Mark Seliternikov

picoCTF - Vault Door 5 [300 points]

לאתגר זה מקבלים קובץ Java, אשר נראה כך:

```java
import java.net.URLDecoder;
import java.util.*;

class VaultDoor5 {
    public static void main(String args[]) {
        VaultDoor5 vaultDoor = new VaultDoor5();
        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!");
        }
    }

    // Minion #7781 used base 8 and base 16, but this is base 64, which is
    // like... eight times stronger, right? Riiighht? Well that's what my twin
    // brother Minion #2415 says, anyway.
    //
    // -Minion #2414
    public String base64Encode(byte[] input) {
        return Base64.getEncoder().encodeToString(input);
    }

    // URL encoding is meant for web pages, so any double agent spies who steal
    // our source code will think this is a web site or something, defintely not
    // vault door! Oh wait, should I have not said that in a source code
    // comment?
    //
    // -Minion #2415
    public String urlEncode(byte[] input) {
        StringBuffer buf = new StringBuffer();
        for (int i=0; i<input.length; i++) {
            buf.append(String.format("%%%2x", input[i]));
        }
        return buf.toString();
    }

    public boolean checkPassword(String password) {
        String urlEncoded = urlEncode(password.getBytes());
        String base64Encoded = base64Encode(urlEncoded.getBytes());
        String expected = "JTYzJTMwJTZlJTc2JTMzJTcyJTc0JTMxJTZlJTY3JTVm"
                        + "JTY2JTcyJTMwJTZkJTVmJTYyJTYxJTM1JTY1JTVmJTM2"
                        + "JTM0JTVmJTMwJTYyJTM5JTM1JTM3JTYzJTM0JTY2";
        return base64Encoded.equals(expected);
    }
}
```

לפי הרמזים של האתגר עצמו וגם מהתגובות הרשומות ב-Source code, ניתן להבין שההצפנה של הסיסמה היא ל-URL ואז Base64.

```java
// Minion #7781 used base 8 and base 16, but this is base 64, which is
// like... eight times stronger, right? Riiighht? Well that's what my twin
// brother Minion #2415 says, anyway.
```

```java
// URL encoding is meant for web pages, so any double agent spies who steal
// our source code will think this is a web site or something, defintely not
// vault door! Oh wait, should I have not said that in a source code
// comment?
```

בנוסף אפשר לראות שהסיסמה היא הדגל עצמו, ומה שהוצפן זה התוכן בתוך הדגל

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

ככה אמור להיראות התוכן המוצפן של הדגל

```java
String expected = "JTYzJTMwJTZlJTc2JTMzJTcyJTc0JTMxJTZlJTY3JTVm"
                + "JTY2JTcyJTMwJTZkJTVmJTYyJTYxJTM1JTY1JTVmJTM2"
                + "JTM0JTVmJTMwJTYyJTM5JTM1JTM3JTYzJTM0JTY2";
```

אפשר לפתור את האתגר ממש בקלות על ידי דיקודרים אונליין (אגב, לאתגר זה נותנים קישור לאחד שפותר את האתגר בשנייה... לא ברור לי למה האתגר הזה 300 נקודות).
אבל לפתור את זה כך לא מרגיש מלמד בשבילי, לכן קראתי קצת על Base64 ועל URL encoding. וכתבתי את הסקריפט הבא בפייתון כדי לפתור את האתגר.

```python
from base64 import b64decode
from requests.utils import unquote

text = "JTYzJTMwJTZlJTc2JTMzJTcyJTc0JTMxJTZlJTY3JTVmJTY

print(f"Original : {text}\n")

textv2 = b64decode(text).decode("utf-8")

print(f"Base64 decoded : {textv2}\n")

textv3 = unquote(textv2)

print(f"URL decoded : {textv3}\n")

print("flag : picoCTF{" + textv3 + "}")
```

לאחר מכן הסתכלתי על הפלט שיצא מהסקריפט שכתבתי
ולאחר בדיקה זה אכן הדגל :)

```
mark@mark-ubuntu:~/Repos$ python3 solver.py
Original : JTYzJTMwJTZlJTc2JTMzJTcyJTc0JTMxJTZlJTY3JTVmJTY2JTcyJTMwJTZkJTVmJTYyJTYxJTM1JTY1JTVmJTM2JT
M0JTVmJTMwJTYyJTM5JTM1JTM3JTYzJTM0JTY2

Base64 decoded : %63%30%6e%76%33%72%74%31%6e%67%5f%66%72%30%6d%5f%62%61%35%65%5f%36%34%5f%30%62%39%3
%37%63%34%66

URL decoded : c0nv3rt1ng_fr0m_ba5e_64_0b957c4f

flag : picoCTF{c0nv3rt1ng_fr0m_ba5e_64_0b957c4f}
mark@mark-ubuntu:~/Repos$
```