Daniel Beck

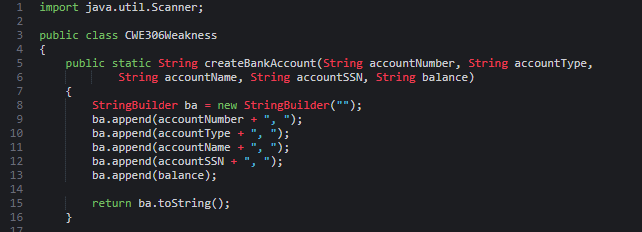
SDEV-325

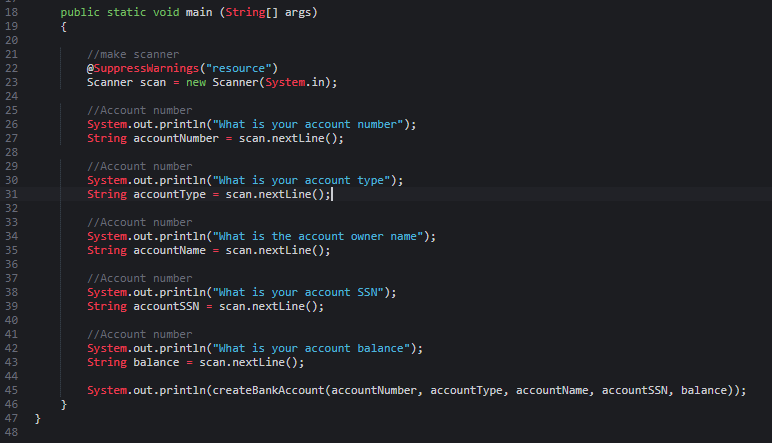
September 28, 2020

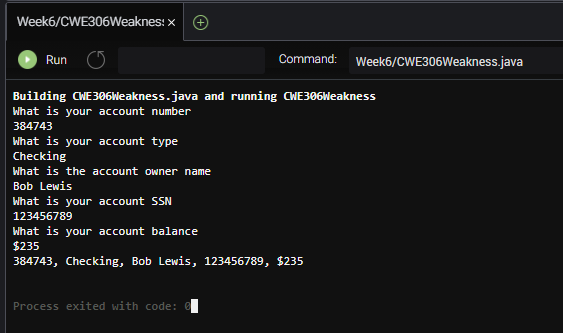
1. The first software vulnerability that was addressed was CWE-306: Missing Authentication for Critical Function. A CWE-306 vulnerability occurs when “the software does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources (*Common Weakness Enumeration,* 2020).” An example of where this vulnerability may be exposed is in software that accepts setting for a bank account. 1a shows a program that accepts information for a bank account. 1b shows the result of the weakness being mitigated by having the program run through a function that prompts the user for a password.

2. The second software vulnerability that was addressed was CWE-311: Missing Encryption of Sensitive Data. A CWE-311 vulnerability occurs when “the software does not encrypt sensitive or critical information before storage or transmission (*Common Weakness Enumeration,* 2020).” If users’ passwords are not encrypted, there is a chance that their passwords may be exposed. 2a shows an example of a of what a user’s password is stored as. 2b shows the mitigation of the vulnerability by using a python extension, cryptography.fernet, to use functions that encrypt passwords that are passed to them.

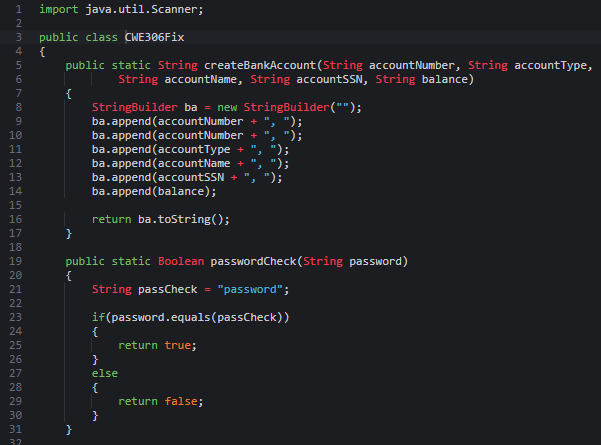
1a.

