



# **Security Vulnerability Report for** **Stock App**

**Thick application audit done by EPITA CS Spring 2022**

**Submitted By:**

**Tanzila Hasan Pinky**

**Sanujan Thavarasa**

**Anantha Sagar Singitham**

**Submission Date:**

**7<sup>th</sup> November 2022**

---

## Table of Contents:

1.Password Visibility while typing.....	1
2. Passwords hardcoded within the executable file .....	4
3. Password in cleartext in the configuration file: .....	7
4. Passwords stored in cleartext within the database:.....	10
5. Arbitrary system commands injection:.....	13
6.Bad profiles segregation: .....	15
7.Secrets present in memory even when not needed: .....	17
8.Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') .....	19
9.Network traffic not encrypted:.....	21
10.Weak passwords accepted: .....	24

---

## **Synthesis**

For the Stock App EPITA CS Spring-22 has been performed an audit report from 29<sup>th</sup> September to 1<sup>st</sup> of October 2022. There were some vulnerabilities while checking the security of the stock app in which we found 16 of them and the selected 10 is mentioned in the following report. The main goal of this report is to find out the vulnerabilities and ensuring stock app is compliant to the security guideline.

There are some critical vulnerabilities that allow the attacker to take the entire control for changing the password and access the database as well change every configuration files. Those are very harmful for the business organization. Most high impact vulnerabilities are about visible and storage password, privileges, and encryption. Credential of app is key of app's entry gate and a defect in it means giving complete access to the application in the hands of attacker. Most of the vulnerabilities are left due to the developer's mistake so that it is quite easy for the attacker to get the credentials for changing or accessing the database, control like stopping or switching the application, changing the password. In the medium risk vulnerabilities, it is allowing the attacker to view all the system works and gain the knowledge about the work process of the application. The low-risk vulnerabilities are in the low priority list for fixing.

The recommendation for preventing the vulnerabilities is- not saving personal information's on the application, as well it's better to use case sensitive passwords in limit of 12-14 characters. As well the encryption methods can be used for password security. It is also advised to make sure that proper testing method with expert testers for avoiding all those plaintext credentials and password issue problems. To prevent the SQL and OS command injection it's better that the users input is verified and validated always.

---

# Vulnerability Sheet

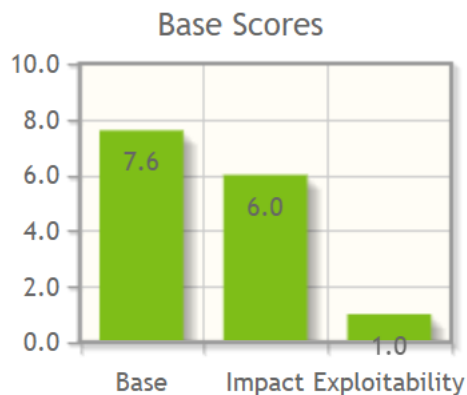
## **1.Password Visibility while typing**

### **1.1 CWE-549: Missing Password Field Masking:**

<https://cwe.mitre.org/data/definitions/549.html>

### **1.2 Base Score Metrics :**

- Risk Level:High
- <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H&version=3.1>



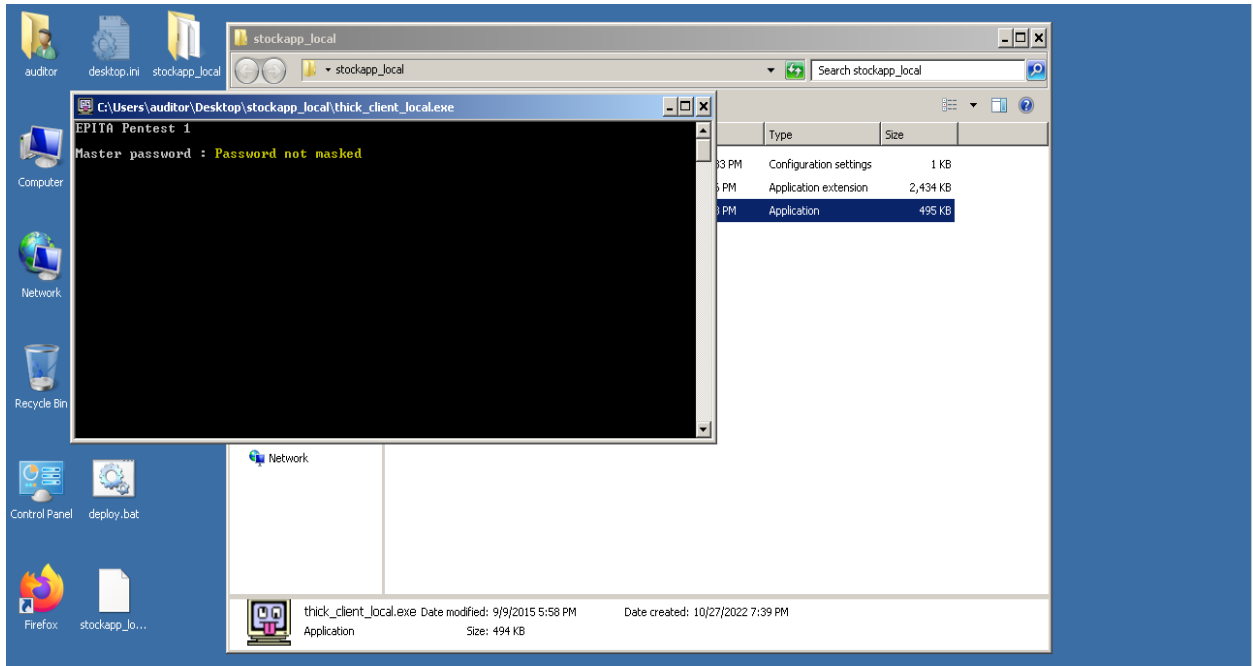
[AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H](https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H&version=3.1)

