vault-door-6

Medium Reverse Engineering picoCTF 2019

AUTHOR: MARK E. HAASE

Description

This vault uses an XOR encryption scheme.

The source code for this vault is here: VaultDoor6.java

Hints

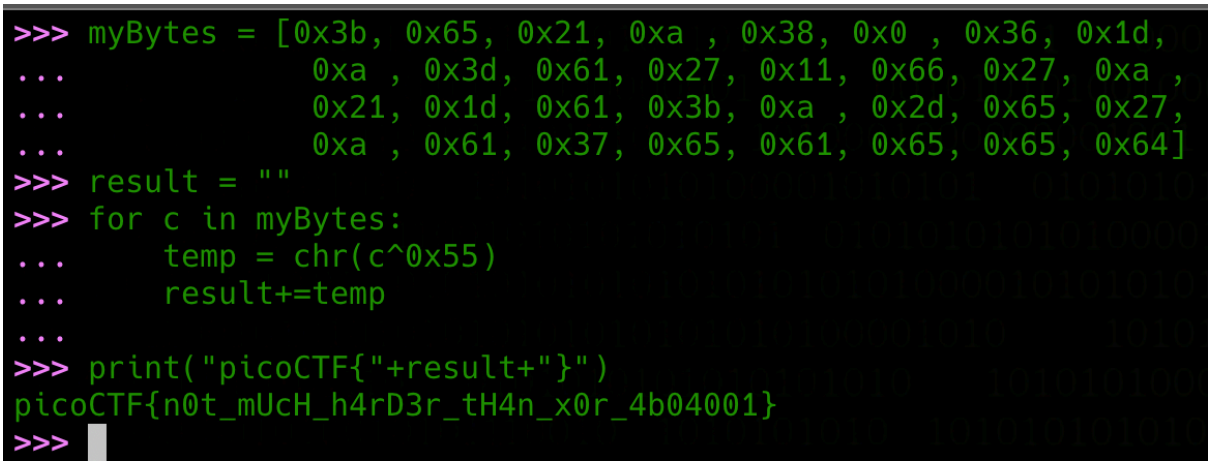
1

If X ^ Y = Z, then Z ^ Y = X. Write a program that decrypts the flag based on this fact.

mulai seru karena scripting wkwkwwk soalnya bisa melatih programming + cysec.

```
public boolean checkPassword(String password) {
    if (password.length() != 32) {
        return false;
    }
    byte[] passBytes = password.getBytes();
    byte[] myBytes = {
        0x3b, 0x65, 0x21, 0xa , 0x38, 0x0 , 0x36, 0x1d,
        0xa , 0x3d, 0x61, 0x27, 0x11, 0x66, 0x27, 0xa ,
        0x21, 0x1d, 0x61, 0x3b, 0xa , 0x2d, 0x65, 0x27,
        0xa , 0x61, 0x37, 0x65, 0x61, 0x65, 0x65, 0x64,
    };
    for (int i=0; i<32; i++) {
        if (((passBytes[i] ^ 0x55) - myBytes[i]) != 0) {
            return false;
        }
    }
    return true;
}
```

Terdapat fungsi validasi password dimana jika passBytes[i] (password input user) di xor dengan 0x55 tidak sama dengan myBytes[i], otomatis akan salah. Maka disini bisa kita asumsikan bahwa myBytes[i] xor 0x55 merupakan password input usernya. jadi kita bisa bikin script berikut.



flag : picoCTF{n0t_mUcH_h4rD3r_tH4n_x0r_4b04001}