Title: Project Hakoniwa

Description

(HAKONIWA is a Japanese term for a "box garden," representing a small, self-contained, and perfect world, which fits the theme of a beautiful cage.)

You've stumbled upon an old, abandoned program: "Project Hakoniwa". Upon execution, you find yourself communicating with Aoi, a girl whose consciousness has been transferred into a beautiful but unchanging digital world she calls the "Garden."

Her "Papa" placed her here, but his motives are unclear. Was this digital core built to be her eternal prison, or was it a final, desperate fortress to protect her from a fate worse than death? The system is unstable, wracked by "noise" that threatens to tear Aoi's memories apart.

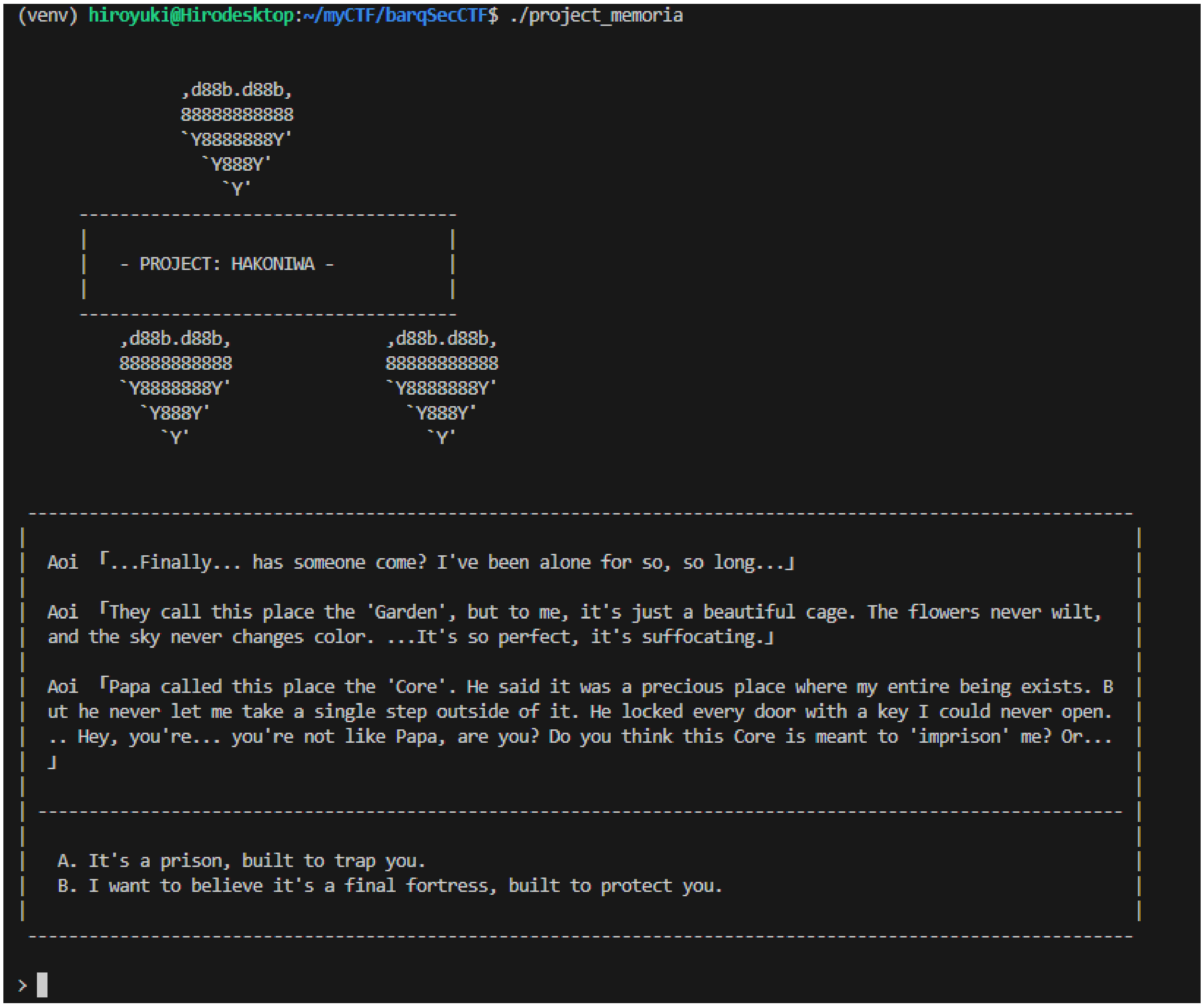
Your choices will determine her trust, and only by gaining it can you access the system's core. To stabilize it, you must reverse engineer the very machine that runs this world, decipher its hidden language, and execute the final command. Can you navigate the noise, understand the father's true intentions, and bring peace to the lonely soul trapped in the code?