### **1.3 Description:**

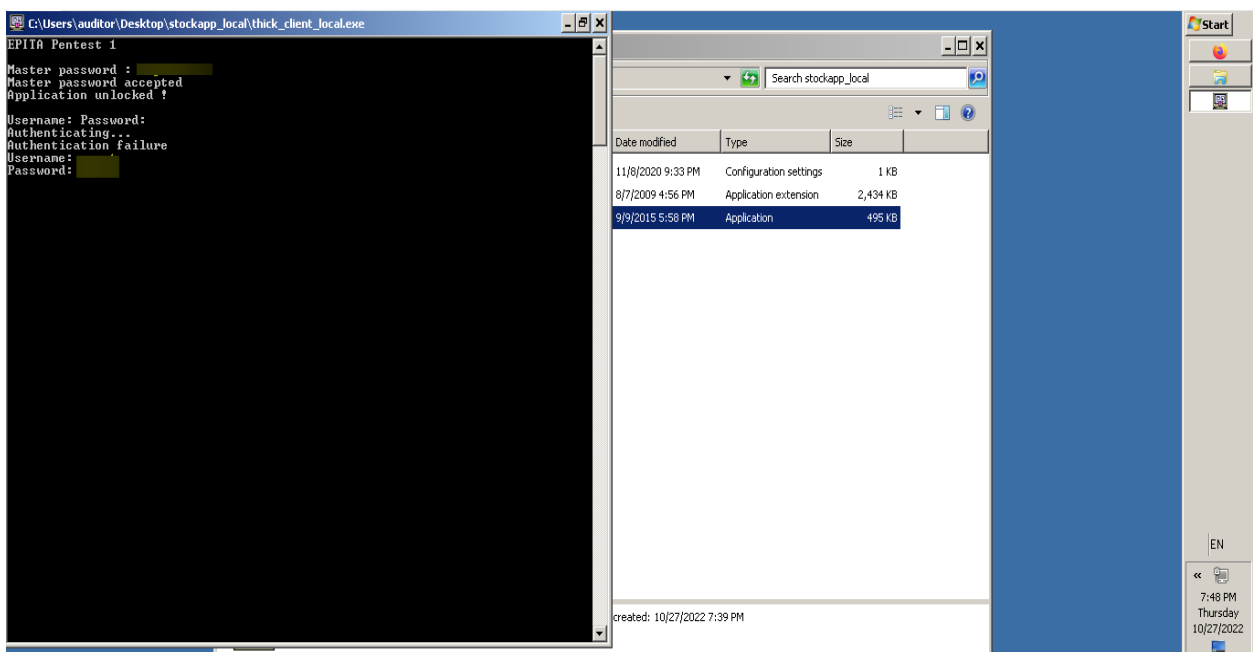
If an attacker gets a chance to see the password entered by the user on the command prompt while typing, he may simply see it and gain access to the application and authenticate. This type of vulnerability can be attacked by people who don't need much technical knowledge.

## 1.4 Exploitation:

- For the master password attacker need to view the screen used by the user.



- Type password and it's visible that the password is fully exposed.
- Not only master password we can also see username and password seen after application is unlocked.



- An attacker just must see the screen of user when he is entering his username and password to replicate the process and gain access.

### 1.5 Recommendations:

- Its better to use the masking system for hiding the password.
- In place of the password if asterisk's or hashed are used its also better.
- Long password character like 12-14 are also advised able to use and repetitive password attempts should be avoidable (Brute force attack for the attackers to try).
- Read more <https://cloudinfrastructureservices.co.uk/nist-password-guidelines-requirements-best-practices/#:~:text=NIST%20Password%20Guidelines%20for%202022%201%201.%20Password,context%20specific%20words%20as%20passwords%20...%20%C3%89I%C3%A9ments%20suppl%C3%A9mentaires>

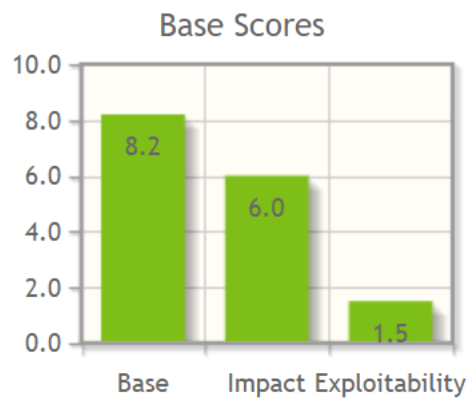
## **2. Passwords hardcoded within the executable file**

### **2.1 CWE-798: Use of Hard-coded Credentials:**

<https://cwe.mitre.org/data/definitions/798.html>

### **2.2 Base Score Metrics :**

- Risk Level: High
- <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H&version=3.1>



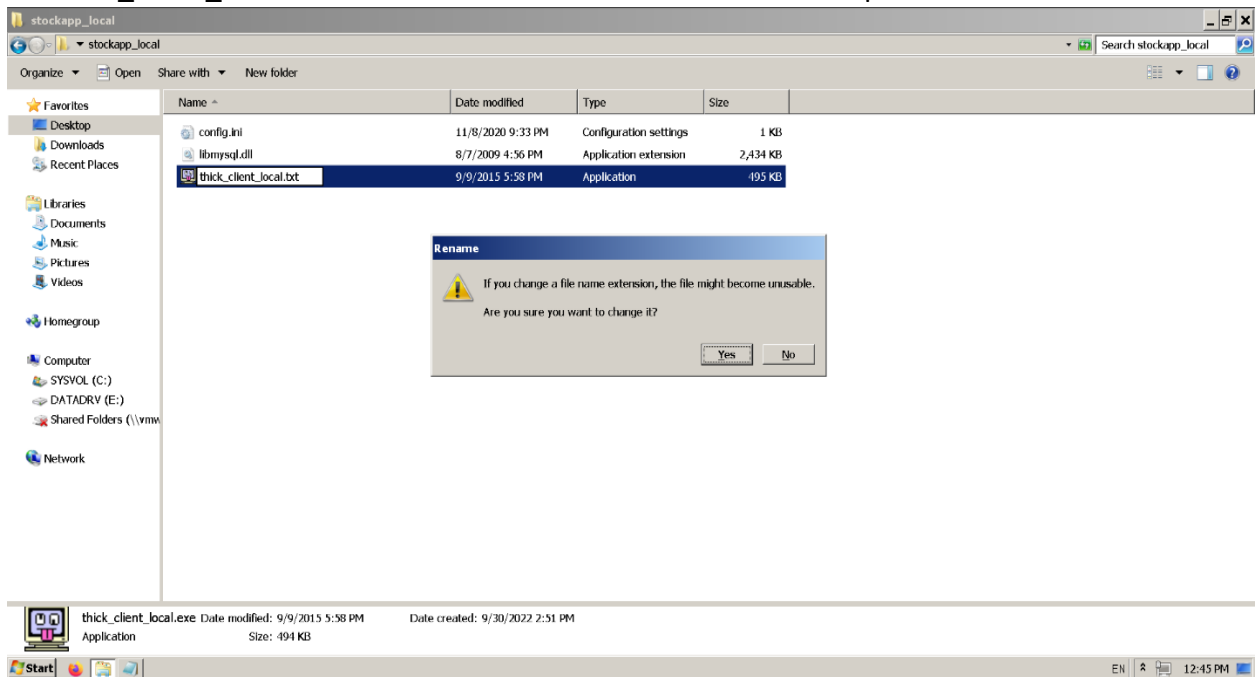
[AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H](https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H&version=3.1)

