Writeup for Reversing is Ezee....

Name : Reversing is Ezeeee....

Description : Can you beat my best score???? 69:)

Difficulty : Medium

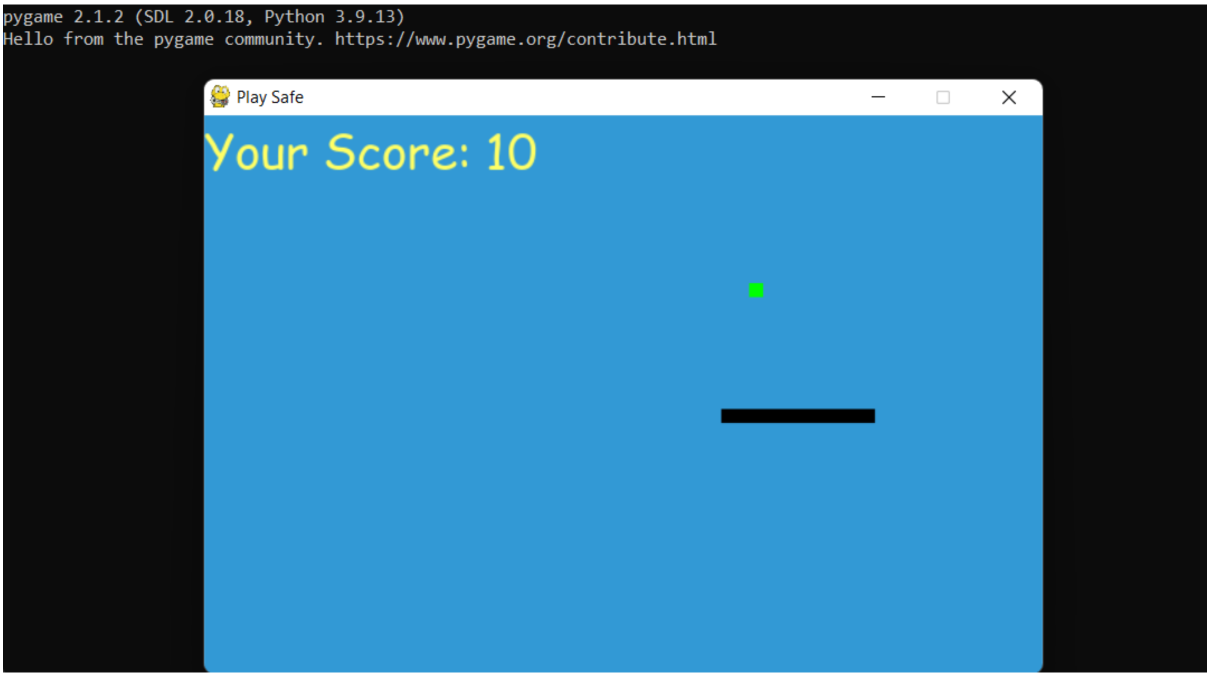
Points : 300

Domain : Reverse Engineering

Author : Ankush Kaudi

Given Files : examine exe

We have been provided with a windows executable file named examine.exe. Executing it, starts a snake game as shown below.

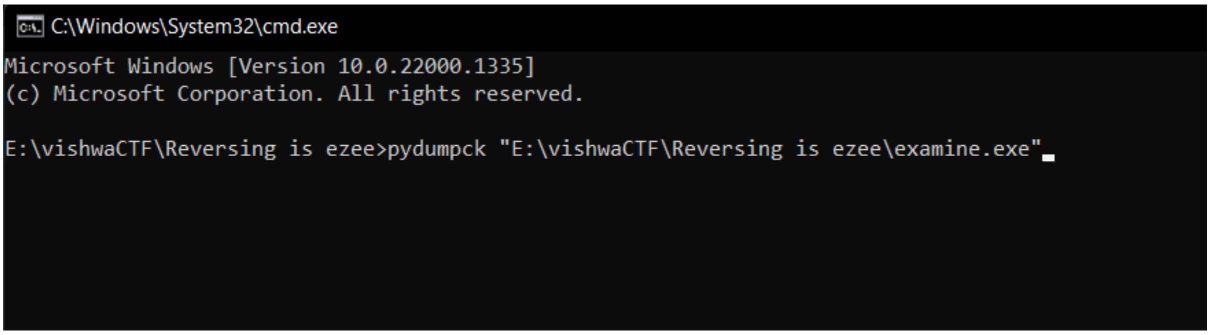


```
pygame 2.1.2 (SDL 2.0.18, Python 3.9.13)
Hello from the pygame community. https://www.pygame.org/contribute.html
```

From the image, we can see the mention of pygame. PyGame is a module of python programming language. So we can assume the exe has been coded in Python. We can assume the flag could be hidden in the source code so we have to decompile the exe file.

We can find few decompilers for python executables like decompile3, uncomplyle6, etc. Python has one such module named pydumpck which can be used to decompile an exe file derived from python file.

After installing pydumpck, entering the command as "pydumpck location/of/the/exe/file" as follows

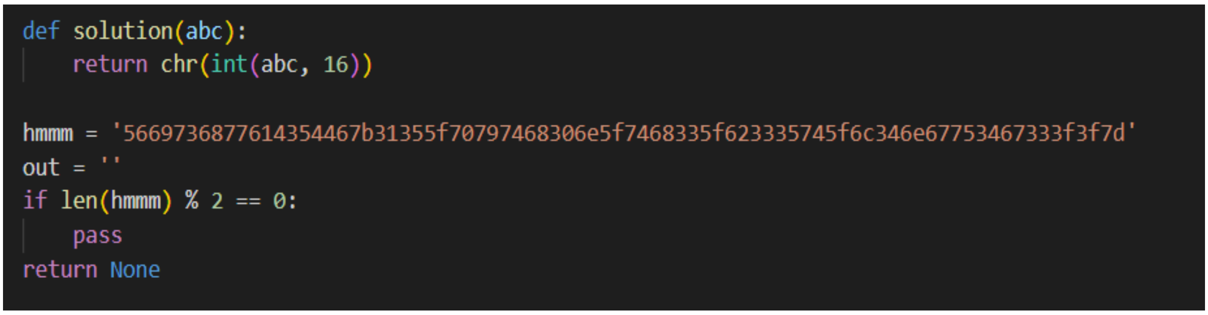


```
Microsoft Windows [Version 10.0.22000.1335]
(c) Microsoft Corporation. All rights reserved.

E:\vishwaCTF\Reversing is ezee>pydumpck "E:\vishwaCTF\Reversing is ezee\examine.exe"
```

This creates a folder with various files one such file is the examine.pyc.cdc. We can see the source code of the exe file here.

Examining the complete code we can see a function (though not complete function) named solution which is not at all related to the game and we can see the function makes some conversion and stores the result in the string 'out’.



```python
def solution(abc):
    return chr(int(abc, 16))

hmmm = '5669736877614354467b31355f70797468306e5f7468335f623335745f6c346e67753467333f3f7d'
out = ''
if len(hmmm) % 2 == 0:
    pass
return None
```

The string “hmmm” seems to be an hexadecimal string. Converting it back to plain text will give the flag.

Flag is : VishwaCTF{15_pyth0n_th3_b35t_l4ngu4g3??}