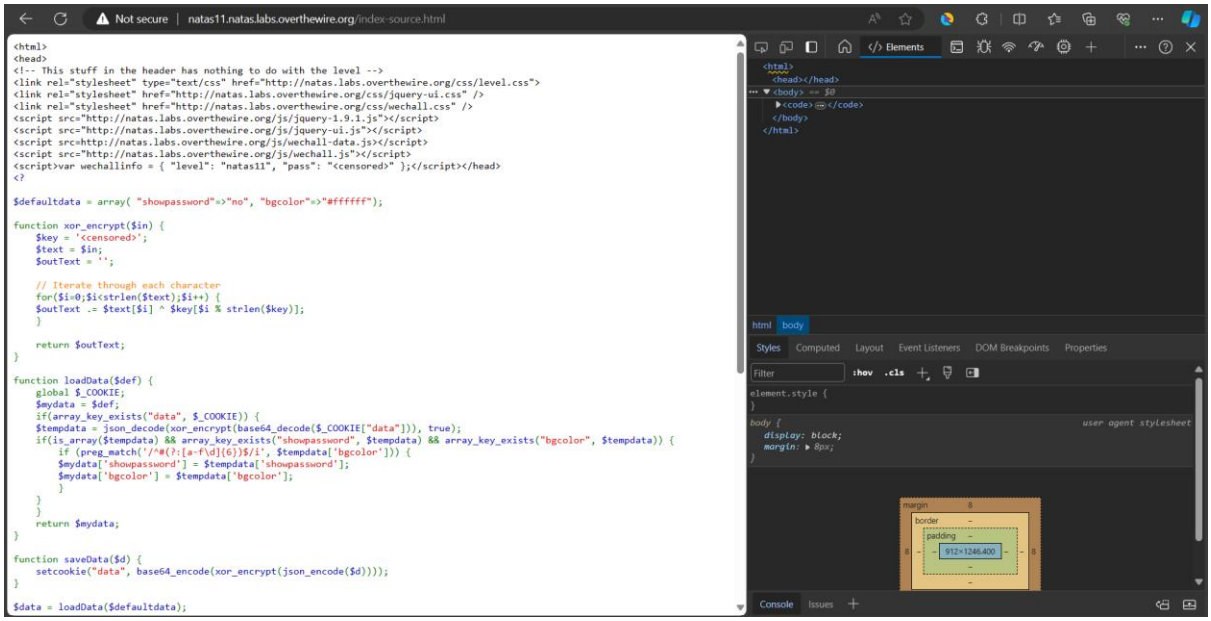
Type this one on the webpage search bar “grep -i -v /ect/natas_webpass/natas11 dctionary.txt”. And get the Natas 11 password.