### **2.3 Description:**

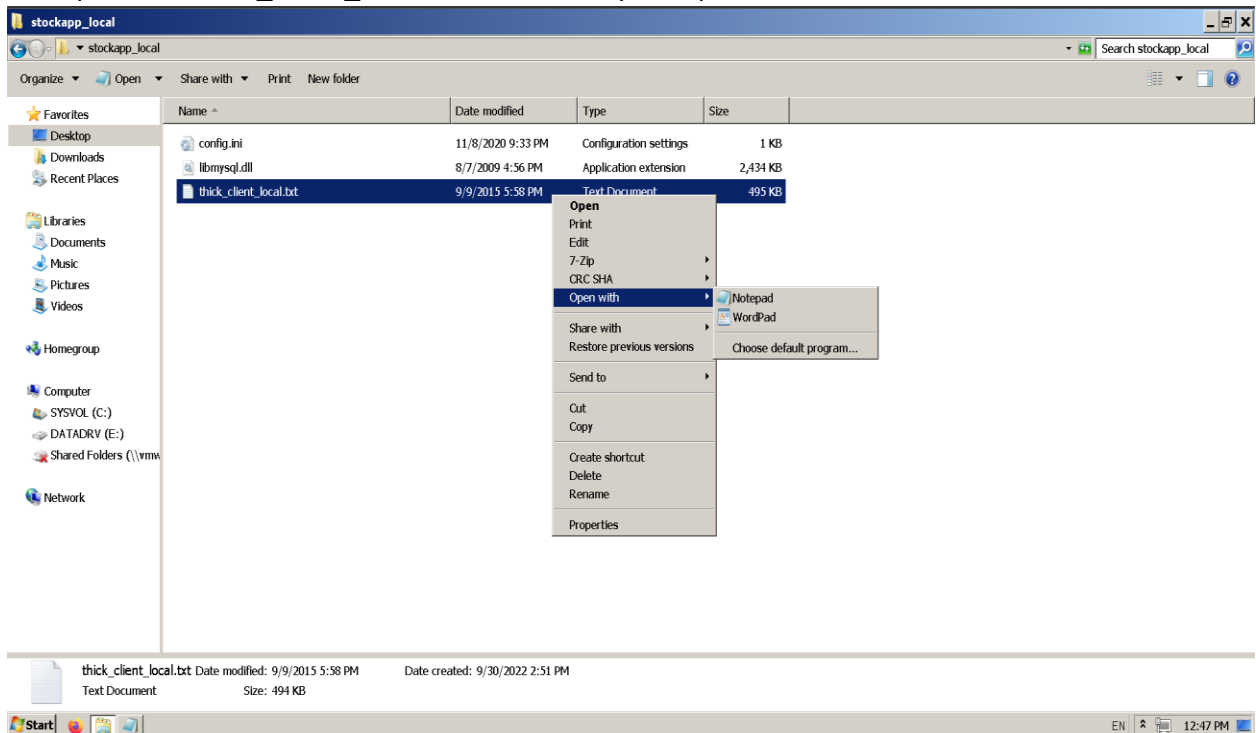
This password is retrieved using notepad or any text editor since it is hardcoded. Attackers can easily unlock the application and exploit it. Anyone has access to the PC will be able to access this file as do not have any access restrictions to the app folder access.

## 2.4 Exploitation:

- Launch the Stock app application folder and rename the thick\_client\_local.exe in thick\_client\_local.txt. For the file name extension click “YES” option.

