CyberSecureX CTF

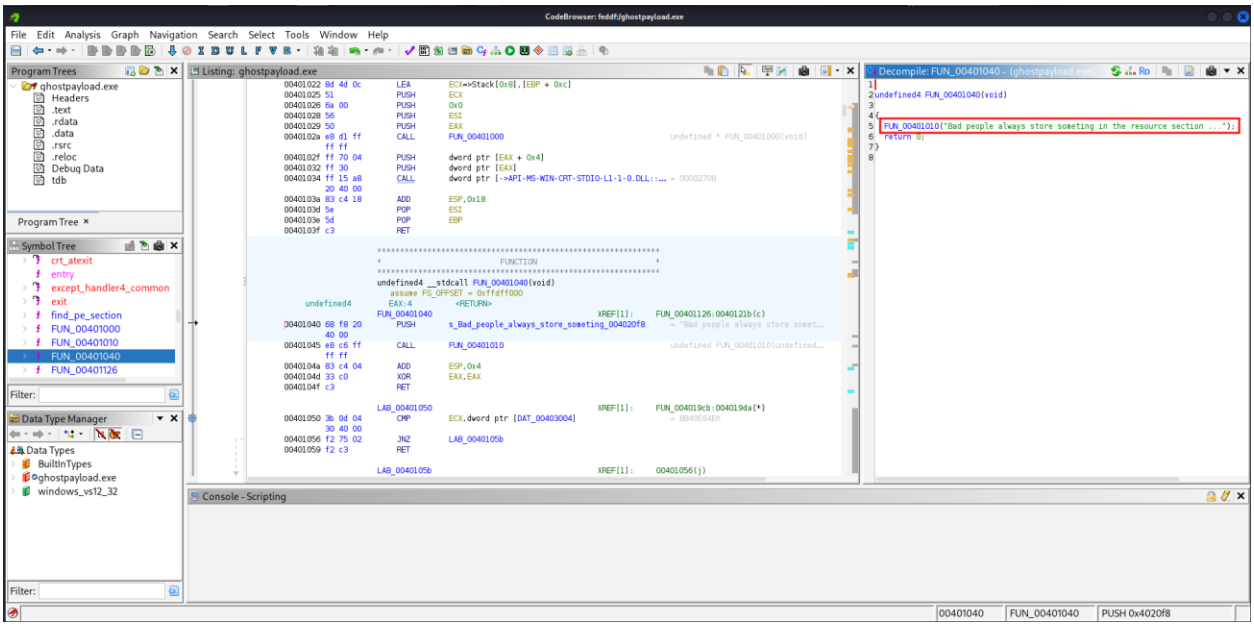
Challenge Name: GhostPayload (100 Points) (Reversing)

GhostPayload was a reversing challenge.

- I started by using the file command on the downloaded .exe file of the challenge.

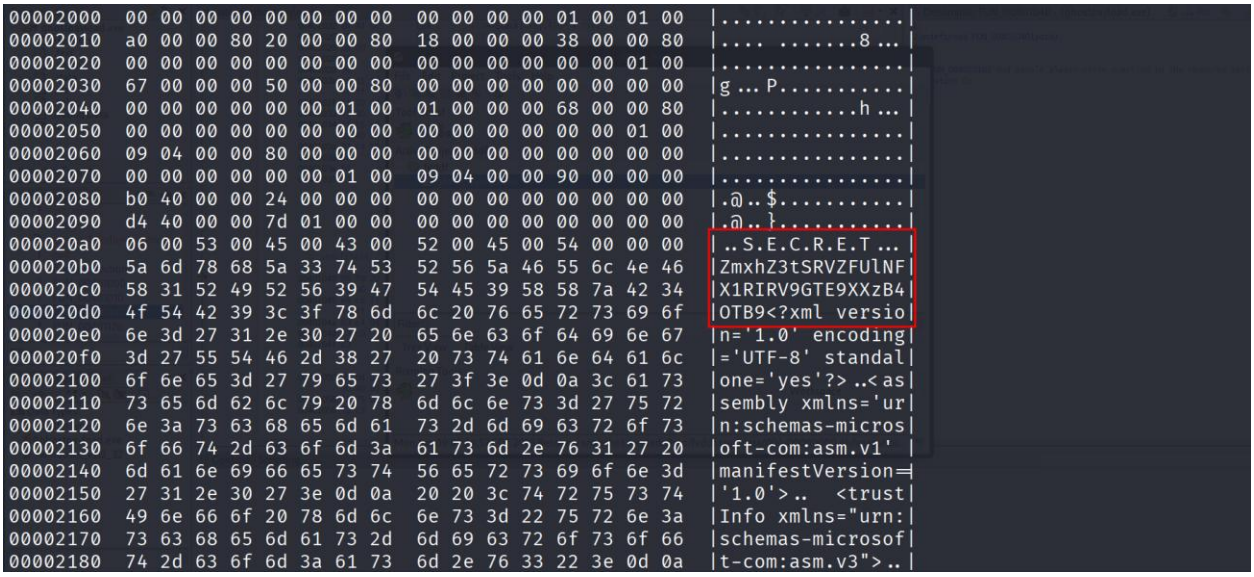
```
┌──(kali㉿kali)-[~/ctf]
└─$ ls
ghostpayload.exe

┌──(kali㉿kali)-[~/ctf]
└─$ file ghostpayload.exe
ghostpayload.exe: PE32 executable for MS Windows 6.00 (console), Intel i386, 5 sections

┌──(kali㉿kali)-[~/ctf]
└─$
```

After receiving this message, I thought of running the .exe file through **ghidra** tool

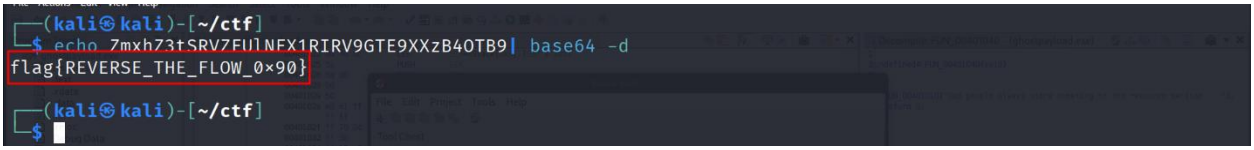


Here in the ghidra console we come across an interesting message. The highlighted text reads “Bad people always store someting in the resource section ...”

This motivated me to use the **hexdump** tool to extract hex data of the .exe file, where we found a ‘SECRET’ message.



Here we can see some text similar to a base64 encoded string, so I decode the string to get the flag



And there! We have the flag for the challenge

Flag{REVERSE_THE_FLOW_0x90}

~ By Team justahacker