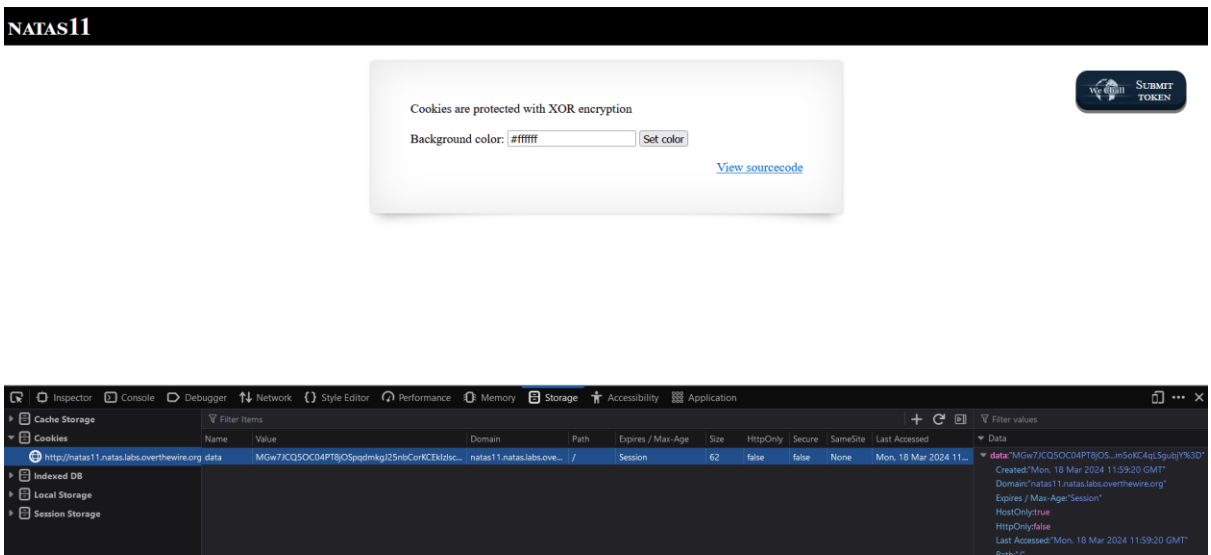
Natas11 -> Natas12

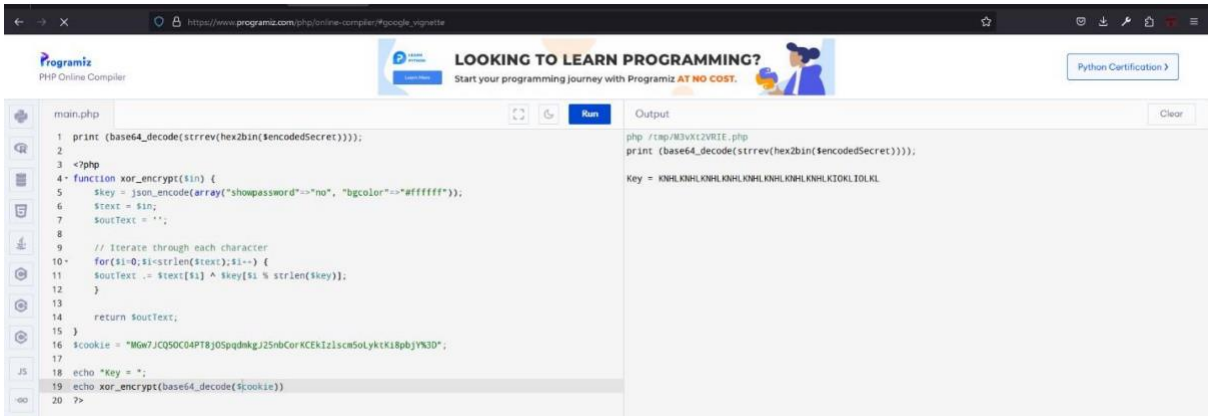
Go to Natas11 and open the source code.



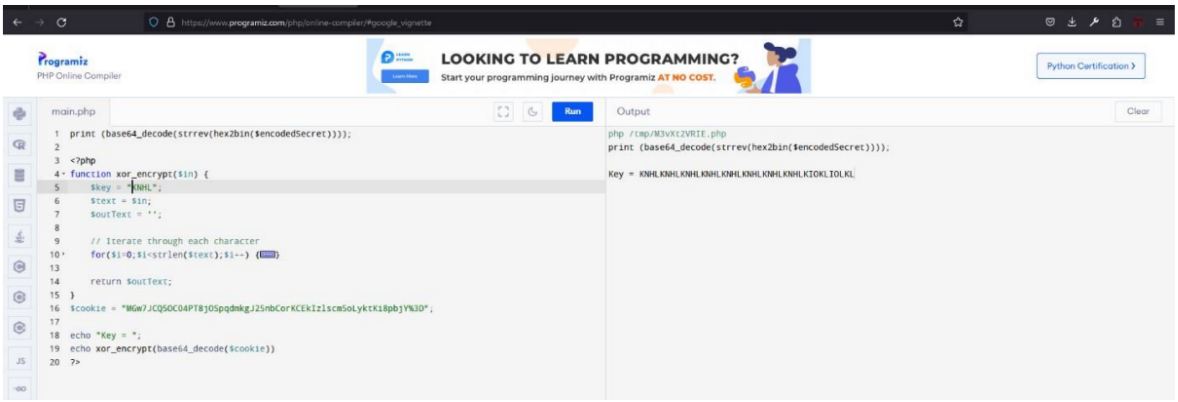


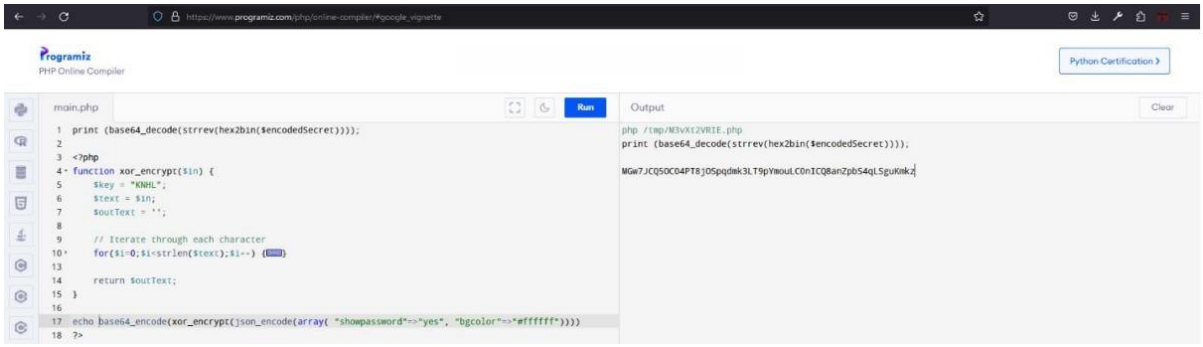
Cookies are encoded, so we need to decode them using this PHP code. Firstly, we need to find the key. We can find it using this source code.



