## ***Test Summary Report***

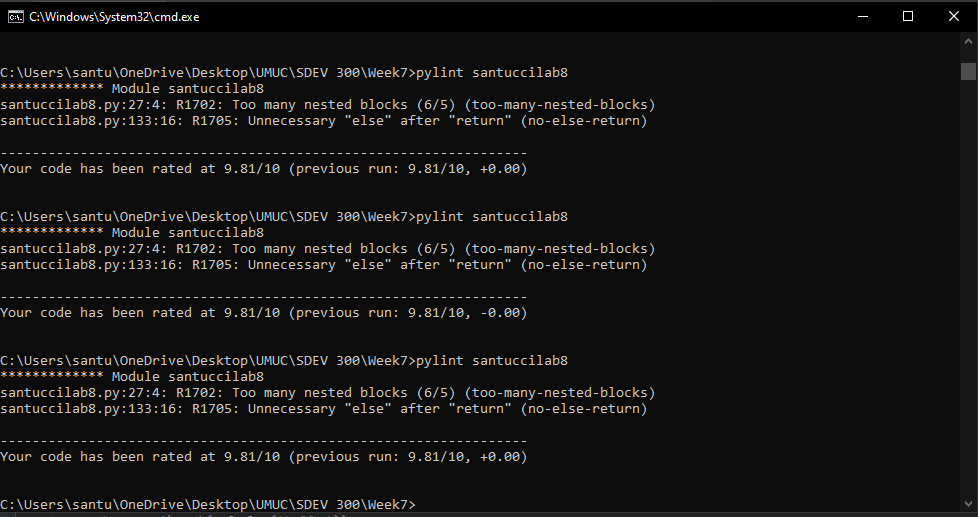
**Joe Santucci**

**SDEV 300 7383**

**05/11/2021**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Test Case** | **Input** | Expected Output | **Actual Output** | **Result** |
| **1.**  **Figure 1** | JoeDoe1  Joedoe | Fills log with Client IP and date/time | **Successfully filled log with Client IP and date/time** | **Pass** |
| **2.**  **Figure 2** | Password:  ranger | “This password has previously been compromised, enter another password” | **“This password has previously been compromised, enter another password”** | **Pass** |
| **3.**  **Figure 3** | Password:  password | “This password has previously been compromised, enter another password” | **“This password has previously been compromised, enter another password”** | **Pass** |

**Pylint Results:**



I tried my best to consolidate the nested statements, which were actually at 7, got it down to six.

Not sure about the unnecessary return statements, most of the return statements provided direction from the IF statements.

I am done continuing to try and fix it.