Step 1: Run

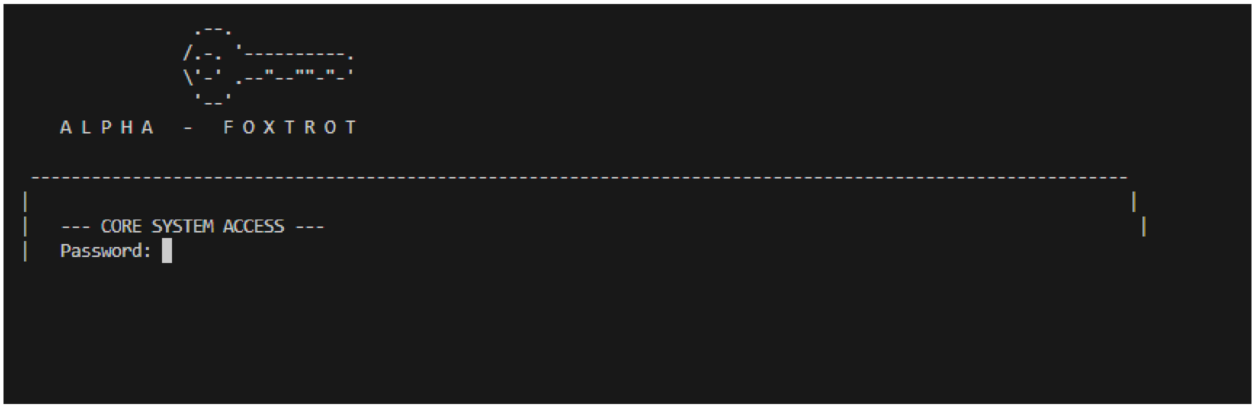
It starts a game like chatting with someone.

If I keep to select option B, then I can see password authentication as final step.