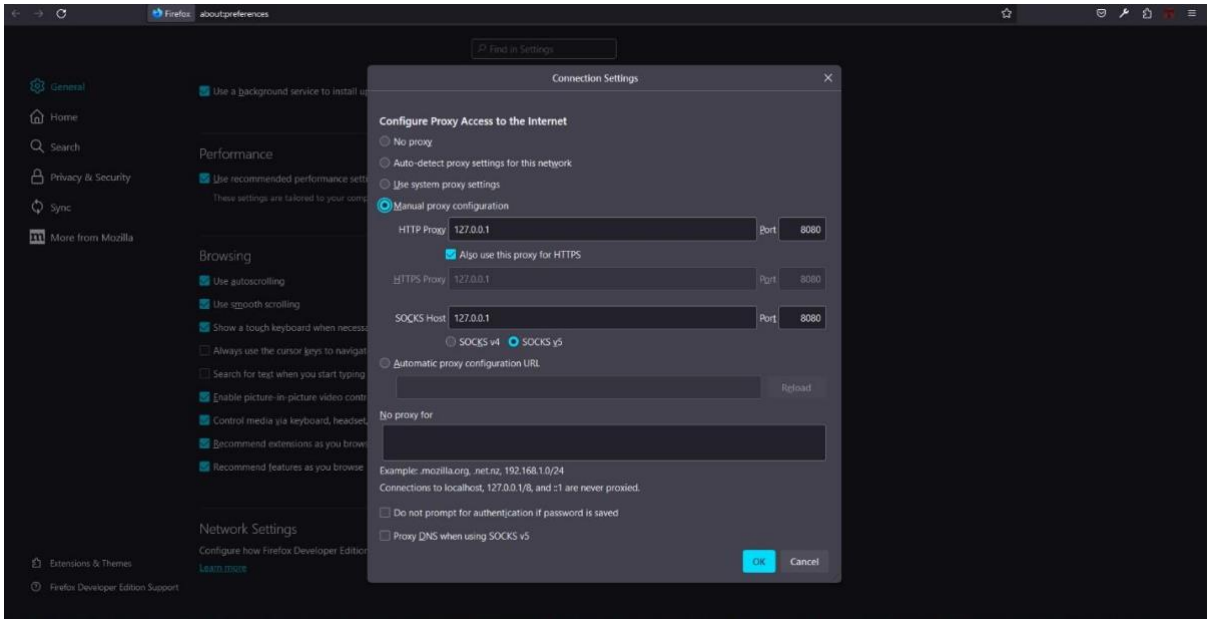


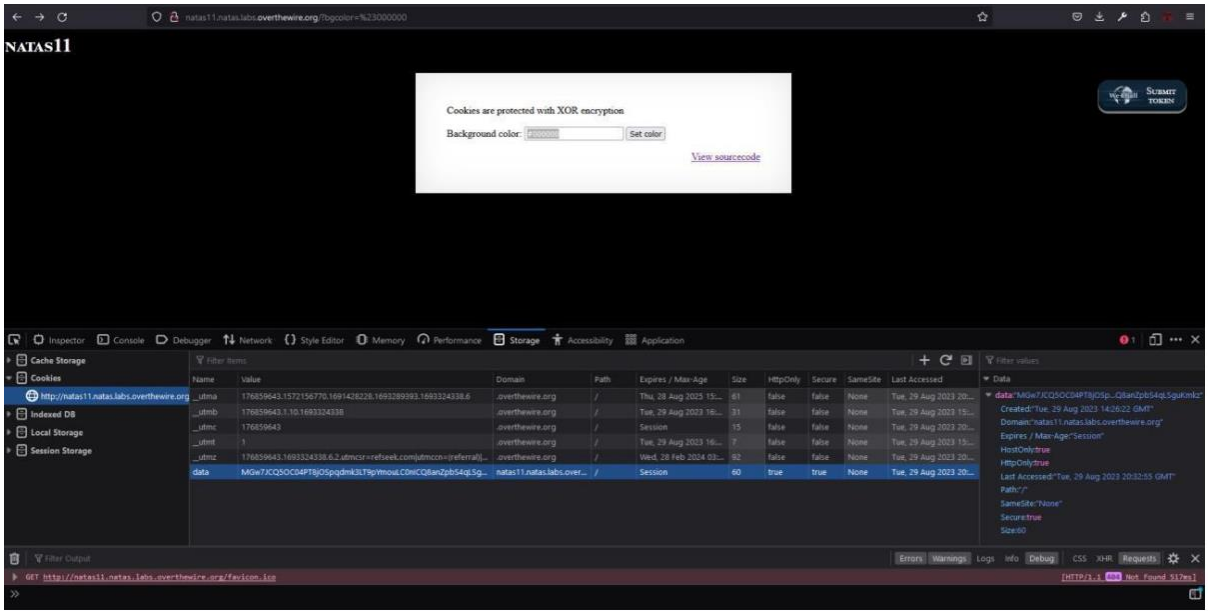
After finding the key we can decode to cookies.





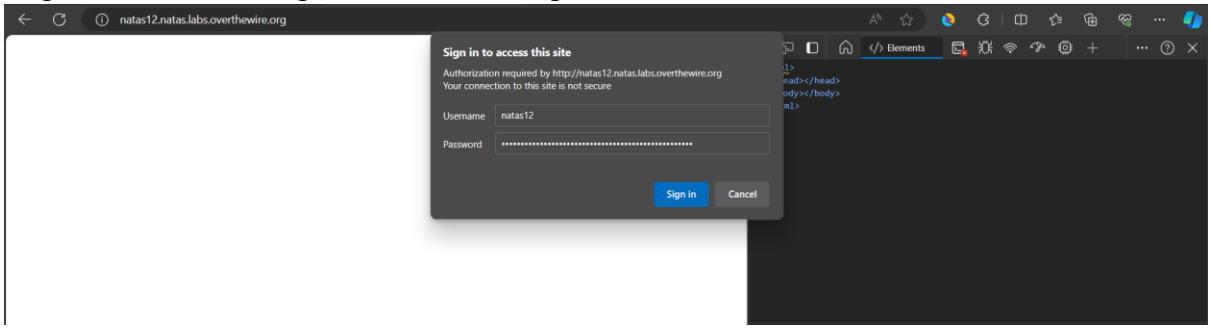
After the change proxy setting, we can change the cookies. After changing it, the password can be contained.