1. Displays warning that user failed to login and fills log with IP/Date/Time:

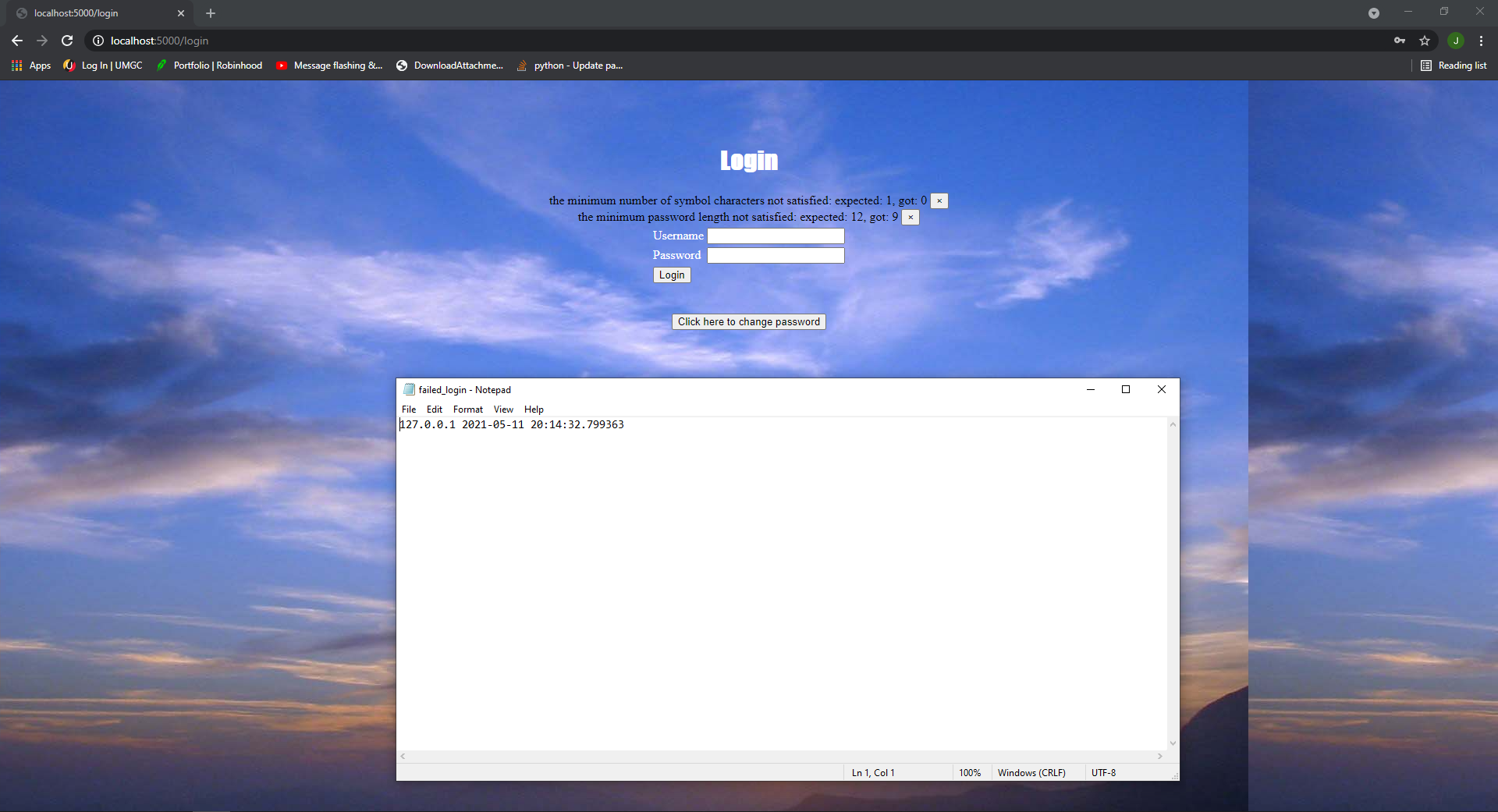


Figure 1: log with IP/Date/Time