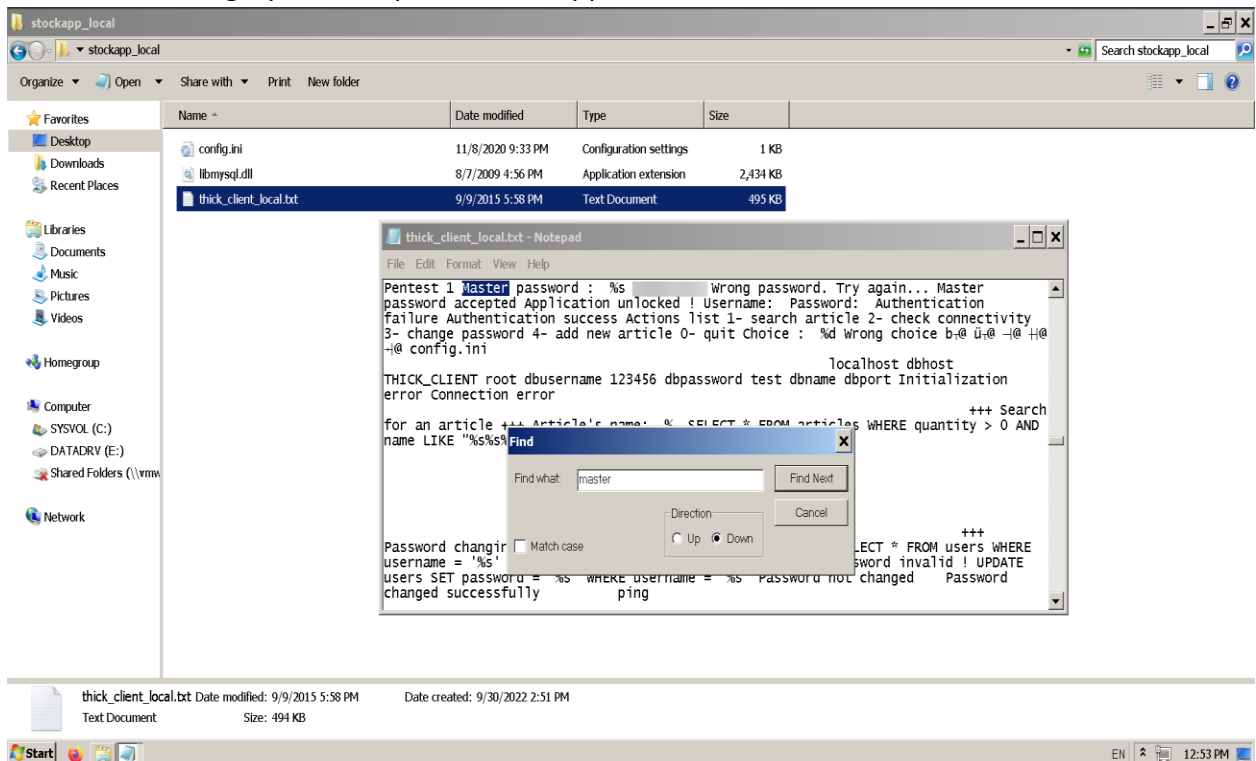


- Open that thick\_client\_local.txt file with any notepad or WordPad.





- Search “Master” password in that text editor. Master password is being hardcoded as below in the gray marked place in this application executable file.



## 2.5 Recommendations:

- Application password is better to be hashed.
- The access of the application folder needs to be limited, make sure only for the authorized group of people can access it.
- To open the application Master password can be used and again for the authentication use user name and password and this log in authentication need to be very strong.
- For strong password protection yescryptp can be used for encryption. It is the most scalable password hashing scheme.
- Read more: <https://www.openwall.com/yescrypt/>

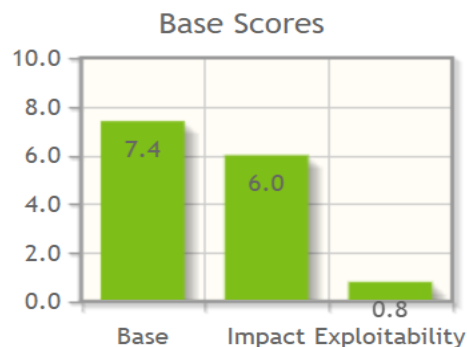
### 3. Password in cleartext in the configuration file:

#### 3.1 CWE-260: Password in Configuration File:

<https://cwe.mitre.org/data/definitions/260.html>

#### 3.2 Base Score Metrics :

- Risk Level:High
- <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:L&version=3.1>



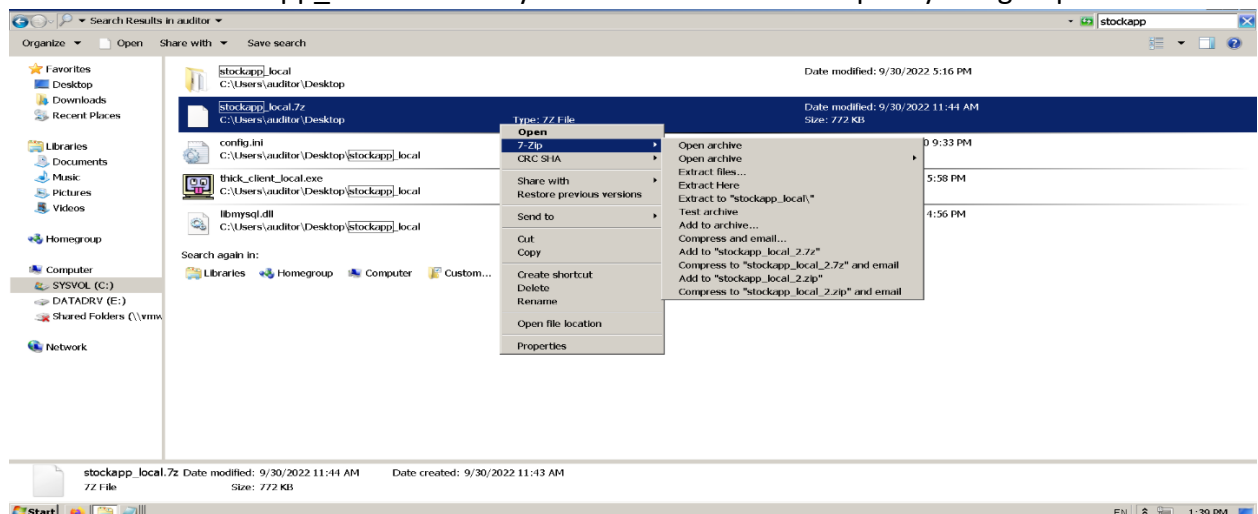
[AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:L](https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:L&version=3.1)

