Mark Seliternikov
picoCTF - Vault Door Training [50 points]

לאתגר אנחנו מקבלים קובץ בשם VaultDoorTraining מסוג java.
הקובץ הוא ה-source code של תוכנה שאמורה לבדוק אם הסיסמה שנכתבה נכונה.
ה-source code נראה כך:

```
import java.util.*;

class VaultDoorTraining {
    public static void main(String args[]) {
        VaultDoorTraining vaultDoor = new VaultDoorTraining();
        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!");
    }
   }

    // The password is below. Is it safe to put the password in the source code?
    // What if somebody stole our source code? Then they would know what our
    // password is. Hmm... I will think of some ways to improve the security
    // on the other doors.
    //
    // -Minion #9567
    public boolean checkPassword(String password) {
        return password.equals("w4rm1ng_Up_w1tH_jAv4_eec0716b713");
    }
}
```

ניתן לראות התחלה של דגל:

```
String input = userInput.substring("picoCTF{".length(),userInput.length()-1)
```

הסקריפט לוקח את החלק שנכתב לאחר picoCTF{, ומוריד את התו האחרון. לפי כך ניתן להבין שהסיסמה היא הדגל.
ה-STR בתוך הדגל נבדק אם הוא שווה לSTR הבא:

```
public boolean checkPassword(String password) {
    return password.equals("w4rm1ng_Up_w1tH_jAv4_eec0716b713");
```

מכך ניתן להבין כי הדגל הוא

picoCTF{w4rm1ng_Up_w1tH_jAv4_eec0716b713}

וזאת אכן התשובה!

מה למדתי:

- למרות שבשלב זה כאשר אני פותר CTF, איני יודע כל כך java. אבל מה שעזר לי לפתור זה ההבנה לאיך קוד עובד, אולי השפה משתנה אבל החוקים הם עדיין אותם חוקים. לכן חשוב ללמוד איך קוראים קוד כך שתוכל להשליך את זה לשפות אחרות.