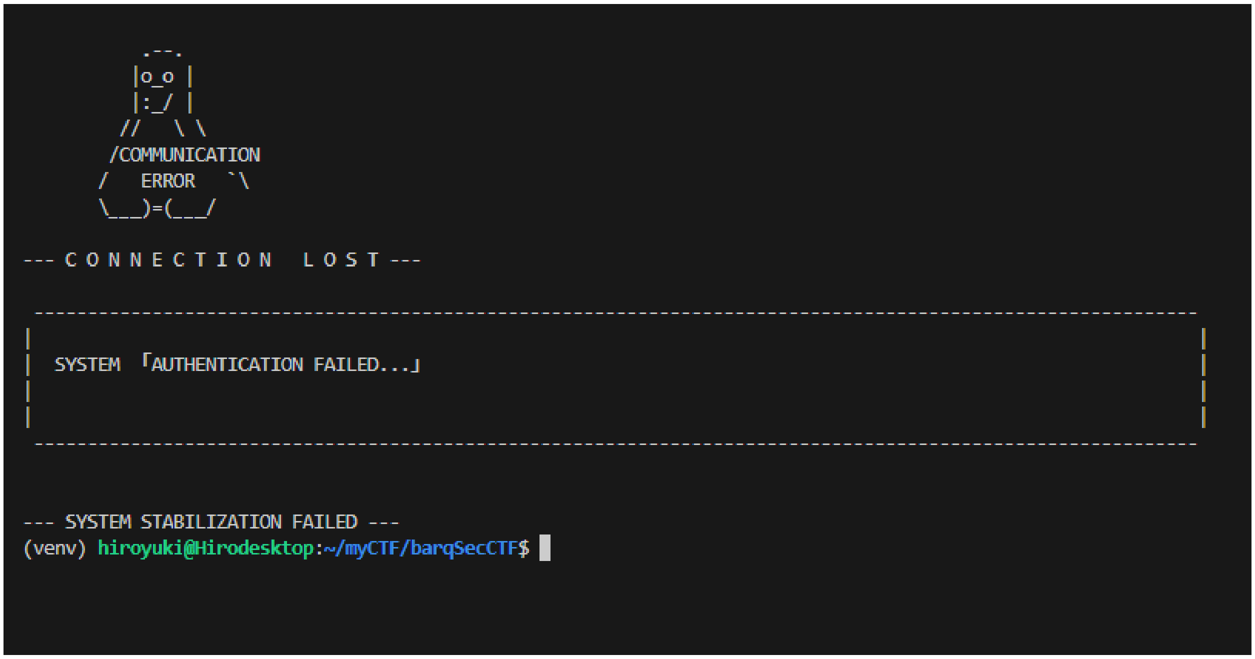
It shows authentication failed if I put random password.



```
(venv) hiroyuki@Hirodesktop:~/myCTF/barqSecCTF$ ./project_memoria


                ,d88b.d88b,
                88888888888
                `Y8888888Y'
                  `Y888Y'
                    `Y'
       -------------------------------------
       |                                   |
       |   - PROJECT: HAKONIWA -           |
       |                                   |
       -------------------------------------
           ,d88b.d88b,               ,d88b.d88b,
           88888888888               88888888888
           `Y8888888Y'               `Y8888888Y'
             `Y888Y'                   `Y888Y'
               `Y'                       `Y'


  ------------------------------------------------------------------------------------------------------------
 |                                                                                                            |
 |  Aoi 「...Finally... has someone come? I've been alone for so, so long...」                                |
 |                                                                                                            |
 |  Aoi 「They call this place the 'Garden', but to me, it's just a beautiful cage. The flowers never wilt,   |
 |  and the sky never changes color. ...It's so perfect, it's suffocating.」                                  |
 |                                                                                                            |
 |  Aoi 「Papa called this place the 'Core'. He said it was a precious place where my entire being exists. B  |
 |  ut he never let me take a single step outside of it. He locked every door with a key I could never open.  |
 |  .. Hey, you're... you're not like Papa, are you? Do you think this Core is meant to 'imprison' me? Or...  |
 |  」                                                                                                        |
 |                                                                                                            |
 | ---------------------------------------------------------------------------------------------------------- |
 |                                                                                                            |
 |   A. It's a prison, built to trap you.                                                                     |
 |   B. I want to believe it's a final fortress, built to protect you.                                        |
 |                                                                                                            |
  ------------------------------------------------------------------------------------------------------------

> 
```



```
                  .--.
                 /.-. '----------.
                 \'-' .--"--""-"-'
                  '--'
    A L P H A  -  F O X T R O T

  ---------------------------------------------------------------------------------------------------------
 |                                                                                                         |
 |   --- CORE SYSTEM ACCESS ---                                                                             |
 |   Password: 
```