#### 3.3 Description:

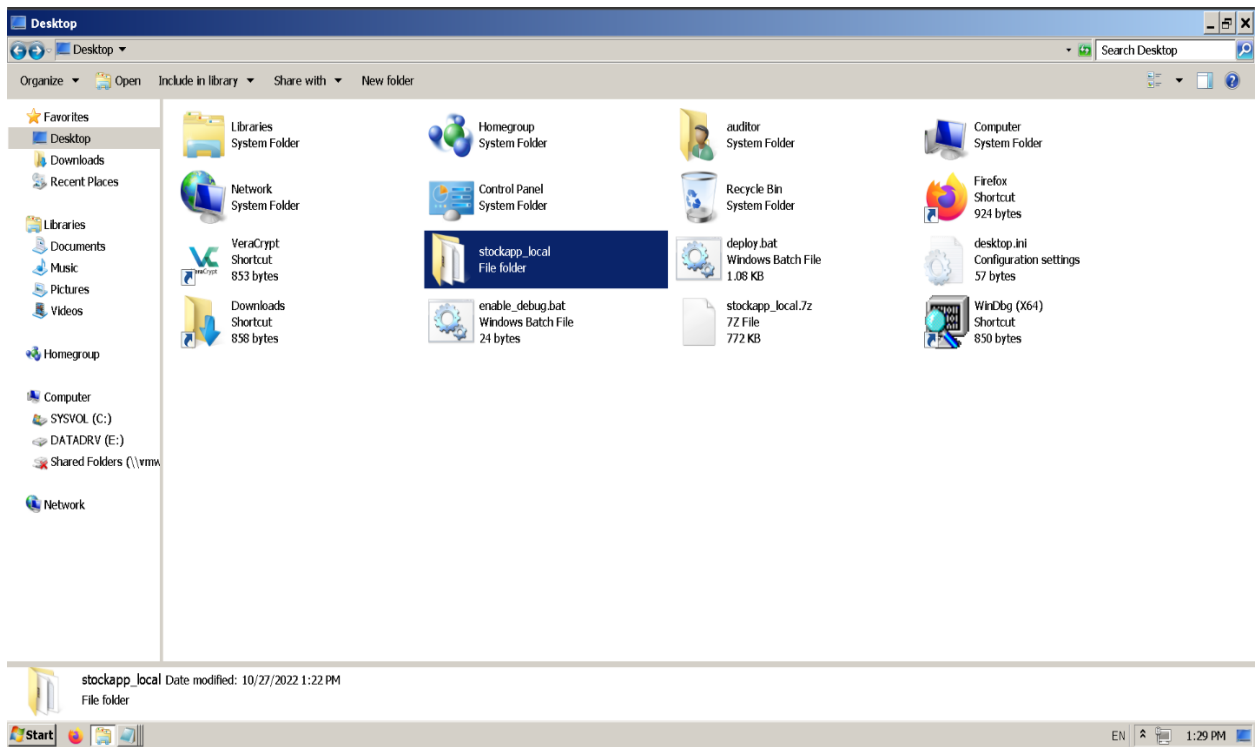
Database credentials are stored in the configuration file (config.ini) in plain text format. An attacker with access to the stock app can quickly discover the password and username. They may be able to change the account and password.

#### 3.4 Exploitation:

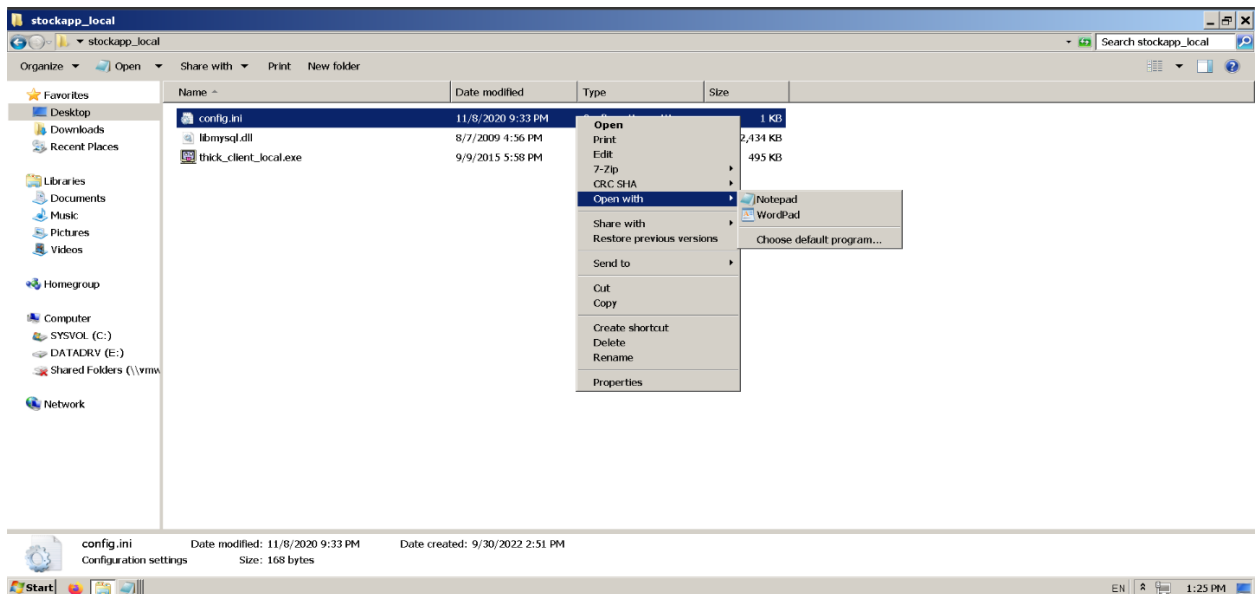
- Download stockapp\_local.7z file to your workstation and unzip it by using 7zip.



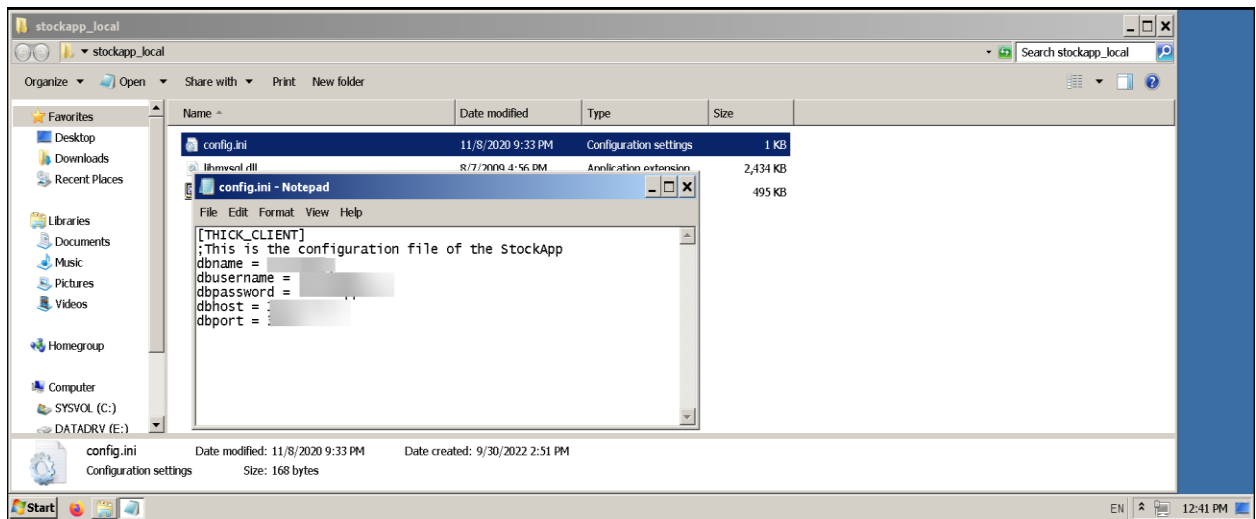
- Open the stockapp\_local folder.



