Daniel Beck

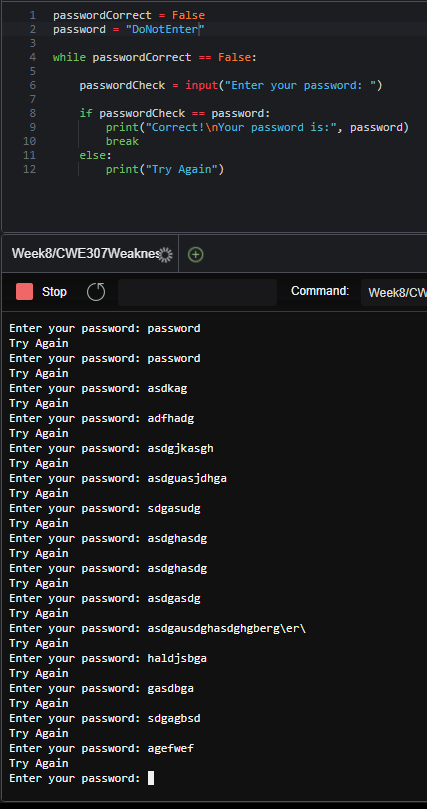
SDEV-325

October 13, 2020

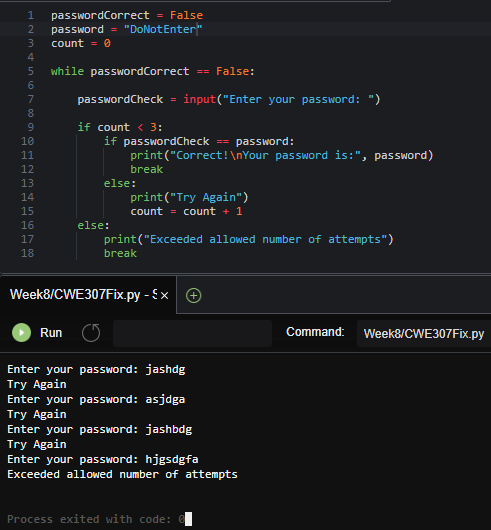
1. The first software vulnerability that was addressed was CWE-307: Improper Restriction of Excessive Authentication Attempts. A CWE-307 vulnerability occurs when “The software does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame, making it more susceptible to brute force attacks (*Common Weakness Enumeration,* 2020).” If there are no restrictions on how many attempts can be made, then hackers can continuously attack an account until access is granted. 1a shows a program that continuously will allow someone trying to gain access to the account, multiple attempts, without restriction. 1b shows the result of the weakness being mitigated by adding a counter to the password attempts and exits the program after four failed attempts.

2. The second software vulnerability that was addressed was CWE-327: Use of a Broken or Risky Cryptographic Algorithm. A CWE-327 vulnerability occurs when “The use of a broken or risky cryptographic algorithm is an unnecessary risk that may result in the exposure of sensitive information (*Common Weakness Enumeration,* 2020).” If users’ passwords are not encrypted correctly, there is a chance that their passwords may be exposed, or the password may become lost, locking the user out of their account. 2a shows what it may look like when using a python extension, cryptography.fernet that has become broken and is not properly encrypting/decrypting passwords. The output of the program shows that the password that is stored does not get decrypted correctly. 2b shows the mitigation of the vulnerability by using a corrected method that runs the password through a cryptography algorithm.

1a.

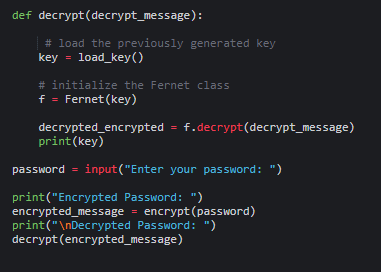


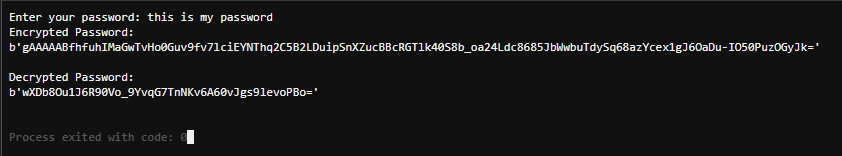
1b.



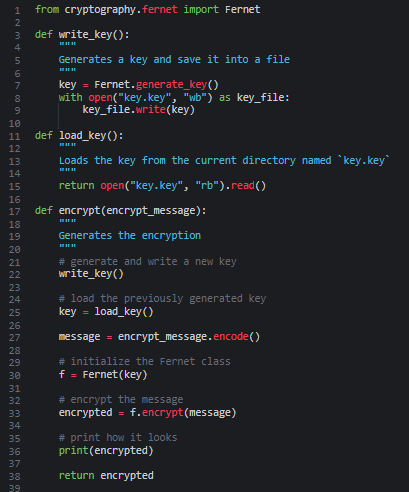
2a.

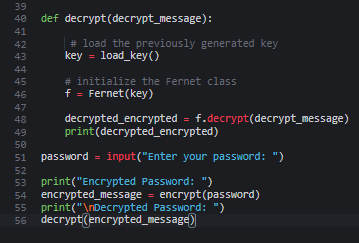


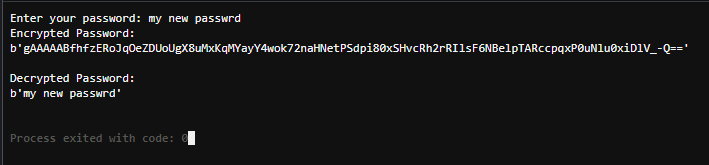




2b.







References:

Common Weakness Enumeration. (2020, August 20). Retrieved October 10, 2020, from https://cwe.mitre.org/data/definitions/