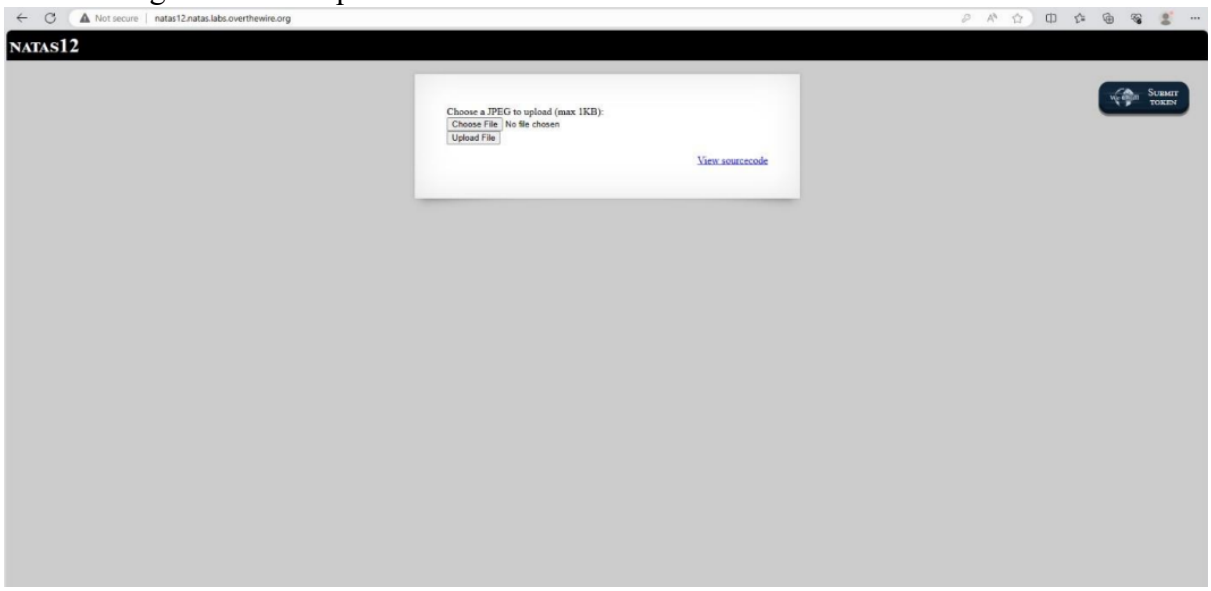


Natas12 -> Natas13

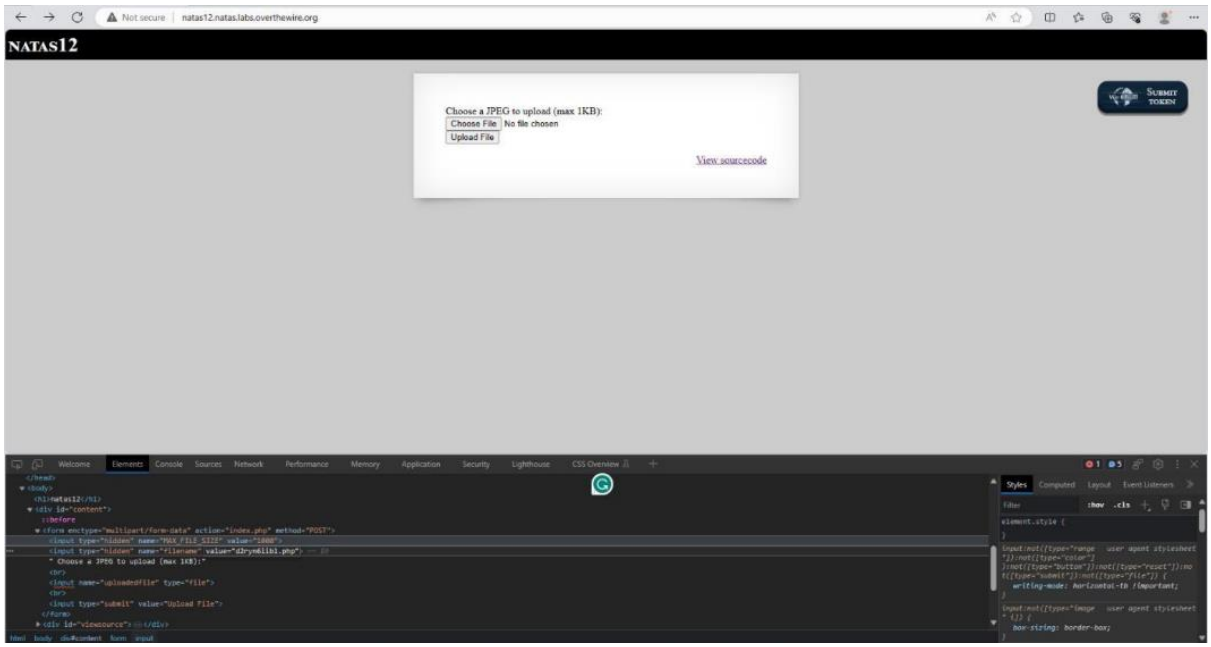
Log in to Natas12 using the username and password.



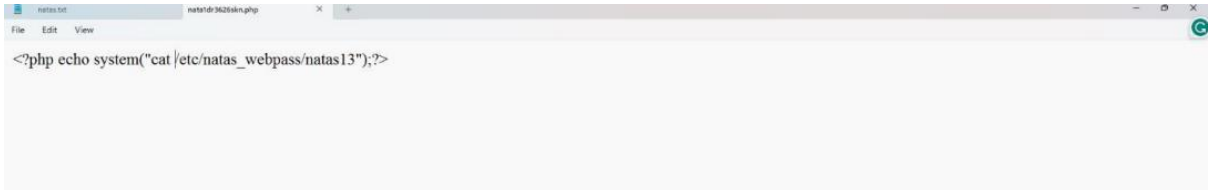
After we log we need to upload a file. So we need to find out it.



