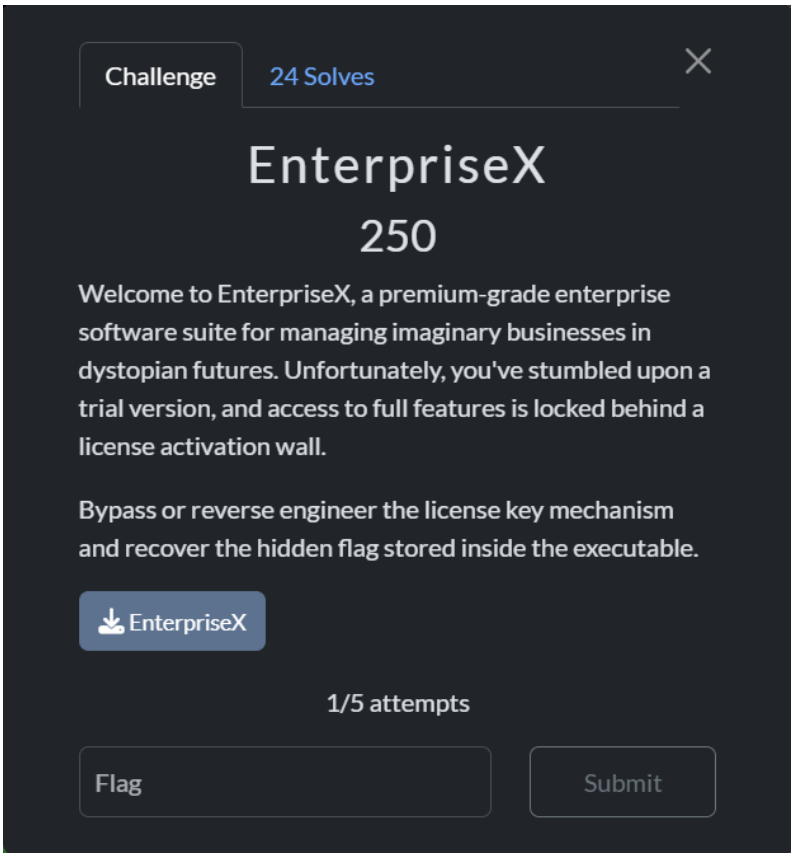
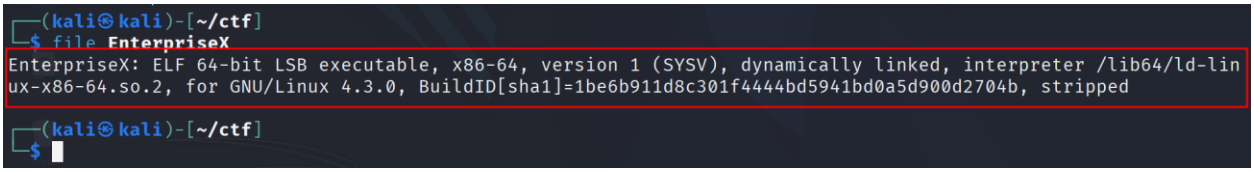
CyberSecureX CTF

Challenge Name: EnterpriseX (250 Points) (Reversing)



After installing the binary file on our local system, we start by running the file command



Now that we know it's a linux file, we can start by executing the file.

```
┌──(kali㉿kali)-[~/ctf]
└─$ ./EnterpriseX
EnterpriseX License Activation
System User Detected: kali
Enter license key: abcd
×  Invalid license key.

┌──(kali㉿kali)-[~/ctf]
└─$
```

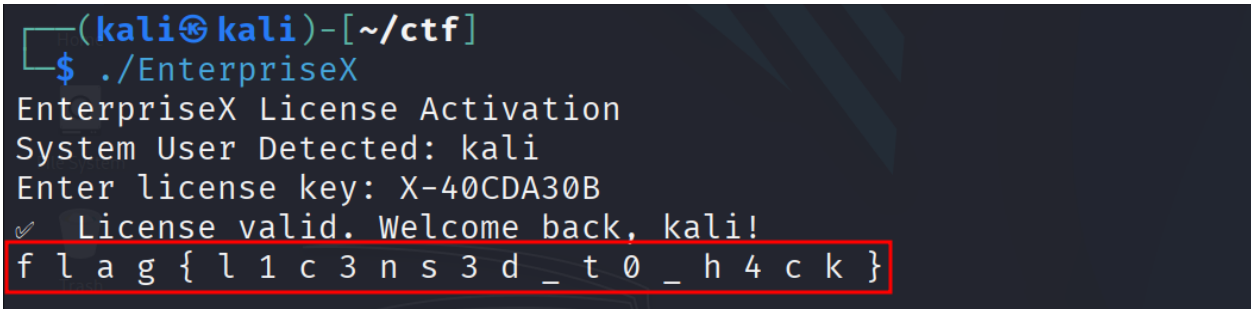
Here I am prompted to enter a 'license key'. I make a guess by entering abcd as input in the license key just to check it, and received an invalid license key reply.

So now we have to find out the license key to get to the flag.

I try using the **ltrace** tool, and to my surprise I found a strcmp function which was comparing my input to a specific string

```
┌──(kali㉿kali)-[~/ctf]
└─$ ltrace ./EnterpriseX
getenv("USER")                                                    = "kali"
puts("EnterpriseX License Activation"EnterpriseX License Activation
)                                 = 31
printf("System User Detected: %s\n", "kali"System User Detected: kali
)                           = 27
printf("Enter license key: ")                                     = 19
fgets(Enter license key: abcd
"abcd\n", 64, 0×7ff2ea7fd8e0)                                 = 0×7ffdd940d770
strcspn("abcd\n", "\n")                                           = 4
strlen("kali")                                                    = 4
sprintf("X-40CDA30B", "X-%08X", 0×40cda30b)                       = 10
strcmp("abcd", "X-40CDA30B")                                      = 9
puts("\342\235\214 Invalid license key."×  Invalid license key.
)                               = 25
+++ exited (status 0) +++
```

Now that we had a value being compared, the next pretty obvious move was to take the value as an input and get the flag.



And that's how we get our flag!

Flag{l1c3ns3d_t0_h4ck}

~ By Team justahacker