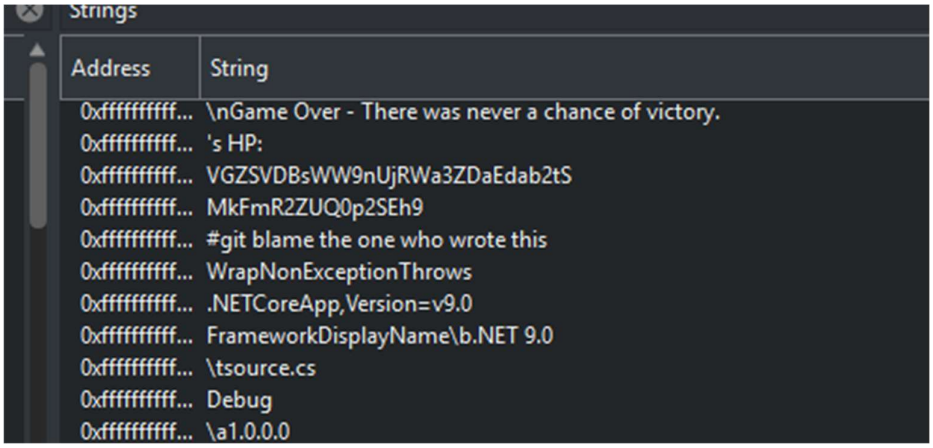
BOSSMAN

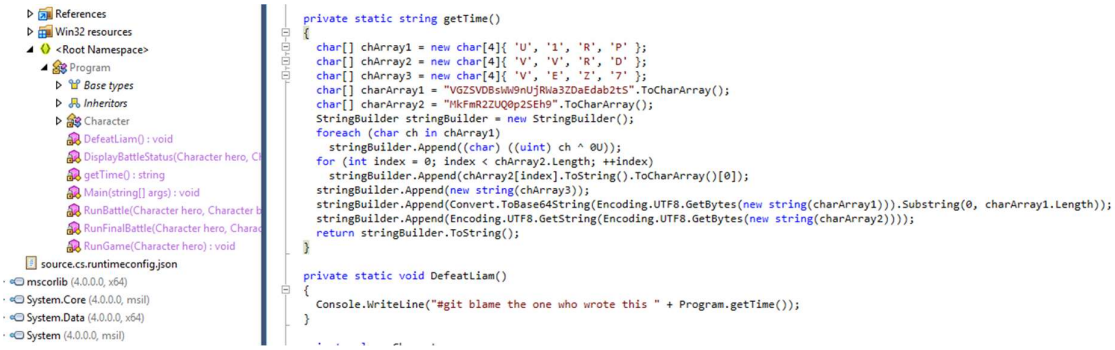
Description:

Null

While trying to analyze the program in DNSpy, I couldn't find anything useful. I then booted up Cutter and encountered some Base64 encoded data. Since I couldn't see the program properly in either DNSpy or ILSpy, I decided to explore alternative tools.



After trying dotPeek, a tool designed for .NET Framework programs, I was able to view the source code clearly. This allowed me to decode the data and eventually obtain the flag.



Script

```
import base64

def get_time():
    ch_array1 = ['U', '1', 'R', 'P']
    ch_array2 = ['V', 'V', 'R', 'D']
    ch_array3 = ['V', 'E', 'Z', '7']
    char_array1 = "VGZSVDBsWW9nUjRWa3ZDaEdab2tS"
    char_array2 = "MkFmR2ZUQ0p2SEh9"

    string_builder = []

    string_builder.extend(ch_array1)
    string_builder.extend(ch_array2)
    string_builder.extend(ch_array3)

    base64_encoded_char_array1 = base64.b64encode(char_array1.encode('utf-
8')).decode('utf-8')
    string_builder.append(base64_encoded_char_array1[:len(char_array1)])

    string_builder.append(char_array2)

    return ''.join(string_builder)

result = get_time()
print(result)
```

```
┌──(osiris㉿ALICE)-[~/Downloads/CTF/STOUTCTF/rev/bossman]
└─$ python solver.py
U1RPVVRDVEZ7VkdaU1ZEQnNXVzluVWpSV2EzWkRhMkFmR2ZUQ0p2SEh9

┌──(osiris㉿ALICE)-[~/Downloads/CTF/STOUTCTF/rev/bossman]
└─$ python solver.py | base64 -d
STOUTCTF{VGZSVDBsWW9nUjRWa3ZDa2AfGfTCJvHH}
┌──(osiris㉿ALICE)-[~/Downloads/CTF/STOUTCTF/rev/bossman]
└─$
```

Flag	STOUTCTF{VGZSVDBsWW9nUjRWa3ZDa2AfGfTCJvHH}