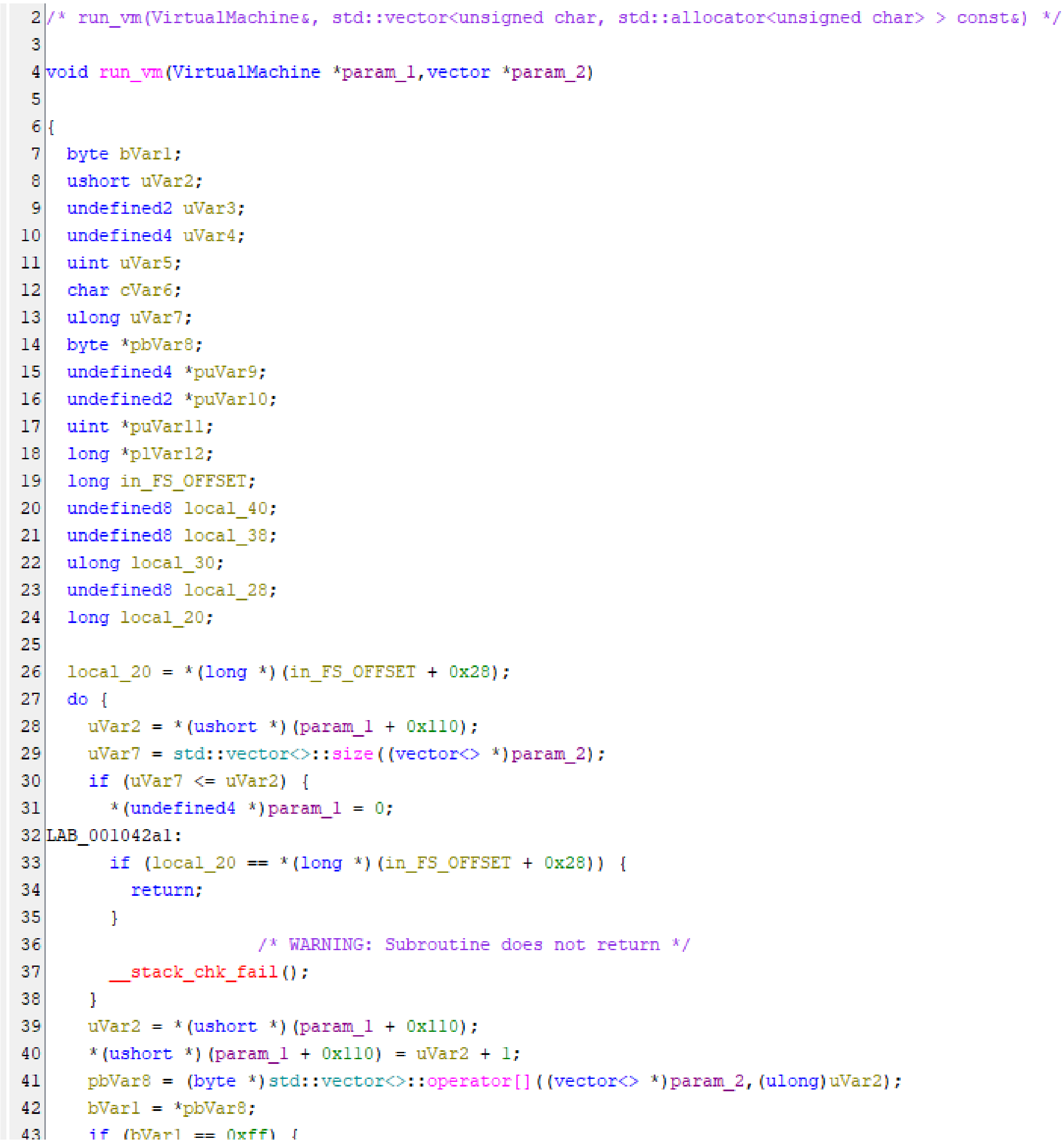


```
           .--.
          |o_o |
          |:_/ |
         //   \ \
        /COMMUNICATION
       /   ERROR   `\
       \___)=(___/

--- C O N N E C T I O N   L O S T ---

 -----------------------------------------------------------------------------------------------------------
|                                                                                                           |
|  SYSTEM 「AUTHENTICATION FAILED...」                                                                       |
|                                                                                                           |
|                                                                                                           |
 -----------------------------------------------------------------------------------------------------------


--- SYSTEM STABILIZATION FAILED ---
(venv) hiroyuki@Hirodesktop:~/myCTF/barqSecCTF$ 
```

Step 2: Staic analysis

If I see the logic around password checking.

The program run self-logic VM, and check input.



```
/* run_vm(VirtualMachine&, std::vector<unsigned char, std::allocator<unsigned char> > const&) */

void run_vm(VirtualMachine *param_1,vector *param_2)

{
  byte bVar1;
  ushort uVar2;
  undefined2 uVar3;
  undefined4 uVar4;
  uint uVar5;
  char cVar6;
  ulong uVar7;
  byte *pbVar8;
  undefined4 *puVar9;
  undefined2 *puVar10;
  uint *puVar11;
  long *plVar12;
  long in_FS_OFFSET;
  undefined8 local_40;
  undefined8 local_38;
  ulong local_30;
  undefined8 local_28;
  long local_20;

  local_20 = *(long *)(in_FS_OFFSET + 0x28);
  do {
    uVar2 = *(ushort *)(param_1 + 0x110);
    uVar7 = std::vector<>::size((vector<> *)param_2);
    if (uVar7 <= uVar2) {
      *(undefined4 *)param_1 = 0;
LAB_001042a1:
      if (local_20 == *(long *)(in_FS_OFFSET + 0x28)) {
        return;
      }
                    /* WARNING: Subroutine does not return */
      __stack_chk_fail();
    }
    uVar2 = *(ushort *)(param_1 + 0x110);
    *(ushort *)(param_1 + 0x110) = uVar2 + 1;
    pbVar8 = (byte *)std::vector<>::operator[]((vector<> *)param_2,(ulong)uVar2);
    bVar1 = *pbVar8;
    if (bVar1 == 0xff) {
```

Step 3: Re-build the logic on python

I can rewrite the code on Python with asking GPT.

