Reverse Engineering

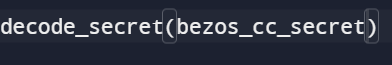
### 1. crackme-py



Solution: On inspecting the python code we see that it is calling the choose greatest function.



We need the decode function. So change the code and execute it.

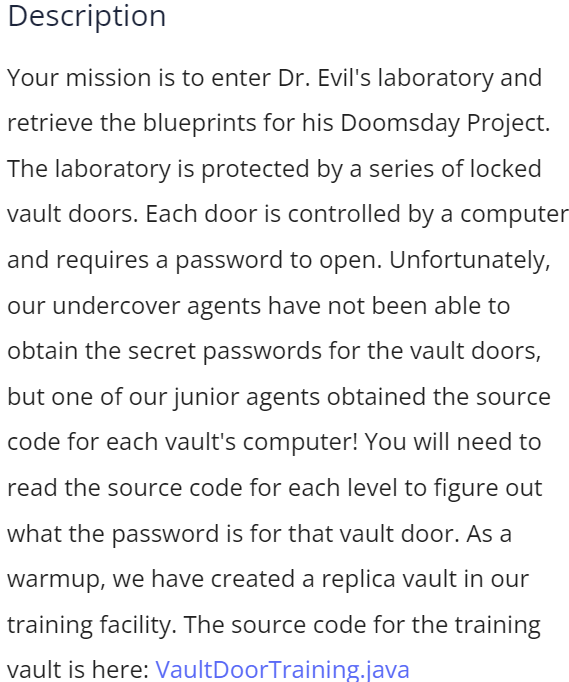


We get the glag after execution.

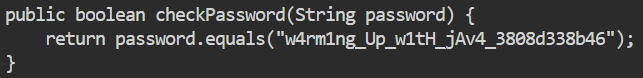


Flag: picoCTF{1|\/|\_4\_p34|\|ut\_4593da8a}

### 2. vault-door-training

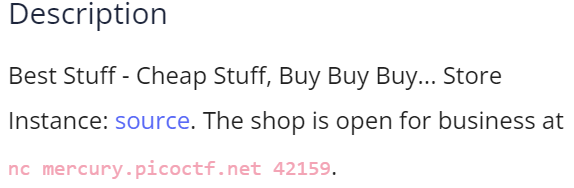


Solution: On inspecting the java code we find the flag.

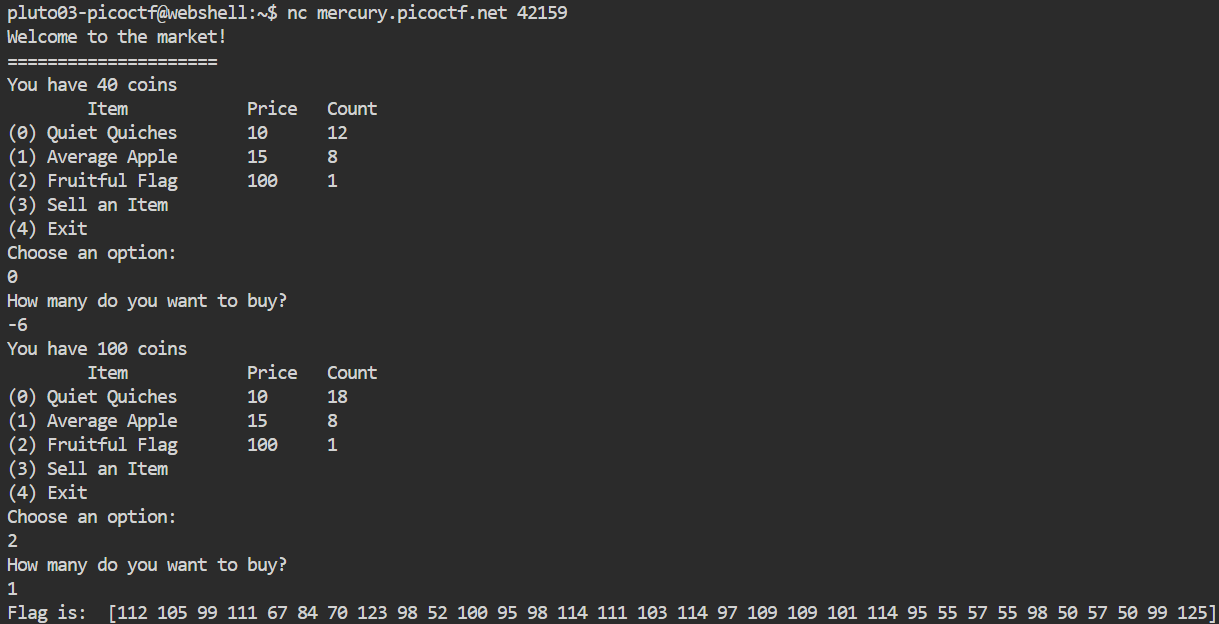


picoCTF{w4rm1ng\_Up\_w1tH\_jAv4\_3808d338b46}

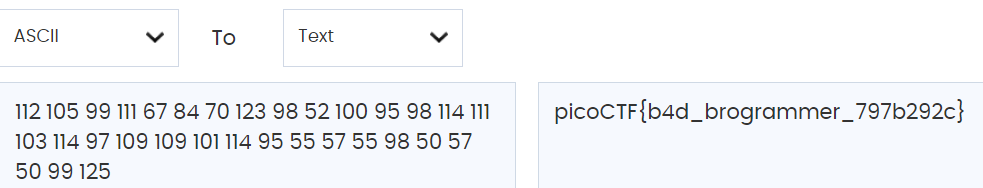
### 3. Shop



Solution: connect using netcat and get more coins to buy a fruitful flag.