1. Displaying Compromised Password (ranger):

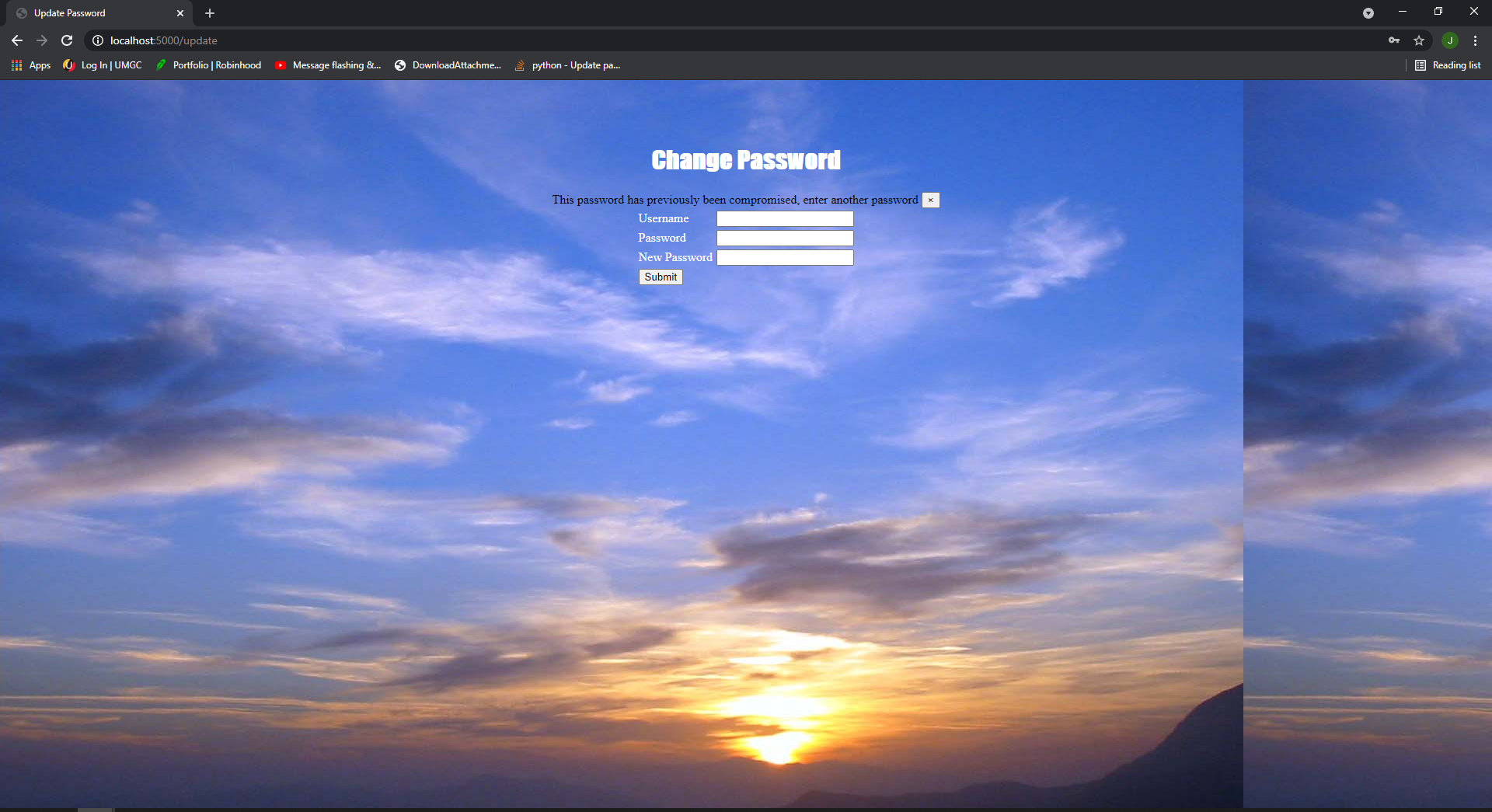


Figure 2: Compromised Password (ranger)