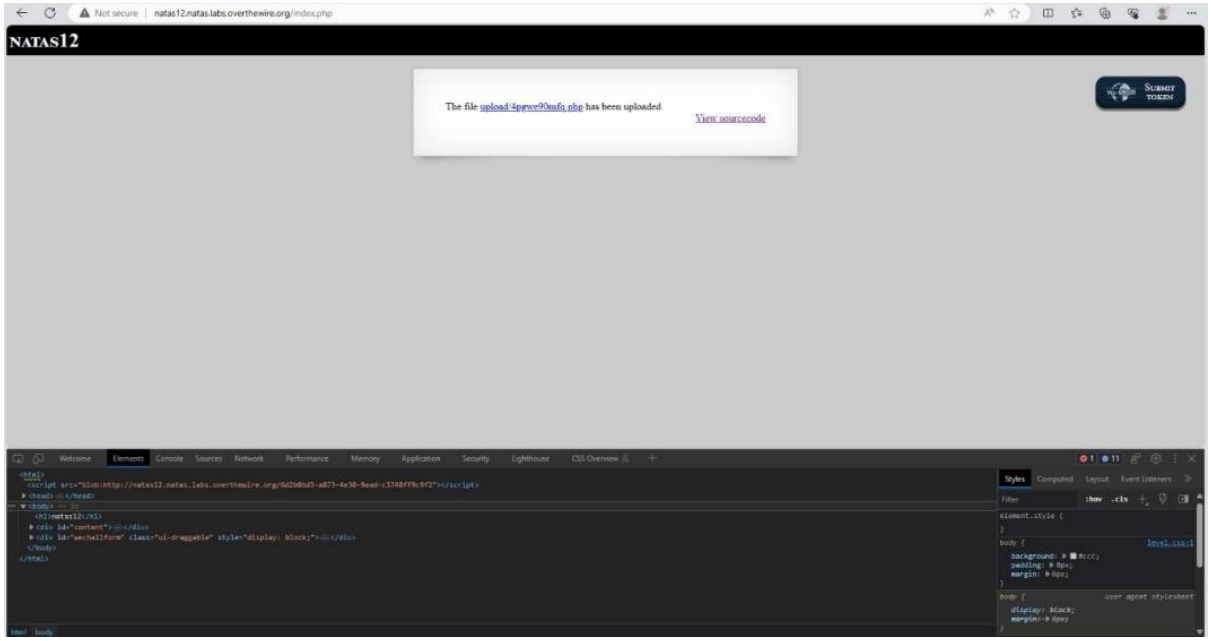
Initially, open elements and find a jpg file in the code. Change it jpg to a php file.



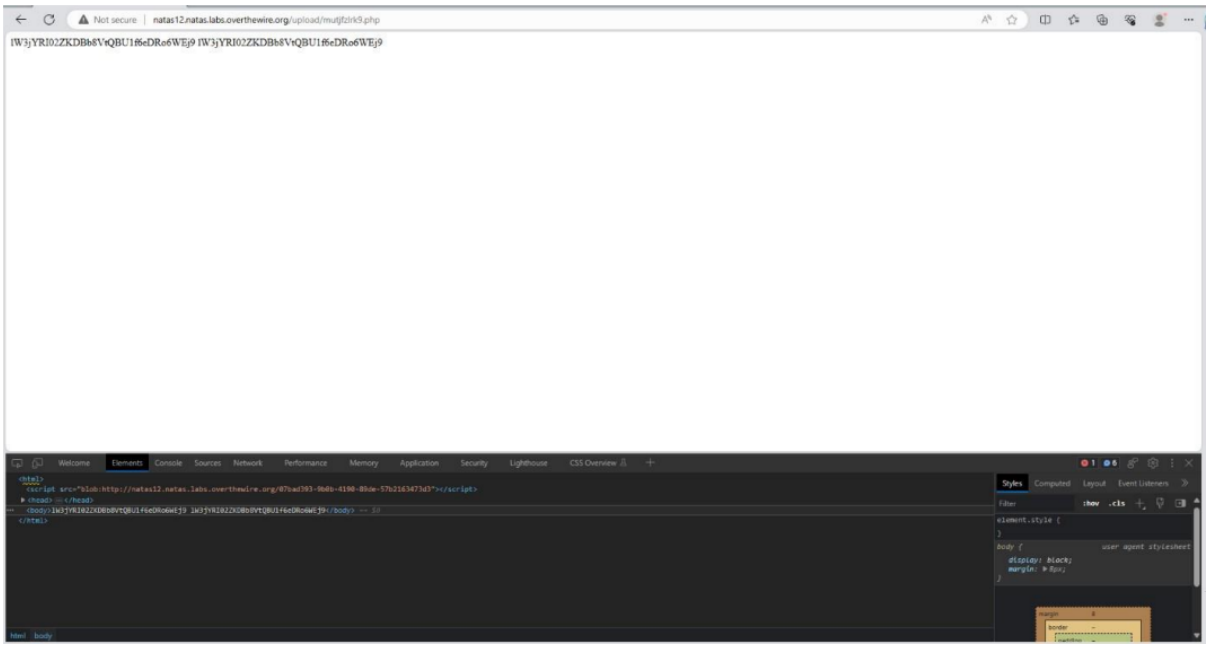
Open notepad and write this code into the notepad. After writing it save it as modified in the code.



After writing upload it to natas12.