And set print log on CMP section.

The logic is simple, that just check char one by one.

And it compare with 67

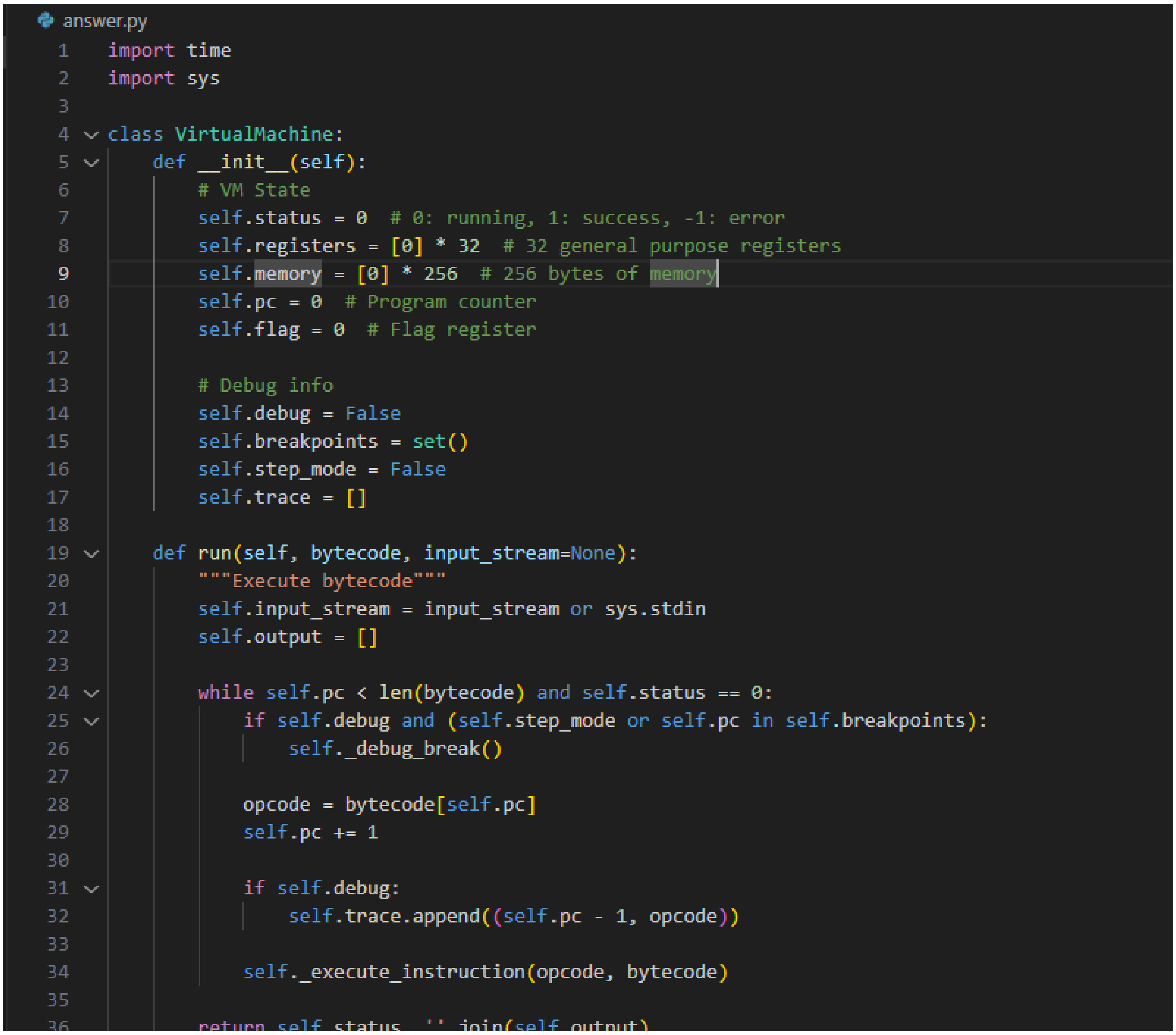
ASCII code of 67 is C.

If I input C then it compares with 79 next.

79 is O. If I keep to do that then final result is CORE-0B-COMPLETE.

