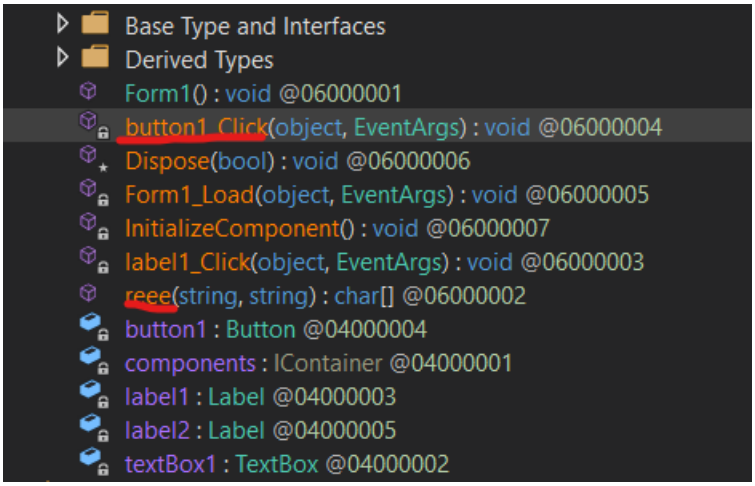
After decompiling with IDA and seeing basically nothing, I was a bit confused.

```
┌──(kali㉿kali)-[/tmp/VMwareDnD/U5EvM8]
└─$ file this_is_wendys.exe
this_is_wendys.exe: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS
Windows, 3 sections
```

Most decompilers won't help as we are dealing with a .NET application. In these situations, we need to use dnspy: https://github.com/dnSpy/dnSpy



After looking through the main functions I concluded those 2 are the most important ones as they process the password.

We conclude we need to perform a cyclical xor between the predefined UTF16 string "a" and an OS environment variable. ChatGPT suggests it might me "Windows_NT"

```python
import codecs
a = 
"4\u001d\b\u001f\fDKk3\\\b\0\r\u0013\u0011neYV\a\nN\u0017:d\r\\RWFFofX^\a\u000eEK
m3Z\rV[\u0011F>5\u000fX\0Z\u0014Ehd_\b\0\r\u0015Dfd\b\fQ\u0012"
decoded_a = codecs.decode(a, 'unicode_escape')
b = "Windows_NT"
result = []
for i in range(len(a)):
    xor_result = chr(ord(a[i]) ^ ord(b[i%8]))
    result.append(xor_result)
print(''.join(result))
```

As a result, this little script prints out the password… which is also the flag!

Made with love by: AndreiCat