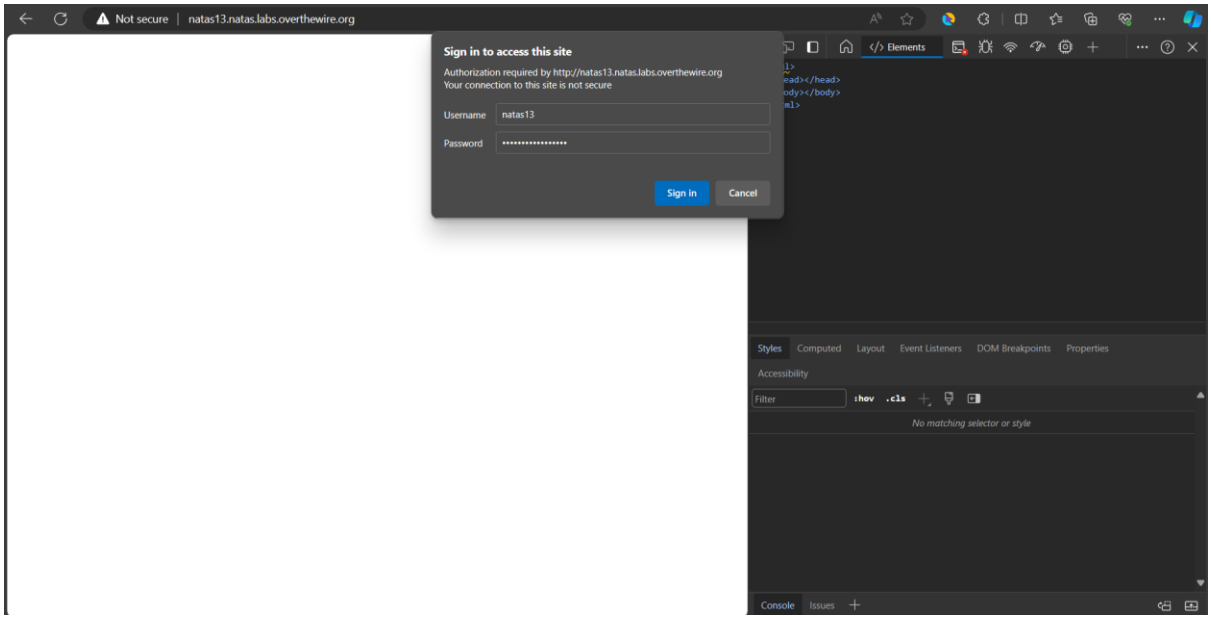


When we upload the system shows us that file on the webpage. After we click it, we can see the password there.

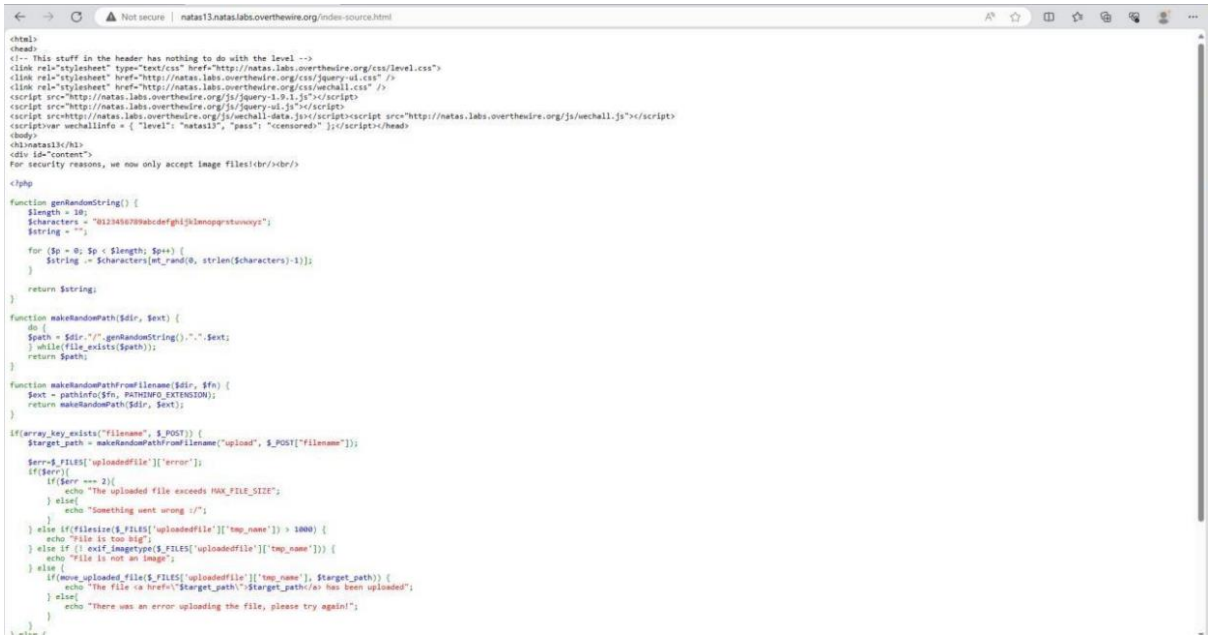


Natas13 -> Natas14

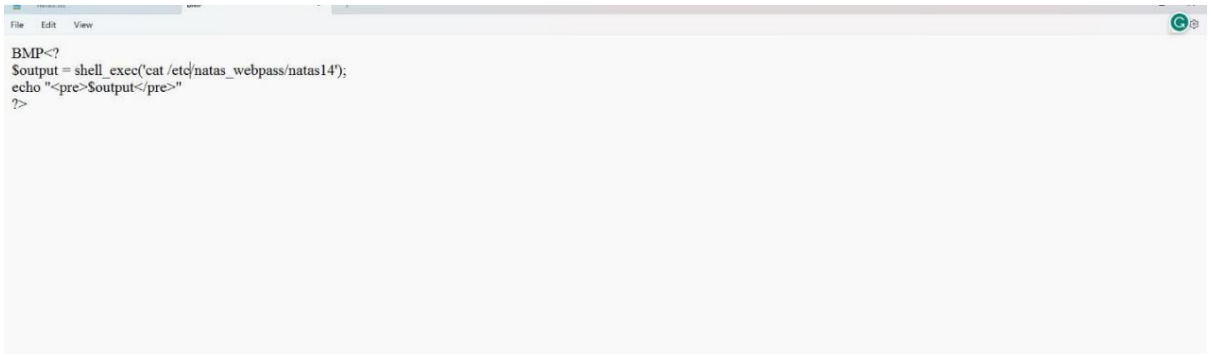
Log into Natas13.