- Open config.ini file from stockapp\_local folder in any text editor.



- Database credentials are in the configuration file and password is in plaintext format.



### 3.5 Recommendations:

- Disabling the default method of password saving.
- Keep password in a secret file in encrypted format and deploy secret file in secured environment.
- Encrypt password by using yescrypt or SRP protocol.
- Provide application folder access to specific user group, could be controlled via Azure AD/LDAP sync.
- Read More: <https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-application-management>

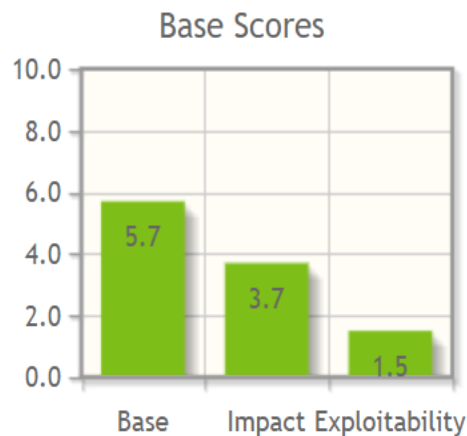
## **4. Passwords stored in cleartext within the database:**

### **4.1 CWE-312: Cleartext Storage of Sensitive Information:**

<https://cwe.mitre.org/data/definitions/312.html>

### **4.2 Base Score Metrics :**

- Risk Level:Medium
- <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:L&version=3.1>



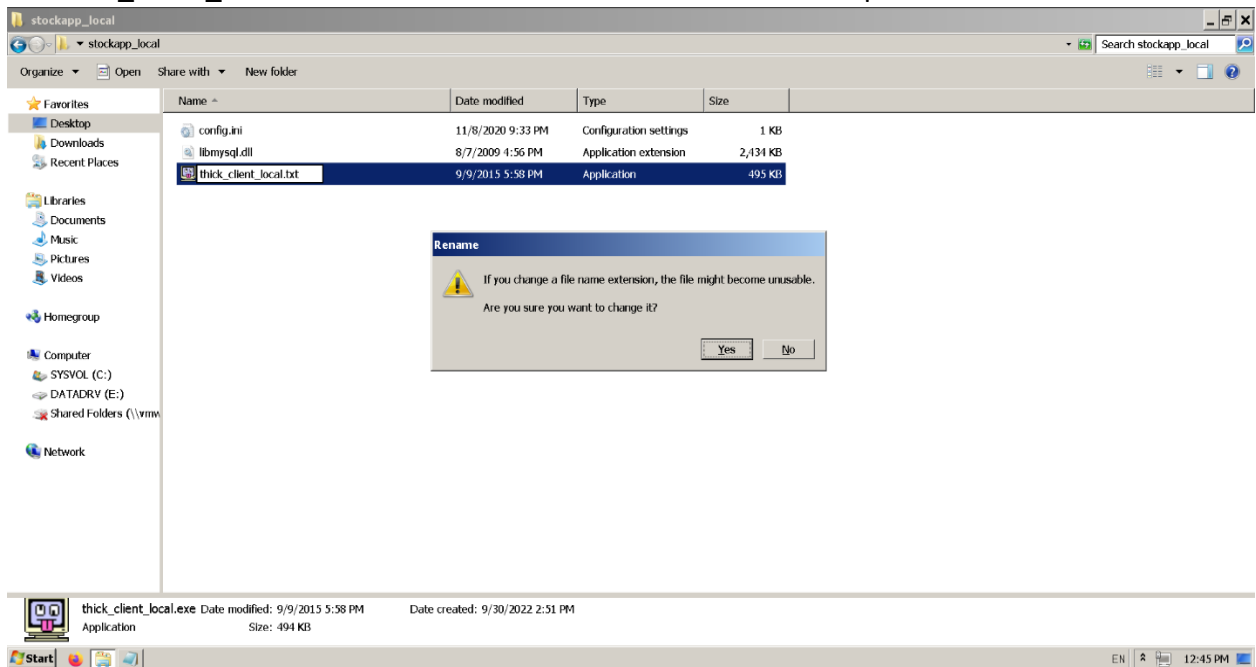
[AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:L](https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:L&version=3.1)