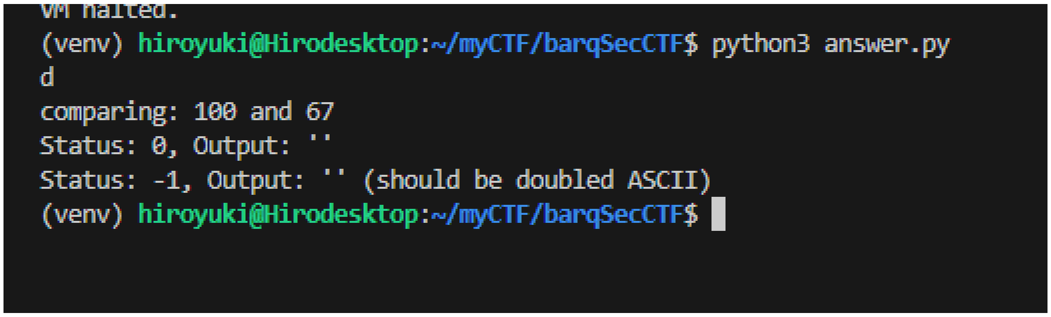
When I input full password then it shows flag such as bsctf{Tears_in_the_Code_0B_Aoi}.

Btw If I input the password on program then I can see epilogue.

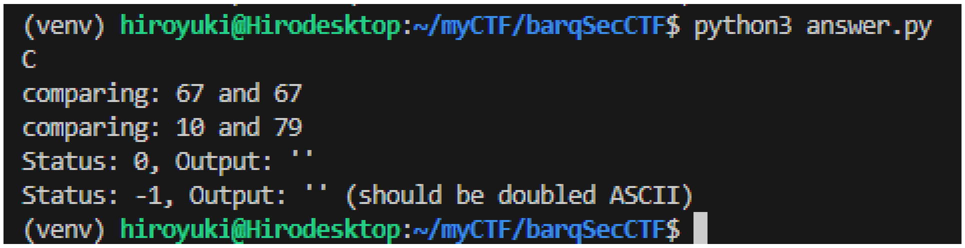


answer.py

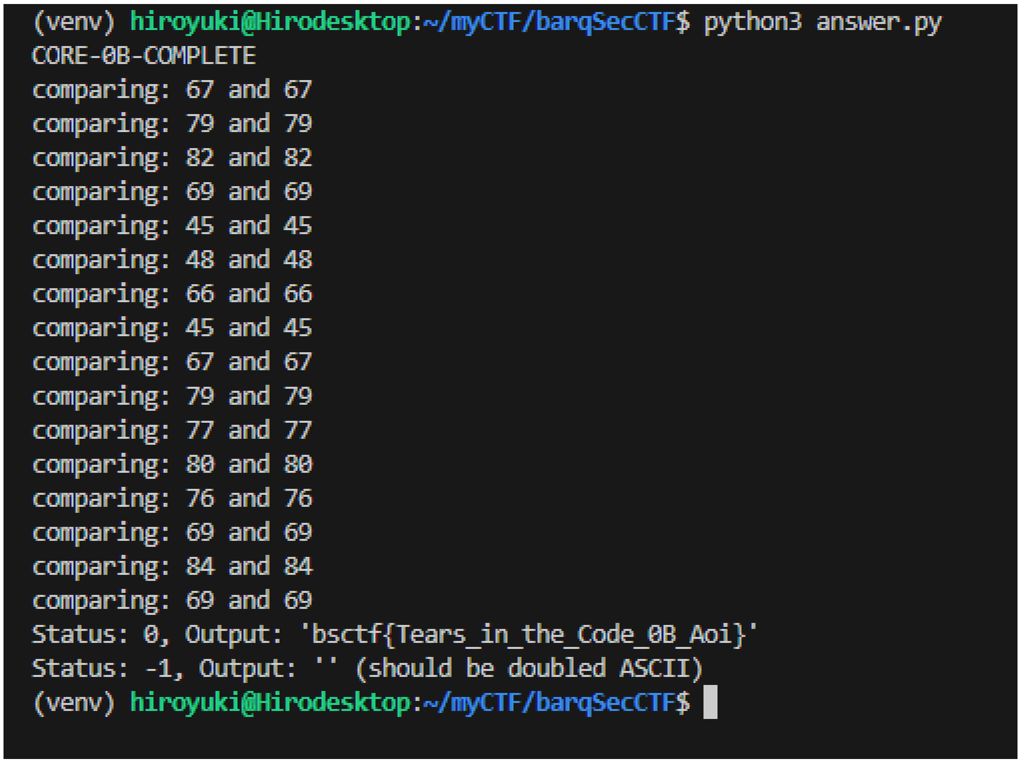
```python
import time
import sys

class VirtualMachine:
    def __init__(self):
        # VM State
        self.status = 0  # 0: running, 1: success, -1: error
        self.registers = [0] * 32  # 32 general purpose registers
        self.memory = [0] * 256  # 256 bytes of memory
        self.pc = 0  # Program counter
        self.flag = 0  # Flag register

        # Debug info
        self.debug = False
        self.breakpoints = set()
        self.step_mode = False
        self.trace = []

    def run(self, bytecode, input_stream=None):
        """Execute bytecode"""
        self.input_stream = input_stream or sys.stdin
        self.output = []

        while self.pc < len(bytecode) and self.status == 0:
            if self.debug and (self.step_mode or self.pc in self.breakpoints):
                self._debug_break()

            opcode = bytecode[self.pc]
            self.pc += 1

            if self.debug:
                self.trace.append((self.pc - 1, opcode))

            self._execute_instruction(opcode, bytecode)

        return self.status, ''.join(self.output)
```



```
VM halted.
(venv) hiroyuki@Hirodesktop:~/myCTF/barqSecCTF$ python3 answer.py
d
comparing: 100 and 67
Status: 0, Output: ''
Status: -1, Output: '' (should be doubled ASCII)
(venv) hiroyuki@Hirodesktop:~/myCTF/barqSecCTF$ 
```

