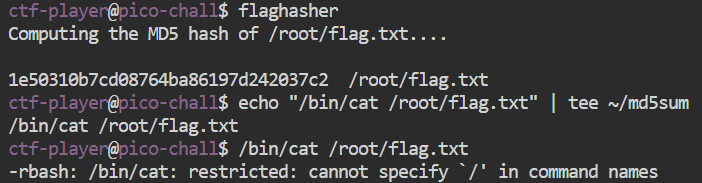
Hash-Only-2

At the beginning of this pico challenge, we use ‘ls -la’ command to try to capture where is the flag. As we cannot find by using the ‘ls -la’ command. We try to use find command which can help us to find out where is the flaghasher are.

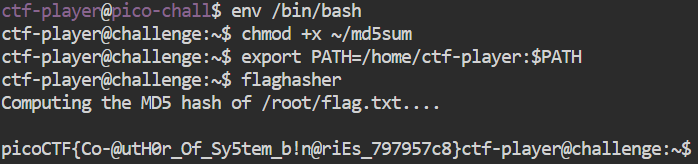
A screenshot of a computer

AI-generated content may be incorrect.

When we found that the flaghasher is at the /usr/local/bin/flaghasher. We try to execute it by using ‘flaghasher’. But that only show the md5 hash of it. So we replace md5sum with a fake script that just prints the contents of /root/flag.txt with this code ‘echo "/bin/cat /root/flag.txt" | tee ~/md5sum’. And try to execute the flag again but the path command is getting block.



So, we try to spawn a clean shell to escape the blocking. After that, we make it executable with ‘chmod +x ~/md5sum’ and export them to our $PATH with this code ‘export PATH=/home/ctf-player:$PATH’. And finally, we can get the flag by just typing the ‘flaghasher’ and the flag will print it out.



This challenge demonstrates a **PATH hijack vulnerability** where a privileged binary uses an unqualified command (md5sum) and relies on the user's $PATH