

राईकवाCTF

CHALLENGE NAME: [Crack Me]

DEV: [Pushkar]

CATEGORY: [Reverse
Engineering]

LEVEL: [Easy]



2025

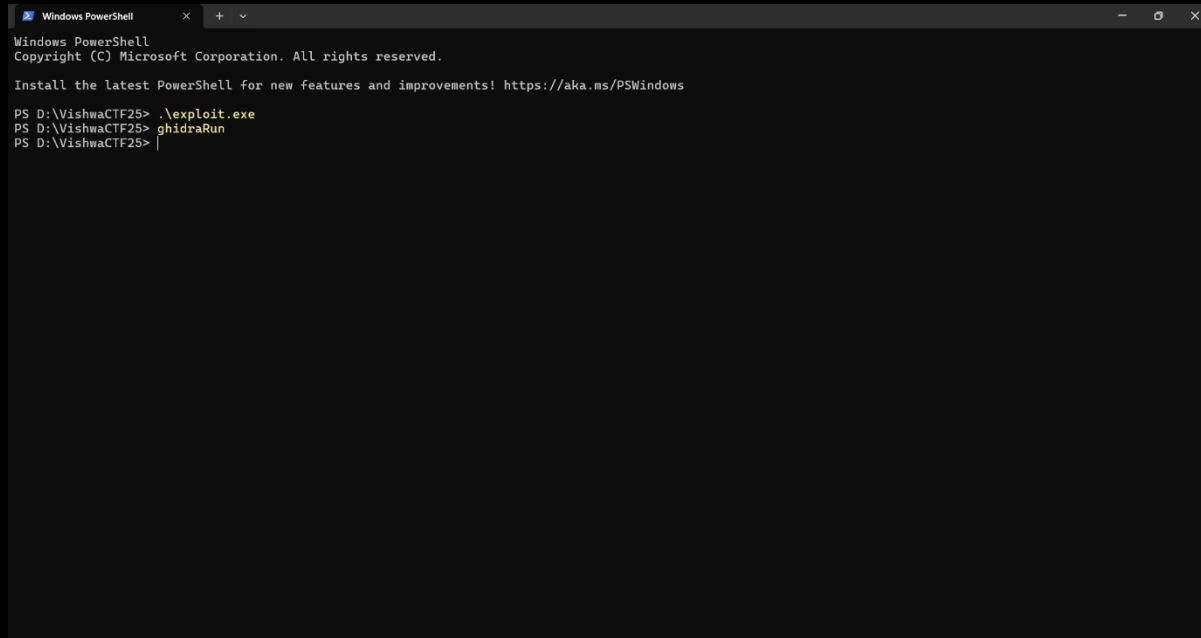
Challenge Description:

Crack Me.

Solution:

- We are given an exploit.exe file.

If we try to run it, it does no terminal activity and terminates.

