Mark Seliternikov

picoCTF - Vault Door 3 [200 points]

```java
import java.util.*;

class VaultDoor3 {
    public static void main(String args[]) {
        VaultDoor3 vaultDoor = new VaultDoor3();
        Scanner scanner = new Scanner(System.in);
        System.out.print("Enter vault password: ");
        String userInput = scanner.next();
    String input = userInput.substring("picoCTF{".length(),userInput.length()-1);
    if (vaultDoor.checkPassword(input)) {
        System.out.println("Access granted.");
    } else {
        System.out.println("Access denied!");
        }
    }

    // Our security monitoring team has noticed some intrusions on some of the
    // less secure doors. Dr. Evil has asked me specifically to build a stronger
    // vault door to protect his Doomsday plans. I just *know* this door will
    // keep all of those nosy agents out of our business. Mwa ha!
    //
    // -Minion #2671
    public boolean checkPassword(String password) {
        if (password.length() != 32) {
            return false;
        }
        char[] buffer = new char[32];
        int i;
        for (i=0; i<8; i++) {
            buffer[i] = password.charAt(i);
        }
        for (; i<16; i++) {
            buffer[i] = password.charAt(23-i);
        }
        for (; i<32; i+=2) {
            buffer[i] = password.charAt(46-i);
        }
        for (i=31; i>=17; i-=2) {
            buffer[i] = password.charAt(i);
        }
        String s = new String(buffer);
        return s.equals("jU5t_a_sna_3lpm18gb41_u_4_mfr340");
    }
}
```

לאתגר זה מקבלים קובץ Java, האתגר הוא למצוא את הסיסמה.
לפי האתגר הסיסמה עצמה היא בעצם הדגל.

```java
String input = userInput.substring("picoCTF{".length(),userInput.length()-1);
if (vaultDoor.checkPassword(input)) {
    System.out.println("Access granted.");
```

כאן ניתן לראות שהסיסמה מורידה את החלק של הפורמט של הדגל מהסיסמה עצמה ומבצעת פונק' על התוכן של הדגל.

```java
public boolean checkPassword(String password) {
    if (password.length() != 32) {
        return false;
    }
    char[] buffer = new char[32];
    int i;
    for (i=0; i<8; i++) {
        buffer[i] = password.charAt(i);
    }
    for (; i<16; i++) {
        buffer[i] = password.charAt(23-i);
    }
    for (; i<32; i+=2) {
        buffer[i] = password.charAt(46-i);
    }
    for (i=31; i>=17; i-=2) {
        buffer[i] = password.charAt(i);
    }
    String s = new String(buffer);
    return s.equals("jU5t_a_sna_3lpm18gb41_u_4_mfr340");
}
```

אפשר לראות כיצד התוכנה משנה את הסדר של ה-input ומשווה לתוצאה שהוגדרה מראש.
לכן אפשר להבין שכדי למצוא את הדגל צריך לעשות סידור לאחור של ה"בילגון" שעשו בתוכנה.

לכן כתבתי סקריפט פייתון שיעשה את העבודה בשבילי וידפיס את התוצאה בפורמט של הדגל

```python
text = list("jU5t_a_sna_3lpm18gb41_u_4_mfr340")
result = list("jU5t_a_sna_3lpm18gb41_u_4_mfr340")

for i in range(8):
    result[i] = text[i]

for i in range(8, 16):
   result[23-i] = text[i]

for i in range(16, 32, 2):
    result[46 - i] = text[i]

for i in range(31, 17, -2):
    result[i] = text[i]

print("picoCTF{", end="")
for i in result:
    print(i, end="")
print("}")
```

והנה הדגל :)

```
mark@workstation:~/Repos$ python3 vd3.py
picoCTF{jU5t_a_s1mpl3_an4gr4m_4_u_1fb380}
mark@workstation:~/Repos$
```