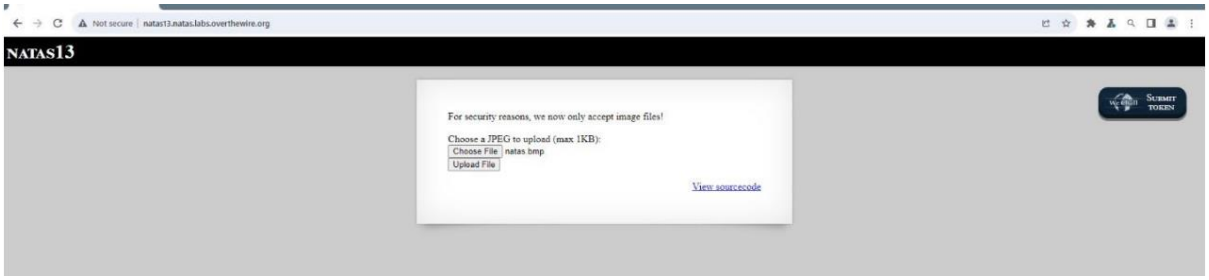
Also here is to upload a jpg file, we don't have it so go to the source file and see if there is a hint.



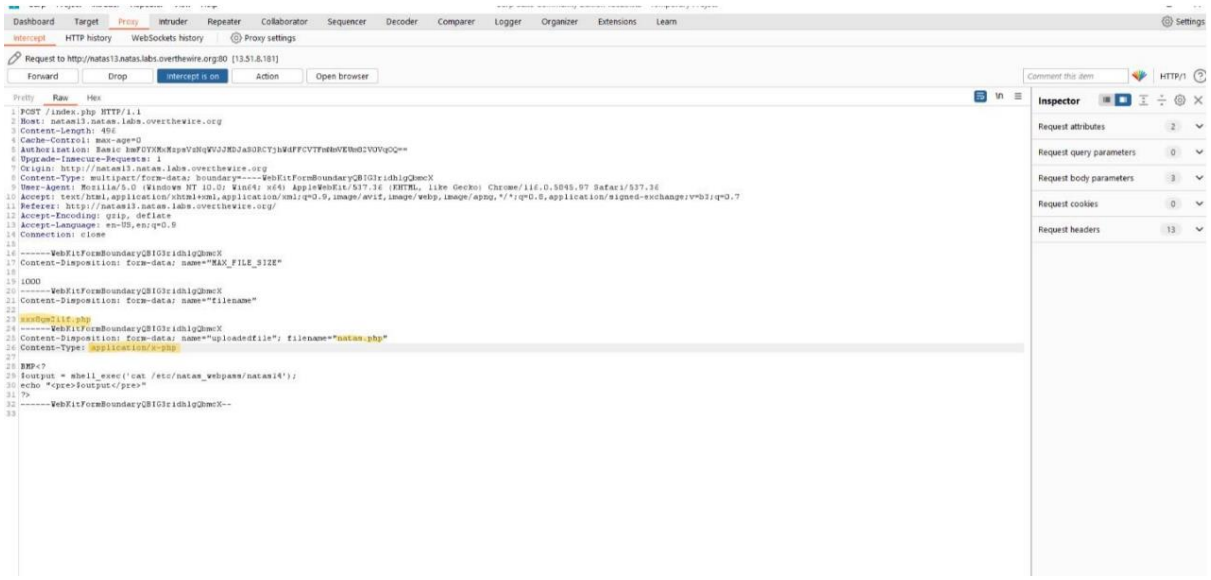
Now open the notepad and write this code. After writing it save it as a ".bmp" file.



Open the burp suite software log into Natas13 and upload that bmp file to it.



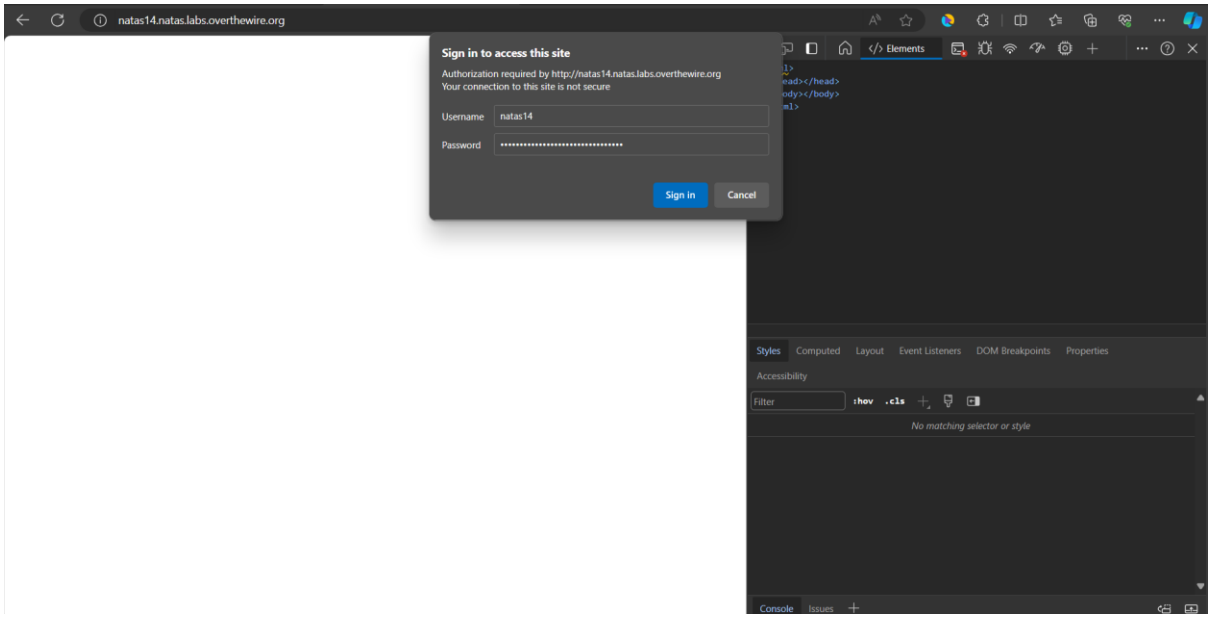
Change these jpg files as php files. After changing them forward proxy file code.