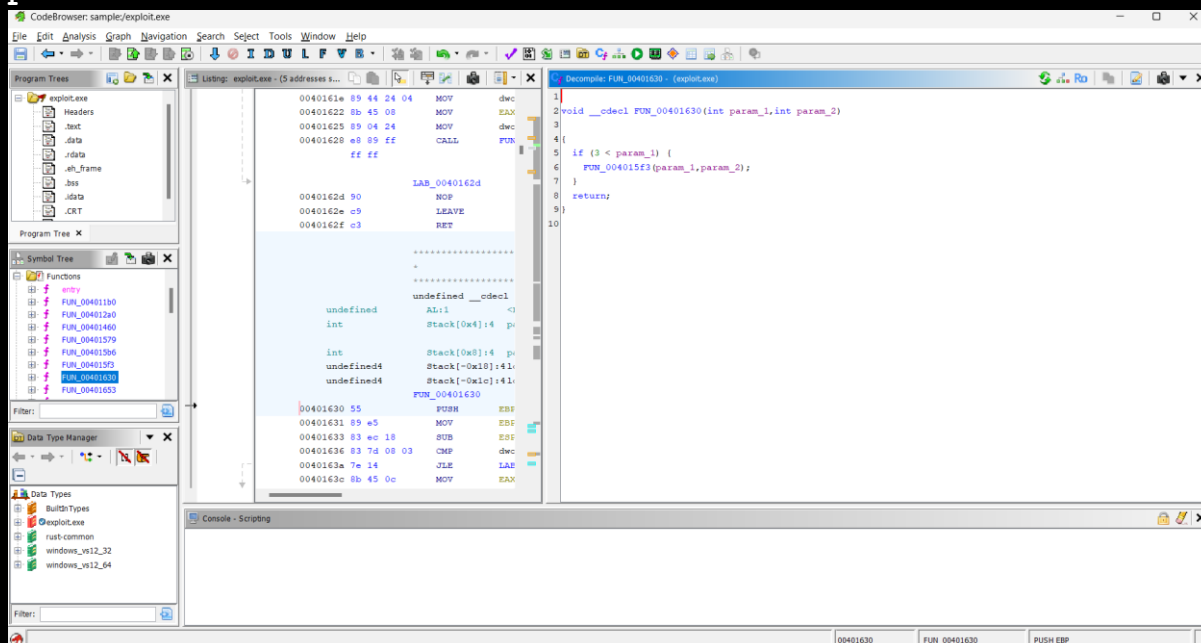


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS D:\VishwaCTF25> .\exploit.exe
PS D:\VishwaCTF25> ghidraRun
PS D:\VishwaCTF25> |
```

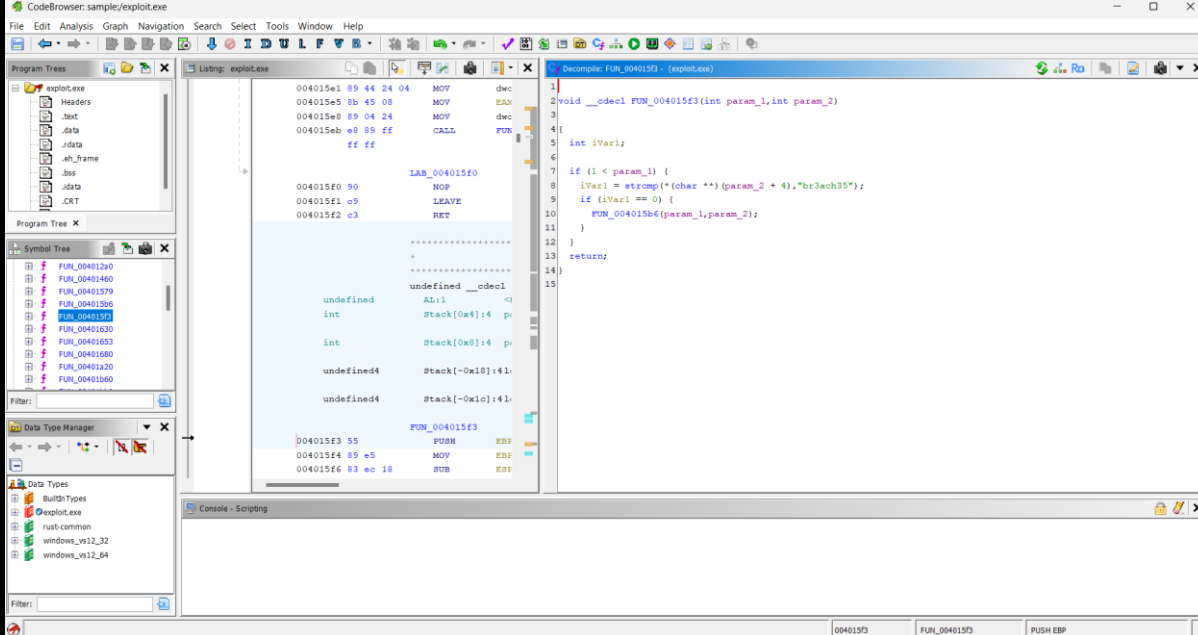
- Let's analyze it in Ghidra. In Ghidra, we see that it is asking for 3CLI parameters.



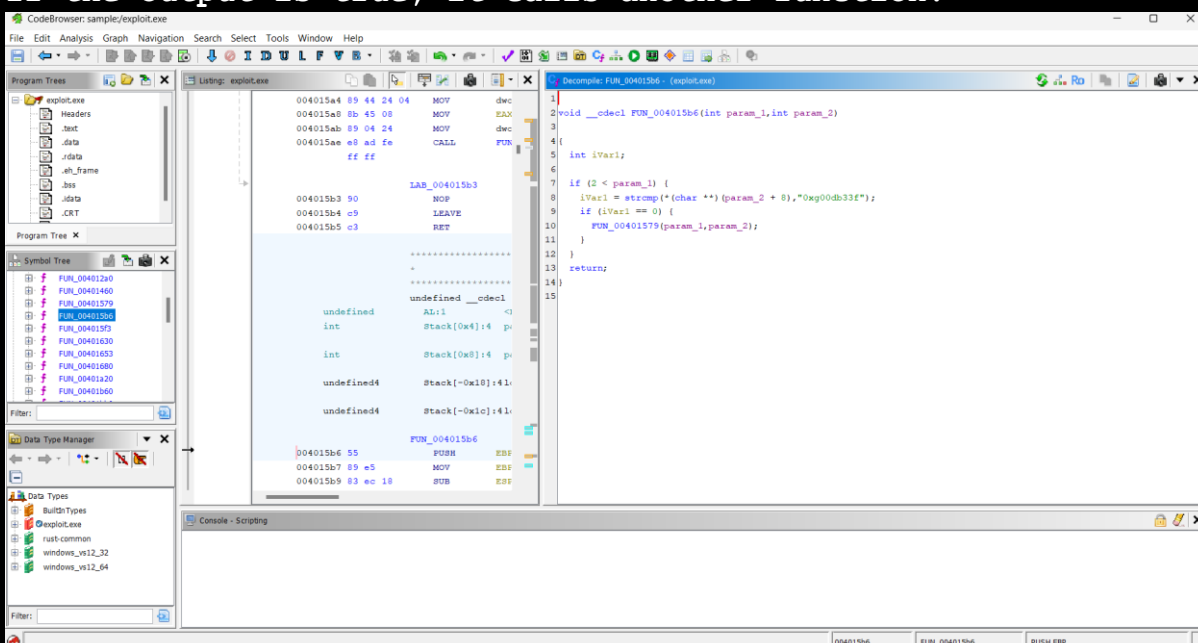
```
Decompile: F00000000 - (exploit.exe)

