

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.

```
1  import java.util.Scanner;
2
3  public class CWE306Weakness
4  {
5      public static String createBankAccount(String accountNumber, String accountType,
6          String accountName, String accountSSN, String balance)
7      {
8          StringBuilder ba = new StringBuilder("");
9          ba.append(accountNumber + ", ");
10         ba.append(accountType + ", ");
11         ba.append(accountName + ", ");
12         ba.append(accountSSN + ", ");
13         ba.append(balance);
14
15         return ba.toString();
16     }
17
18     public static void main (String[] args)
19     {
20
21         //make scanner
22         @SuppressWarnings("resource")
23         Scanner scan = new Scanner(System.in);
24
25         //Account number
26         System.out.println("What is your account number");
27         String accountNumber = scan.nextLine();
28
29         //Account number
30         System.out.println("What is your account type");
31         String accountType = scan.nextLine();
32
33         //Account number
34         System.out.println("What is the account owner name");
35         String accountName = scan.nextLine();
36
37         //Account number
38         System.out.println("What is your account SSN");
39         String accountSSN = scan.nextLine();
40
41         //Account number
42         System.out.println("What is your account balance");
43         String balance = scan.nextLine();
44
45         System.out.println(createBankAccount(accountNumber, accountType, accountName, accountSSN, balance));
46     }
47 }
48
```

Week6/CWE306Weaknes: x



Run



Command:

Week6/CWE306Weakness.java

**Building CWE306Weakness.java and running CWE306Weakness**

What is your account number

384743

What is your account type

Checking

What is the account owner name

Bob Lewis

What is your account SSN

123456789

What is your account balance

\$235

384743, Checking, Bob Lewis, 123456789, \$235

Process exited with code: 0

1b.

```
1  import java.util.Scanner;
2
3  public class CWE306Fix
4  {
5      public static String createBankAccount(String accountNumber, String accountType,
6          String accountName, String accountSSN, String balance)
7      {
8          StringBuilder ba = new StringBuilder("");
9          ba.append(accountNumber + ", ");
10         ba.append(accountNumber + ", ");
11         ba.append(accountType + ", ");
12         ba.append(accountName + ", ");
13         ba.append(accountSSN + ", ");
14         ba.append(balance);
15
16         return ba.toString();
17     }
18
19     public static Boolean passwordCheck(String password)
20     {
21         String passCheck = "password";
22
23         if(password.equals(passCheck))
24         {
25             return true;
26         }
27         else
28         {
29             return false;
30         }
31     }
32 }
```

```

33 public static void main (String[] args)
34 {
35
36     //make scanner
37     @SuppressWarnings("resource")
38     Scanner scan = new Scanner(System.in);
39
40     //Account number
41     System.out.println("What is the password");
42     String pass = scan.nextLine();
43
44     boolean test = passwordCheck(pass);
45
46     if(test == true)
47     {
48         //Account number
49         System.out.println("What is your account number");
50         String accountNumber = scan.nextLine();
51
52         //Account number
53         System.out.println("What is your account type");
54         String accountType = scan.nextLine();
55
56         //Account number
57         System.out.println("What is the account owner name");
58         String accountName = scan.nextLine();
59
60         //Account number
61         System.out.println("What is your account SSN");
62         String accountSSN = scan.nextLine();
63
64         //Account number
65         System.out.println("What is your account balance");
66         String balance = scan.nextLine();
67
68         System.out.println(createBankAccount(accountNumber, accountType, accountName, accountSSN, balance));
69     }
70     else
71     {
72         System.out.println("Please enter correct password");
73     }
74 }
75 }

```

Week6/CWE306Fix.java -! x

Run

Command:

Building CWE306Fix.java and running CWE306Fix  
What is the password  
not the password  
Please enter correct password  
  
Process exited with code: 0

Week6/CWE306Fix.java - !x



Run



Command:

Week6/CWE306Fix.j

Building CWE306Fix.java and running CWE306Fix

What is the password

password

What is your account number

3437434657

What is your account type

Savings

What is the account owner name

John Lee

What is your account SSN

2346864567


What is your account balance



\$50,807

3437434657, 3437434657, Savings, John Lee, 2346864567, \$50,807

2a.

```
1 password = input("Enter your password: ")
2
3 print("Your password is:", password) |
```

Week6/CWE311Weaknes: x 

 Run  Command: Week

```
Enter your password: my new password
Your password is: my new password

Process exited with code: 0
```

2b.

```
1  from cryptography.fernet import Fernet
2
3  def write_key():
4      """
5      Generates a key and save it into a file
6      """
7      key = Fernet.generate_key()
8      with open("key.key", "wb") as key_file:
9          key_file.write(key)
10
11 def load_key():
12     """
13     Loads the key from the current directory named `key.key`
14     """
15     return open("key.key", "rb").read()
16
17 def encrypt(encrypt_message):
18     """
19     Generates the encryption
20     """
21     # generate and write a new key
22     write_key()
23
24     # load the previously generated key
25     key = load_key()
26
27     message = encrypt_message.encode()
28
29     # initialize the Fernet class
30     f = Fernet(key)
31
32     # encrypt the message
33     encrypted = f.encrypt(message)
34
35     # print how it looks
36     print(encrypted)
37
38     return encrypted
39
```

```
39
40 def decrypt(decrypt_message):
41
42     # load the previously generated key
43     key = load_key()
44
45     # initialize the Fernet class
46     f = Fernet(key)
47
48     decrypted_encrypted = f.decrypt(decrypt_message)
49     print(decrypted_encrypted)
50
51 password = input("Enter your password: ")
52
53 print("Encrypted Password: ")
54 encrypted_message = encrypt(password)
55 print("\nDecrypted Password: ")
56 decrypt(encrypted_message)
```



Week6/CWE311Fix.py - St x



Run



Command:

Week6/CWE311Fix.py

Enter your password: my password

Encrypted Password:

b'gAAAAABfcrZavSm52ds4IFC9m-dsqqFvgB7ijXq1RRMrsANZHSh4tipGnQ\_x6\_CZJLTFjHIqRaZJKpRAT91WmBYK3DZYOKrZUw=='

Decrypted Password:

b'my password'

Process exited with code: 0

#### References:

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