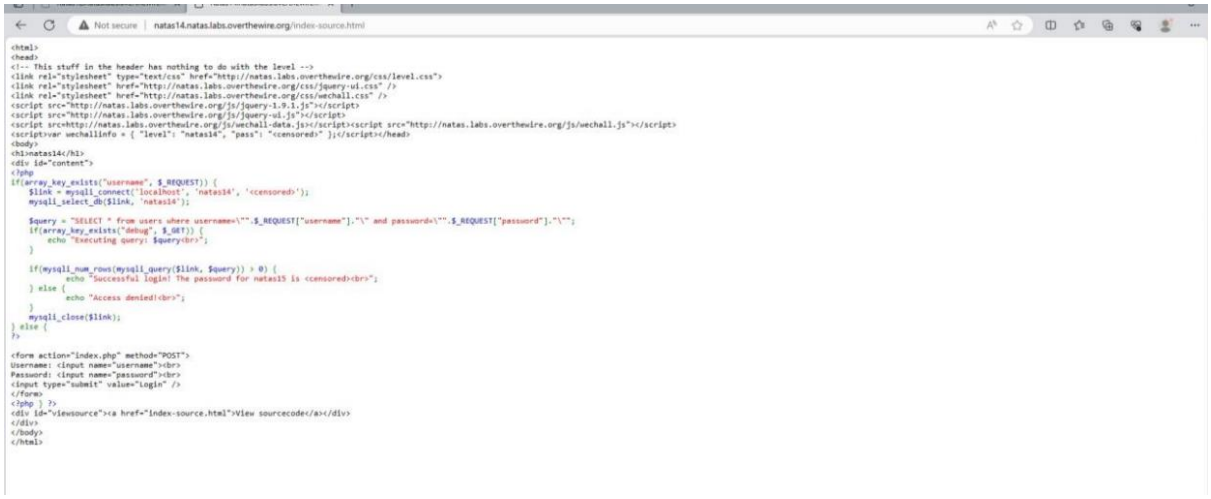
Now we can see the uploaded php file, once we click it we can get the password.

Natas14 -> Natas15

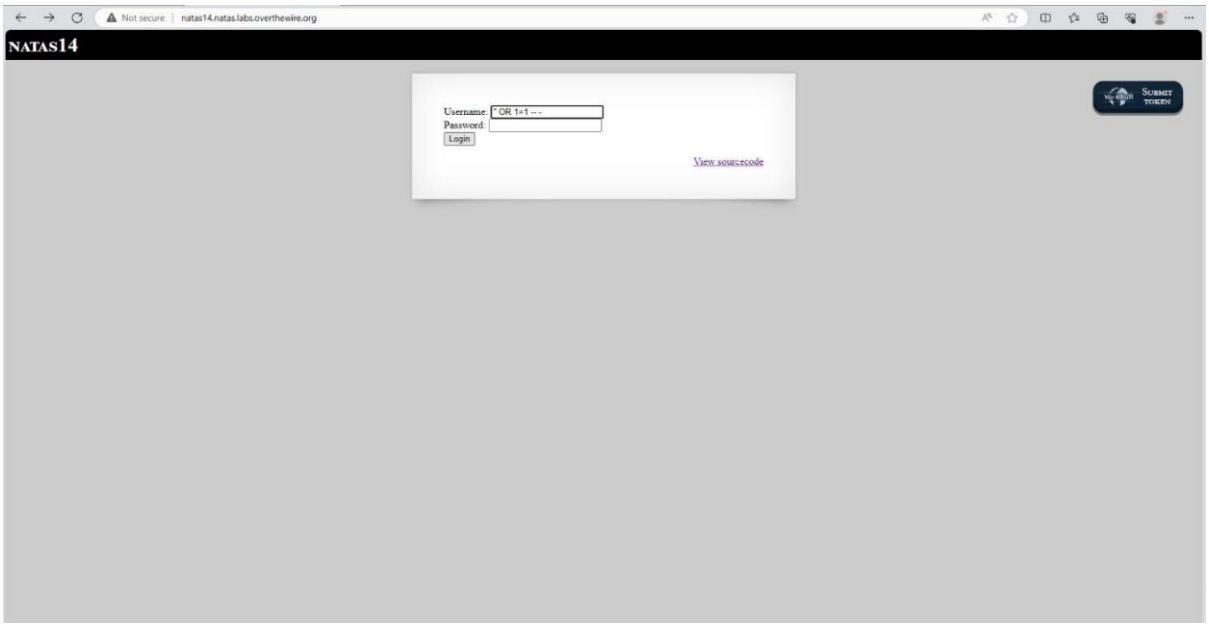
Log into Natas14 first.



First, look at the source code and read it carefully and try to understand.



Now fill the username field using (“ OR 1=1 -- -) and password field keep empty.



After we login, they give us the password of next level.