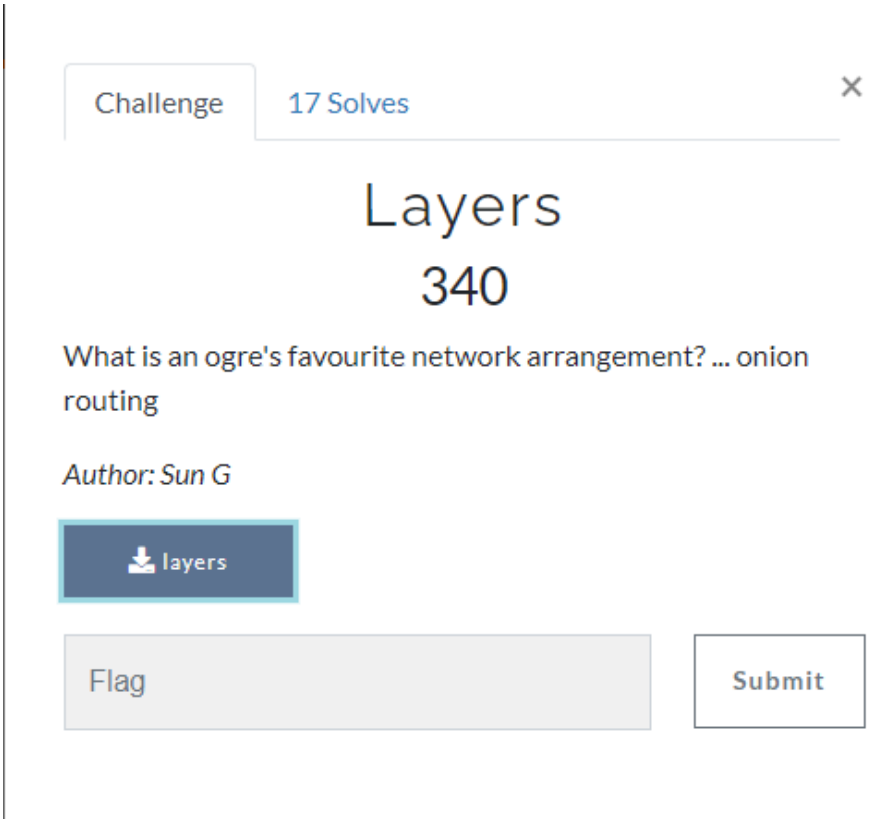
Layers CTF challenge - secchallenge.crysys.hu

1. brief explanation about the challenge:



2. After downloading the “Layers” exe file and running the program we got this result:

```
┌──(noa㉿kali)-[~/Desktop]
└─$ ./layers
Okay, um, Ogres are like onions.
```

the program is waiting for some input, and then printing “Wrong” to screen if the input is not the right string.

3. we tried to see if we can find some suspicious strings:

```
zsh: corrupt history file /home/noa/.zsh_history
┌──(noa㉿kali)-[~/Desktop]
└─$ strings layers
/lib64/ld-linux-x86-64.so.2
__gmon_start__
_ITM_deregisterTMCloneTable
_ITM_registerTMCloneTable
_ZdlPvm
_ZSt29_Rb_tree_insert_and_rebalancebPSt18_Rb_tree_node_baseS0_RS_
_ZSt18_Rb_tree_incrementPSt18_Rb_tree_node_base
__gxx_personality_v0
_Znwm
_ZSt18_Rb_tree_decrementPSt18_Rb_tree_node_base
_Unwind_Resume
__stack_chk_fail
putchar
stdin
printf
fgets
__cxa_atexit
strcmp
__libc_start_main
libstdc++.so.6
libm.so.6
libgcc_s.so.1
libc.so.6
GCC_3.0
CXXABI_1.3
CXXABI_1.3.9
GLIBCXX_3.4
GLIBC_2.4
GLIBC_2.2.5
ATUSH
```

we can understand that the input is compared with some string by the strcmp function.

Lets see what ltrace command will results !