1. Displaying Compromised Password (password):

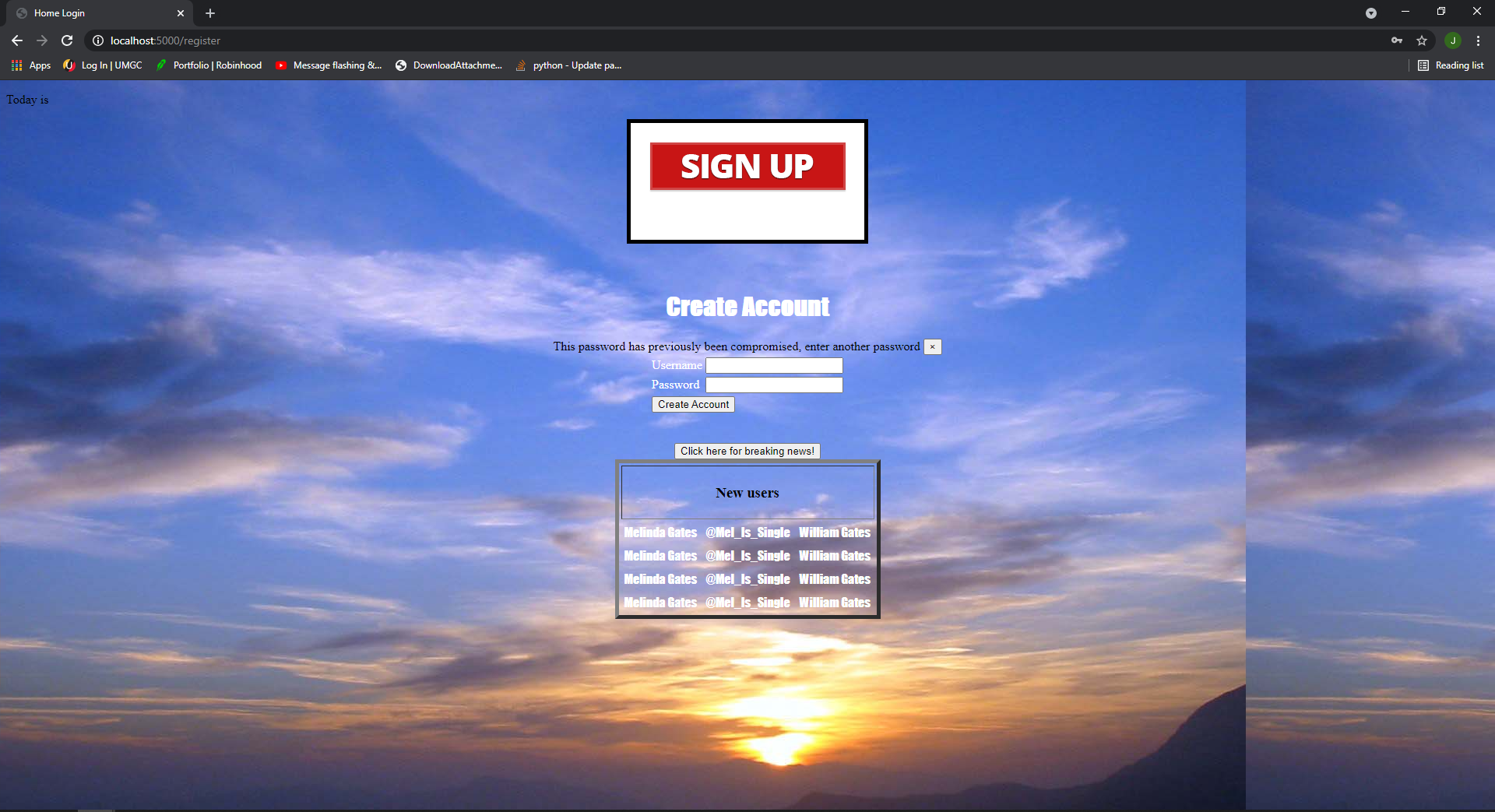
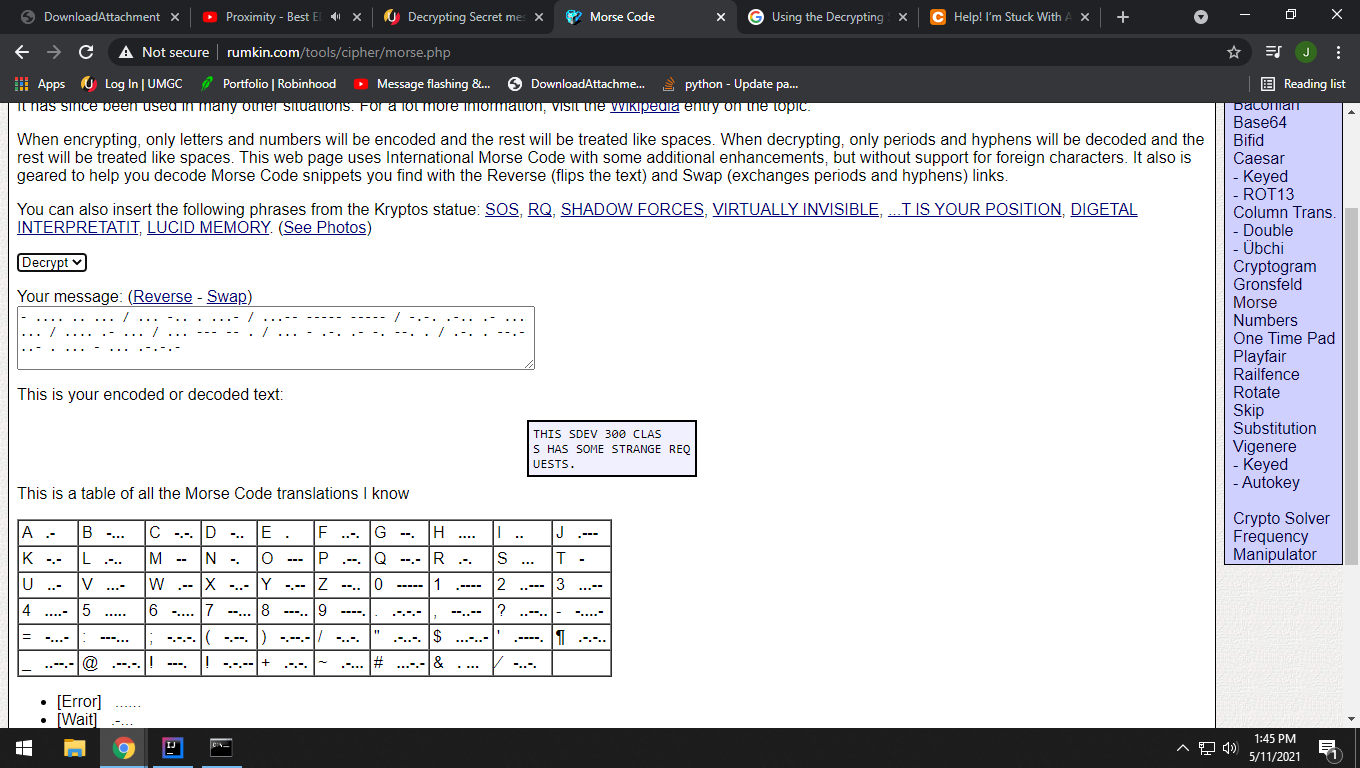