We get a series of ASCII numbers. On converting we get the flag.

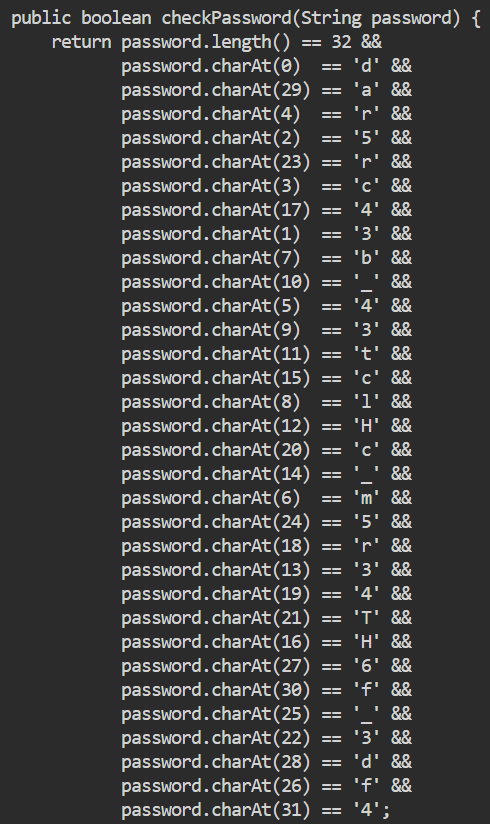


Flag: picoCTF{b4d\_brogrammer\_797b292c}

### 4. vault-door-1

### 

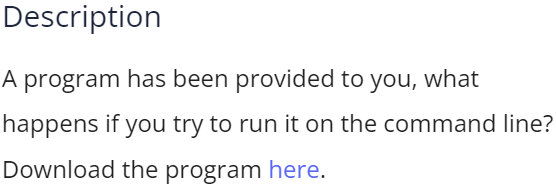
### Solution: On inspecting the java file we see the flag in a jumbled list



After placing each letter in the correct location we get the flag.

Flag: picoCTF{d35cr4mbl3\_th3\_cH4r4cT3r5\_f6daf4}

### 5. file-run1

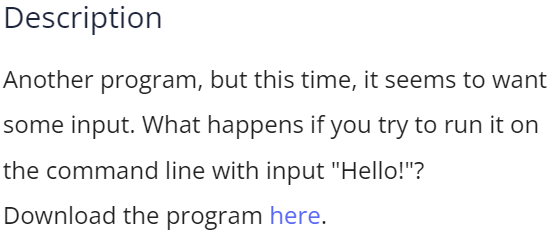


Solution: use srings command

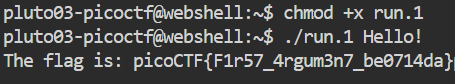


Flag: picoCTF{U51N6\_Y0Ur\_F1r57\_F113\_9bc52b6b}

### 6. file-run2

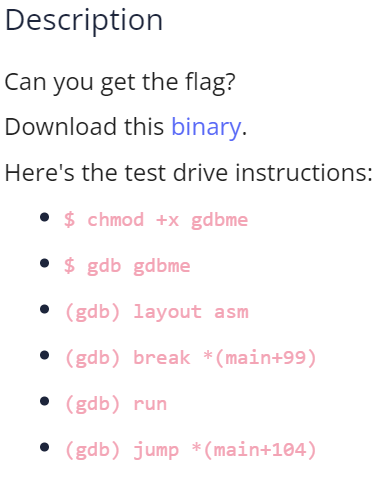


Solution: change the permissions of the file and execute it with given argument

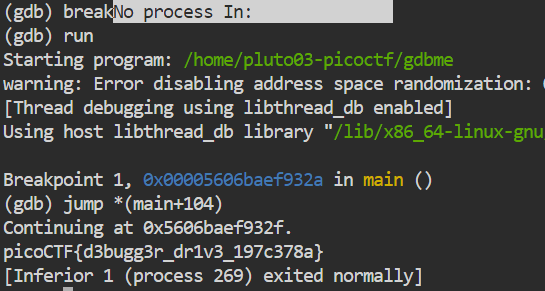


Flag: picoCTF{F1r57\_4rgum3n7\_be0714da}

### 7. GDB Test Drive

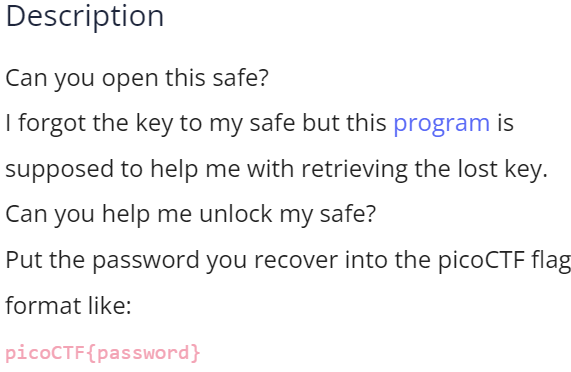


Solution: Download the file and follow the instructions:



Flag: picoCTF{d3bugg3r\_dr1v3\_197c378a}

### 8. Safe Opener



Solution: On inspecting the file we find the encoded key



This is key is Base64 coded. On decoding we get the flag.



Flag: picoCTF{ pl3as3\_l3t\_m3\_1nt0\_th3\_saf3}