4. using ltrace command with “strcmp” as a filter, results this:

```
┌──(noa㉿kali)-[~/Desktop]
└─$ ltrace -e strcmp ./layers
Okay, um, Ogres are like onions.
h
layers->strcmp("h\n", "{Sniffs} They stink?\n")
Wrong!
+++ exited (status 255) +++

┌──(noa㉿kali)-[~/Desktop]
└─$
```

first time we encounter the strcmp function compares the input to this string – “{Sniffs} They stink?”, this is the expected string! lets write it as input.

5.

```
┌──(noa㉿kali)-[~/Desktop]
└─$ ltrace -e strcmp ./layers
Okay, um, Ogres are like onions.
{Sniffs} They stink?
layers->strcmp("{Sniffs} They stink?\n", "{Sniffs} They stink?\n")
Yes... No!
yes
layers->strcmp("yes\n", "They make you cry?\n")
Wrong!
+++ exited (status 255) +++
```

After using this strings we found as inputs to the program, we encounter this problem – we can’t see the full line:

```
┌──(noa㉿kali)-[~/Desktop]
└─$ ltrace -e strcmp ./layers
Okay, um, Ogres are like onions.
{Sniffs} They stink?
layers->strcmp("{Sniffs} They stink?\n", "{Sniffs} They stink?\n")                    = 0
Yes... No!
They make you cry?
layers->strcmp("They make you cry?\n", "They make you cry?\n")                        = 0
No! Layers! Onions have layers. Ogres have layers! Onions have layers. You get it? We both have layers.
h
layers->strcmp("h\n", "Oh, you both have layers. You kn"...)                          = 25
Wrong!
+++ exited (status 255) +++
```

But don’t worry! by writing “man ltrace” we found this flag:

```
    -r      Print a relative timestamp with each line of the trace.  This records the time differe

    -s strsize
            Specify the maximum string size to print (the default is 32).
```

So now we can see the full line 😊

```
┌──(noa㉿kali)-[~/Desktop]
└─$ ltrace -e strcmp -s 1000 ./layers
Okay, um, Ogres are like onions.
{Sniffs} They stink?
layers->strcmp("{Sniffs} They stink?\n", "{Sniffs} They stink?\n")                    = 0
Yes... No!
They make you cry?
layers->strcmp("They make you cry?\n", "They make you cry?\n")                        = 0
No! Layers! Onions have layers. Ogres have layers! Onions have layers. You get it? We both have layers.
h
layers->strcmp("h\n", "Oh, you both have layers. You know, not everybody likes onions.\n")   = 25
Wrong!
+++ exited (status 255) +++
```

6. Final stage: (the full conversation)

```
┌──(noa㉿kali)-[~/Desktop]
└─$ ltrace -e strcmp -s 1000 ./layers
Okay, um, Ogres are like onions.
{Sniffs} They stink?
layers->strcmp("{Sniffs} They stink?\n", "{Sniffs} They stink?\n")                    = 0
Yes... No!
They make you cry?
layers->strcmp("They make you cry?\n", "They make you cry?\n")                        = 0
No! Layers! Onions have layers. Ogres have layers! Onions have layers. You get it? We both have layers.
Oh, you both have layers. You know, not everybody likes onions.
layers->strcmp("Oh, you both have layers. You know, not everybody likes onions.\n", "Oh, you both have layers. You know, not everybody likes onions.\n") = 0
You dense, irritating, miniature beast of burden, Ogres are like onions!
Parfaits may be the most delicious thing on the whole damn planet.
layers->strcmp("Parfaits may be the most delicious thing on the whole damn planet.\n", "Parfaits may be the most delicious thing on the whole damn planet.\n") =
You know what is something everybody likes?
Fun with flags
layers->strcmp("Fun with flags\n", "Fun with flags\n")                                = 0
cd22{b1N4ry_l4y3r5_4r3_4nN0y1ng}
+++ exited (status 0) +++
```

And we can see the flag **cd22{b1N4ry_l4y3r5_4r3_4nN0y1ng}**