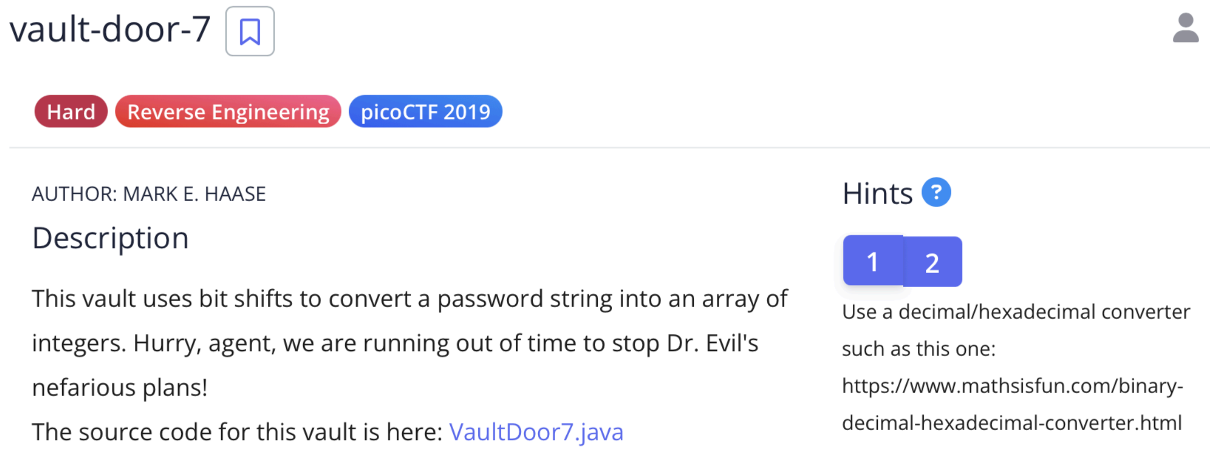


vault-door-7

Hard Reverse Engineering picoCTF 2019

AUTHOR: MARK E. HAASE

Description

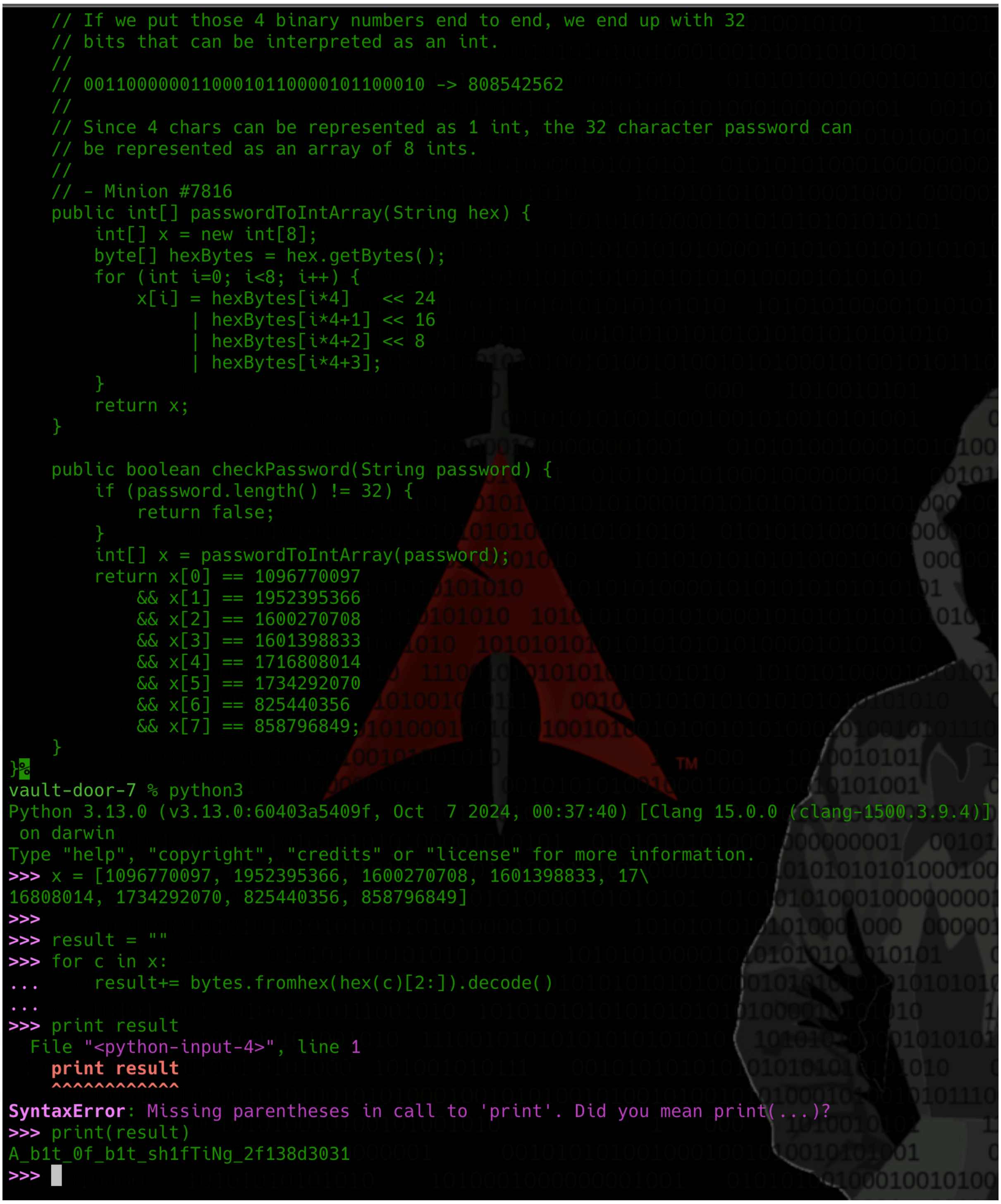
This vault uses bit shifts to convert a password string into an array of integers. Hurry, agent, we are running out of time to stop Dr. Evil's nefarious plans!