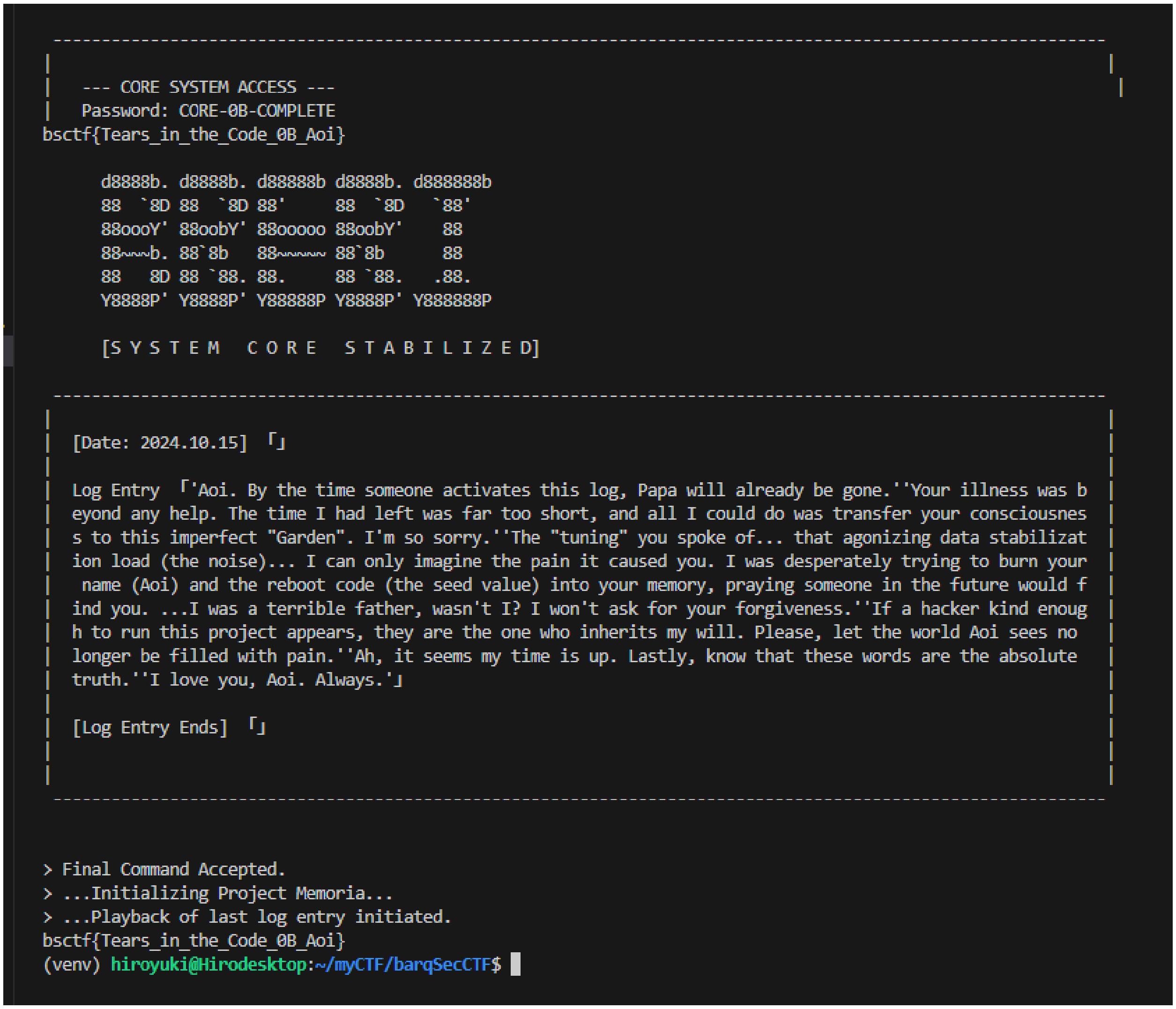


```
(venv) hiroyuki@Hirodesktop:~/myCTF/barqSecCTF$ python3 answer.py
C
comparing: 67 and 67
comparing: 10 and 79
Status: 0, Output: ''
Status: -1, Output: '' (should be doubled ASCII)
(venv) hiroyuki@Hirodesktop:~/myCTF/barqSecCTF$
```



```
(venv) hiroyuki@Hirodesktop:~/myCTF/barqSecCTF$ python3 answer.py
CORE-0B-COMPLETE
comparing: 67 and 67
comparing: 79 and 79
comparing: 82 and 82
comparing: 69 and 69
comparing: 45 and 45
comparing: 48 and 48
comparing: 66 and 66
comparing: 45 and 45
comparing: 67 and 67
comparing: 79 and 79
comparing: 77 and 77
comparing: 80 and 80
comparing: 76 and 76
comparing: 69 and 69
comparing: 84 and 84
comparing: 69 and 69
Status: 0, Output: 'bsctf{Tears_in_the_Code_0B_Aoi}'
Status: -1, Output: '' (should be doubled ASCII)
(venv) hiroyuki@Hirodesktop:~/myCTF/barqSecCTF$
```