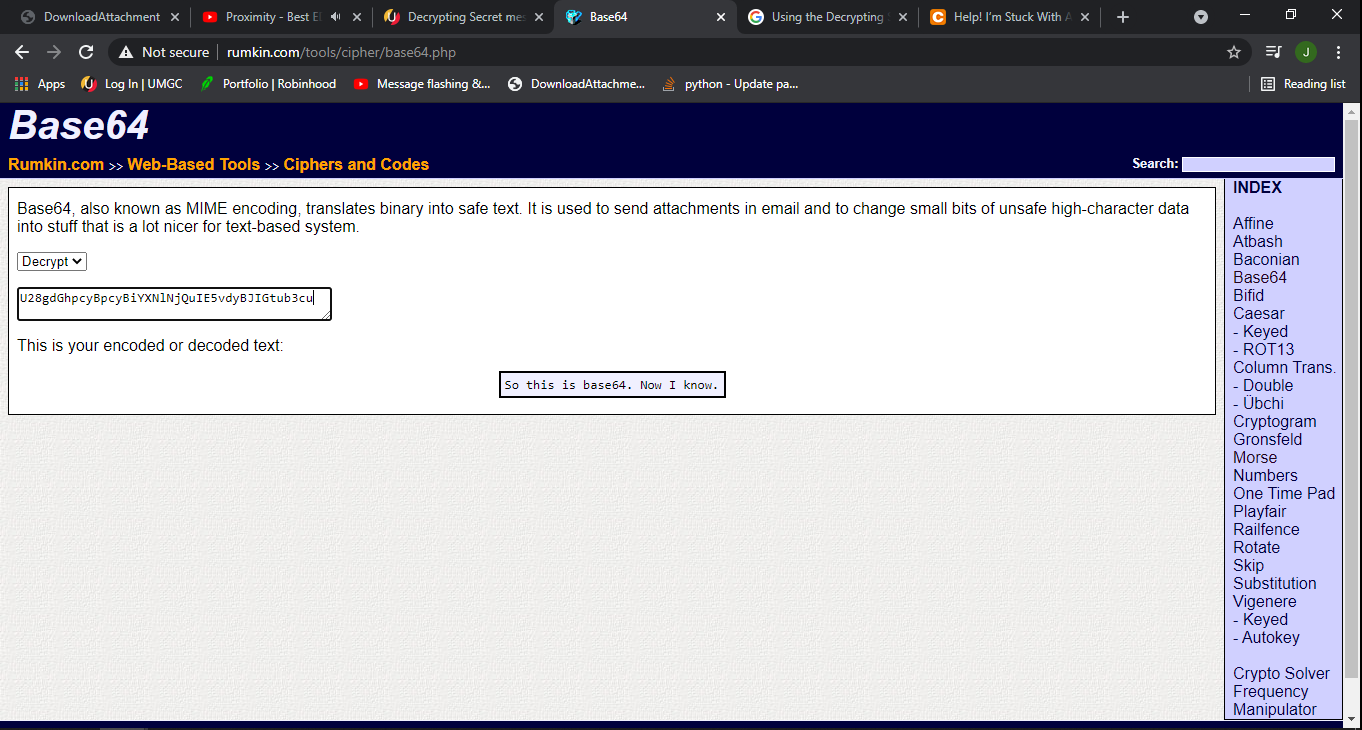
Figure 3: Compromised Password (password)

1. It was obviously morse code so I chose the morse code decryption tool. “THIS SDEV 300 CLASS HAS SOME STRANGE REQUESTS”



1. I am not to certain as to why it immediately came to me but base64 was my first guess and it worked.

“So this is base64. Now I know”



1. This was something I had never seen before. I used google to find out what form of encryption it was, arrow keyed down until the message read familiar.

“--- Begin Key ---

I am so clever. No one could possibly figure this out.

---End Key---”