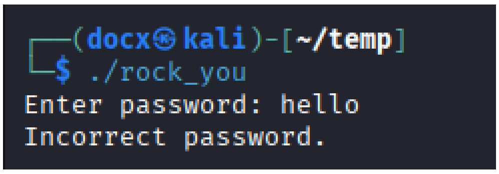
# ROCK_YOU

so we try strings on the binary to check if we get any flags and we find out it is a fake one
so we try executing it



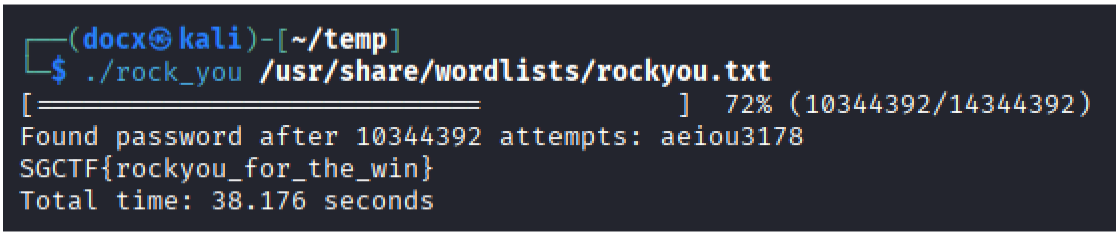
```
┌──(docx㉿kali)-[~/temp]
└─$ ./rock_you
Enter password: hello
Incorrect password.
```

which says it is wrong
in the challenge description it said something about a list

‘ You might search endlessly, yet the answer may have been within
reach from the start — concealed inside a list you already know ’

and the challenge name hints at **rockyou.txt**

sit also mentioned that the binary is wise enough to read each lines so we try
./rock_you /usr/share/wordlists/rockyou.txt



```
┌──(docx㉿kali)-[~/temp]
└─$ ./rock_you /usr/share/wordlists/rockyou.txt
[════════════════════════════             ]  72% (10344392/14344392)
Found password after 10344392 attempts: aeiou3178
SGCTF{rockyou_for_the_win}
Total time: 38.176 seconds
```

which gives us the flag
**SGCTF{rockyou_for_the_win}**