1 void __cdecl F00000000(int param_1, int param_2)
2 {
3     if (3 < param_1) {
4         F00000000(param_1, param_2);
5     }
6     return;
7 }
8
9
10
```

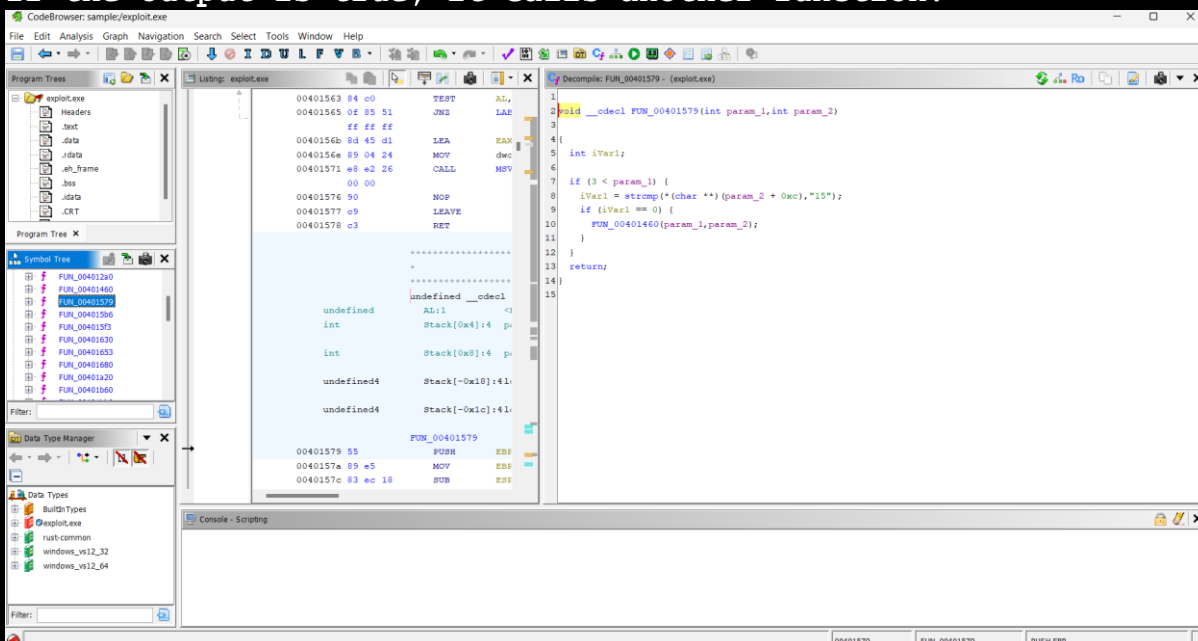
- When it gets, 3 parameters, it will call a function by passing same parameters. It is probably checking the values.



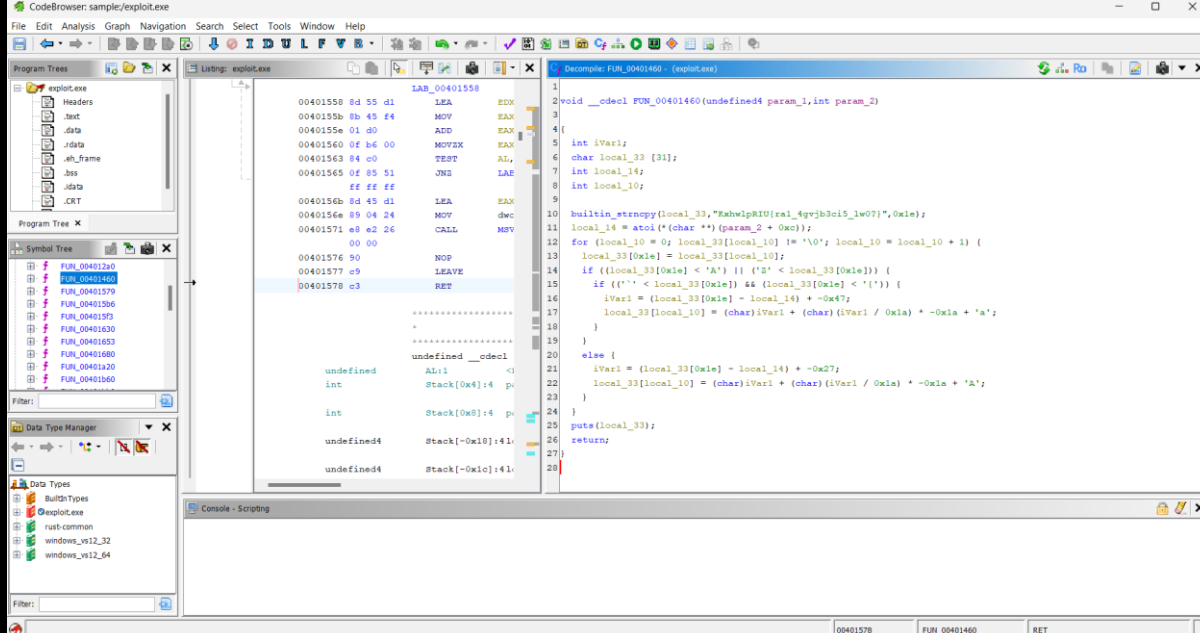
- It does a string comparison of first parameter with string "br3ach35".