The source code for this vault is here: VaultDoor7.java

Hints

Use a decimal/hexadecimal converter such as this one: https://www.mathsisfun.com/binary-decimal-hexadecimal-converter.html

Solver :



```
    // If we put those 4 binary numbers end to end, we end up with 32
    // bits that can be interpreted as an int.
    //
    // 00110000001100010110000101100010 -> 808542562
    //
    // Since 4 chars can be represented as 1 int, the 32 character password can
    // be represented as an array of 8 ints.
    //
    // - Minion #7816
    public int[] passwordToIntArray(String hex) {
        int[] x = new int[8];
        byte[] hexBytes = hex.getBytes();
        for (int i=0; i<8; i++) {
            x[i] = hexBytes[i*4]   << 24
                 | hexBytes[i*4+1] << 16
                 | hexBytes[i*4+2] << 8
                 | hexBytes[i*4+3];
        }
        return x;
    }

    public boolean checkPassword(String password) {
        if (password.length() != 32) {
            return false;
        }
        int[] x = passwordToIntArray(password);
        return x[0] == 1096770097
            && x[1] == 1952395366
            && x[2] == 1600270708
            && x[3] == 1601398833
            && x[4] == 1716808014
            && x[5] == 1734292070
            && x[6] == 825440356
            && x[7] == 858796849;
    }
}%
vault-door-7 % python3
Python 3.13.0 (v3.13.0:60403a5409f, Oct  7 2024, 00:37:40) [Clang 15.0.0 (clang-1500.3.9.4)]
 on darwin
Type "help", "copyright", "credits" or "license" for more information.
>>> x = [1096770097, 1952395366, 1600270708, 1601398833, 17\
16808014, 1734292070, 825440356, 858796849]
>>>
>>> result = ""
>>> for c in x:
...     result+= bytes.fromhex(hex(c)[2:]).decode()
...
>>> print result
  File "<python-input-4>", line 1
    print result
    ^^^^^^^^^^^^
SyntaxError: Missing parentheses in call to 'print'. Did you mean print(...)?
>>> print(result)
A_b1t_0f_b1t_sh1fTiNg_2f138d3031
>>>
```

flag : picoCTF{A_b1t_0f_b1t_sh1fTiNg_2f138d3031}