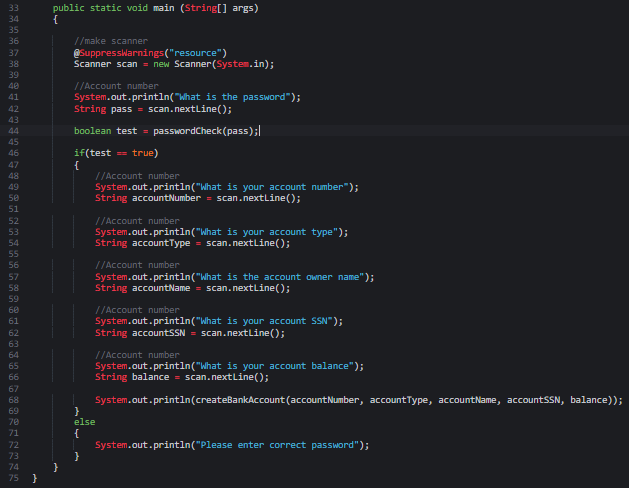


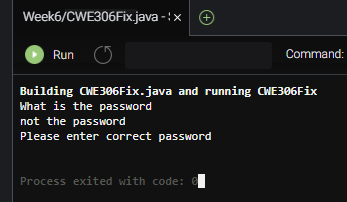


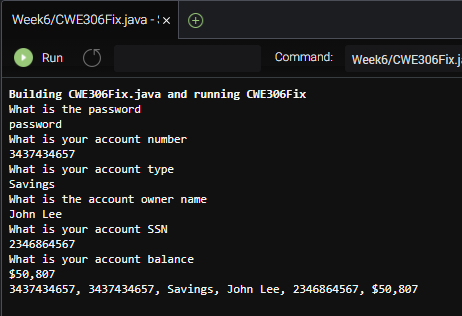


1b.

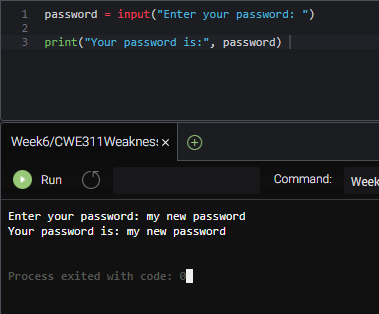




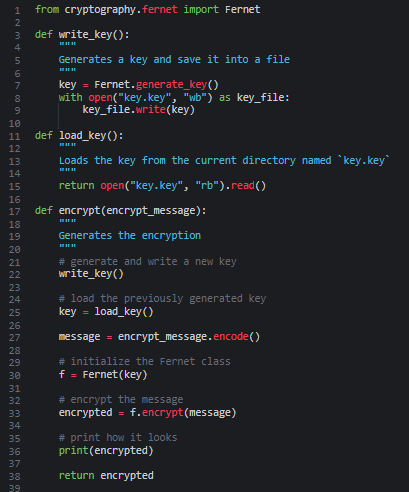


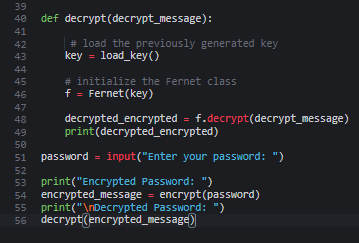


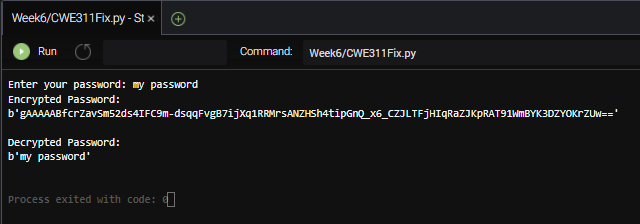
2a.



2b.







References:

Common Weakness Enumeration. (2020, August 20). Retrieved September 29, 2020, from https://cwe.mitre.org/data/definitions/