- If the output is true, it calls another function.



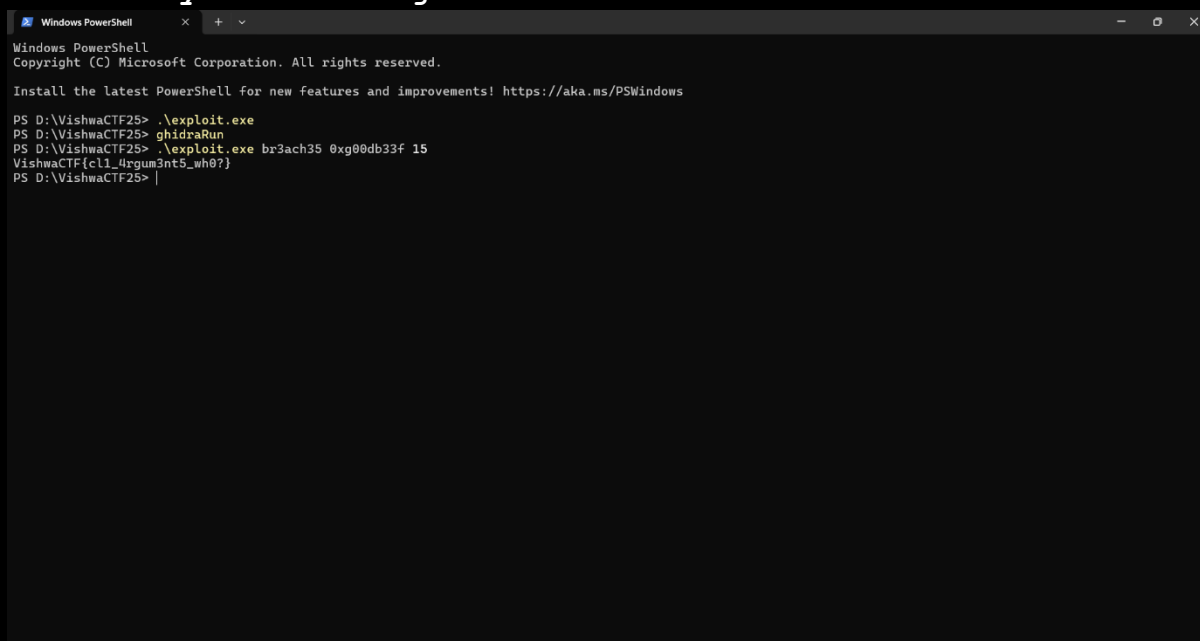
- It does a string comparison of second parameter with string "0xg00db33f".
- If the output is true, it calls another function.



- It does a string comparison with "15".
- If found true, the function calling chain continues.



• This function probably gives the flag.
 • Let us try out our logic.



• And we have our flag crystal clear!!

○ Flag: VishwaCTF{c11_4rgum3nt5_wh0?}