### **4.3 Description:**

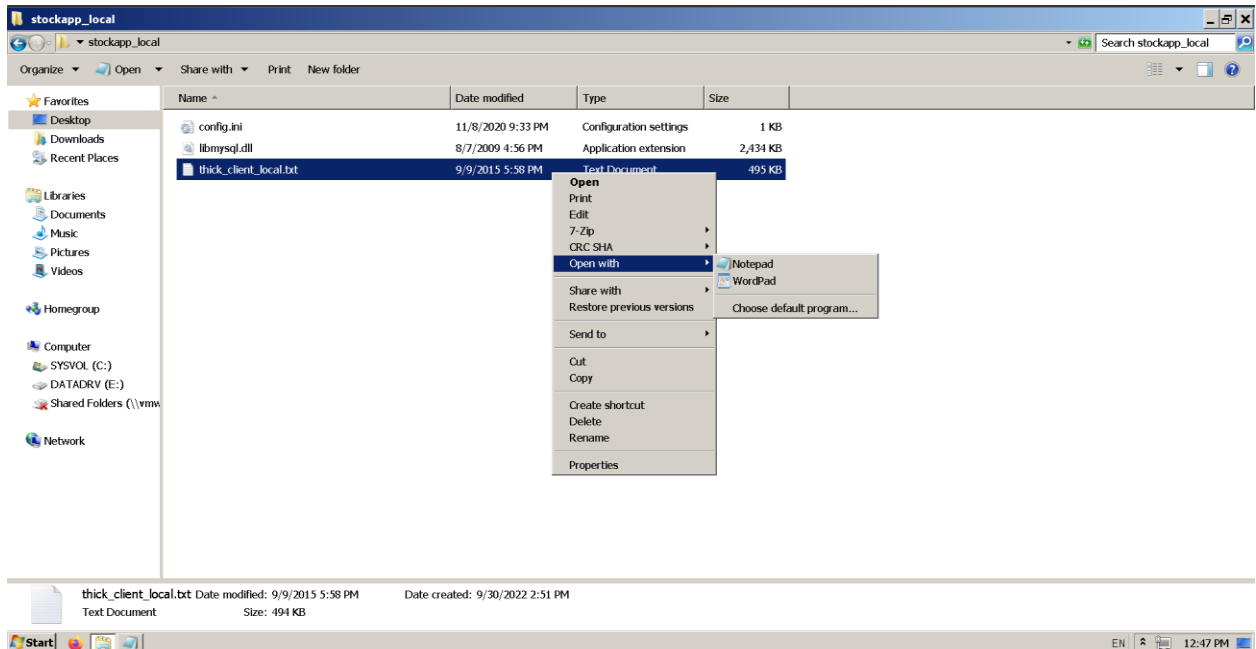
The SQL queries used by the application are visible in cleartext view within the executable file. This kind of information allows the attacker to do SQL Injection and make changes in database.

## 4.4 Exploitation:

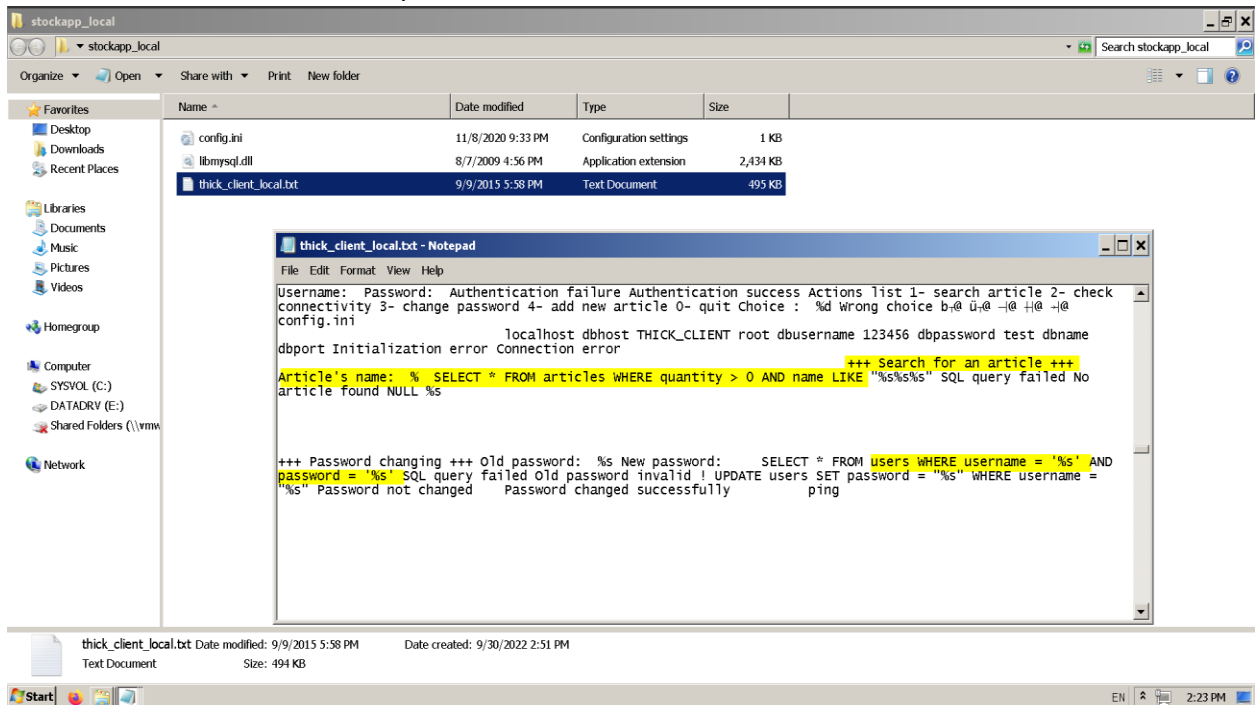
- Launch the Stock app application folder and rename the thick\_client\_local.exe in thick\_client\_local.txt. For the file name extension click “YES” option.



- Open that thick\_client\_local.txt file with Notepad or WordPad.



- In the text editor, the SQLqueries are visible in clear text.



#### 4.5 Recommendations:

- All the sensitive data should be first encrypted first before uploading in the databases like this executable files should be encrypted first.
- Some encrypted software like ArmDot, Crypto obfuscator like those can be used for making the executable file encrypted.
- Hashing algorithms can be used to fix this vulnerability. Hashing algorithms transform the input and produce a fixed size fingerprint hash.
- Read more: <https://www.titanfile.com/blog/22-best-practices-for-protecting-data-privacy-in-2022-infographic/>

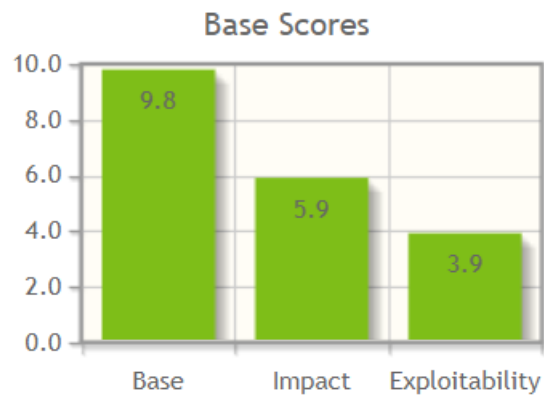
## **5. Arbitrary system commands injection:**