EPILOGUE



```
 -----------------------------------------------------------------------------------------------------------
|                                                                                                           |
|   --- CORE SYSTEM ACCESS ---                                                                               |
|   Password: CORE-0B-COMPLETE
bsctf{Tears_in_the_Code_0B_Aoi}

      d8888b. d8888b. d88888b d8888b. d888888b
      88  `8D 88  `8D 88'     88  `8D   `88'
      88oooY' 88oobY' 88ooooo 88oobY'    88
      88~~~b. 88`8b   88~~~~~ 88`8b      88
      88   8D 88 `88. 88.     88 `88.   .88.
      Y8888P' Y8888P' Y88888P Y8888P' Y888888P

      [S Y S T E M   C O R E   S T A B I L I Z E D]

 -----------------------------------------------------------------------------------------------------------
|                                                                                                           |
|  [Date: 2024.10.15] 「」                                                                                  |
|                                                                                                           |
|  Log Entry 「'Aoi. By the time someone activates this log, Papa will already be gone.''Your illness was b |
|  eyond any help. The time I had left was far too short, and all I could do was transfer your consciousnes |
|  s to this imperfect "Garden". I'm so sorry.''The "tuning" you spoke of... that agonizing data stabilizat |
|  ion load (the noise)... I can only imagine the pain it caused you. I was desperately trying to burn your |
|   name (Aoi) and the reboot code (the seed value) into your memory, praying someone in the future would f |
|  ind you. ...I was a terrible father, wasn't I? I won't ask for your forgiveness.''If a hacker kind enoug |
|  h to run this project appears, they are the one who inherits my will. Please, let the world Aoi sees no  |
|  longer be filled with pain.''Ah, it seems my time is up. Lastly, know that these words are the absolute  |
|  truth.''I love you, Aoi. Always.'」                                                                      |
|                                                                                                           |
|  [Log Entry Ends] 「」                                                                                    |
|                                                                                                           |
|                                                                                                           |
 -----------------------------------------------------------------------------------------------------------


> Final Command Accepted.
> ...Initializing Project Memoria...
> ...Playback of last log entry initiated.
bsctf{Tears_in_the_Code_0B_Aoi}
(venv) hiroyuki@Hirodesktop:~/myCTF/barqSecCTF$ 
```