### **5.1 CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection'):**

<https://cwe.mitre.org/data/definitions/77.html>

#### **5.2: Base score Metrics:**

- Risk Level:Critical
- [NVD - CVSS v3 Calculator \(nist.gov\)](#)



AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

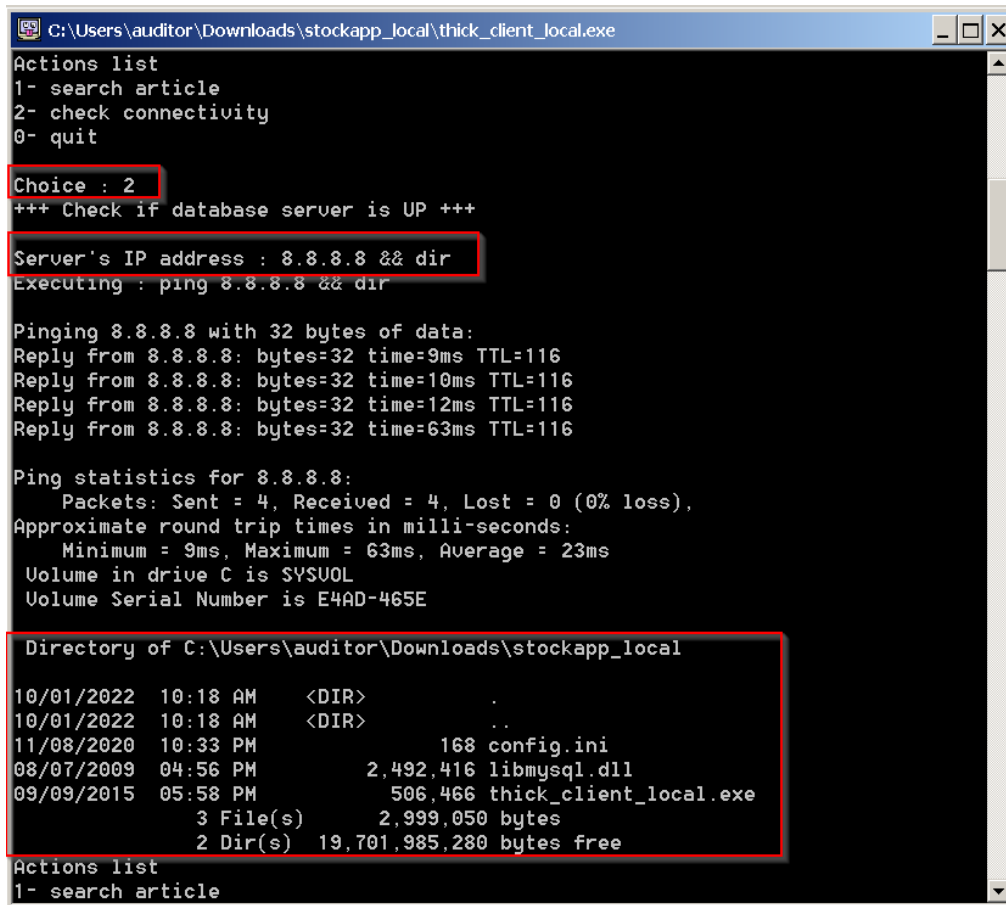
#### **5.3: Description:**

If application is failed to sanitize between normal commands and OS commands then there will be a possibility of OS command injection. This type of vulnerability can be exploited by anyone with basic knowledge



## 5.4: Exploitation:

- Login to the StockApp as agent
- Enter number 2 to check the connectivity
- Enter IP address and OS commands like DIR (8.8.8.8 && dir)
- By entering && we are merging the commands to run together as single command



```
C:\Users\auditor\Downloads\stockapp_local\thick_client_local.exe
Actions list
1- search article
2- check connectivity
0- quit
Choice : 2
+++ Check if database server is UP +++
Server's IP address : 8.8.8.8 && dir
Executing : ping 8.8.8.8 && dir

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=9ms TTL=116
Reply from 8.8.8.8: bytes=32 time=10ms TTL=116
Reply from 8.8.8.8: bytes=32 time=12ms TTL=116
Reply from 8.8.8.8: bytes=32 time=63ms TTL=116

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 63ms, Average = 23ms
    Volume in drive C is SYSUOL
    Volume Serial Number is E4AD-465E

Directory of C:\Users\auditor\Downloads\stockapp_local

10/01/2022  10:18 AM    <DIR>          .
10/01/2022  10:18 AM    <DIR>          ..
11/08/2020  10:33 PM                168 config.ini
08/07/2009  04:56 PM           2,492,416 libmysql.dll
09/09/2015  05:58 PM           506,466 thick_client_local.exe
               3 File(s)          2,999,050 bytes
               2 Dir(s)         19,701,985,280 bytes free

Actions list
1- search article
```

In the above screenshot we see we selected chose 2 – Given IP address as Google DNS servers 8.8.8.8 and OS command DIR. First it run the ping and show the results then it ran DIR command and reviled directories of the application server.

## 5.5: Remediation:

- Always check what user is providing
- Only allow whitelisted characters and numbers
- Don't allow any special characters
- Don't allow spaces

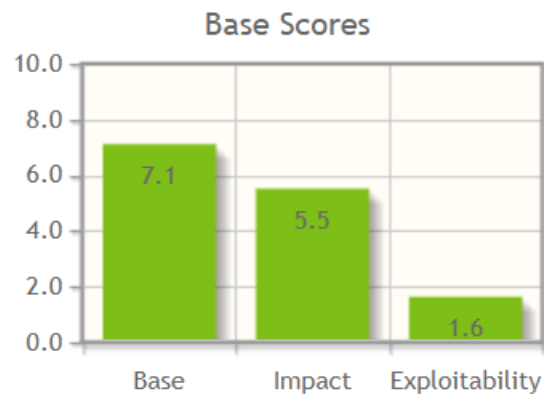
## **6.Bad profiles segregation:**

### **6.1 Improper Handling of Insufficient Privileges:**

[CWE - CWE-274: Improper Handling of Insufficient Privileges \(4.9\) \(mitre.org\)](#)

### **6.2 Base score Metrics:**

- Risk Level:High
- [NVD - CVSS v3 Calculator \(nist.gov\)](#)



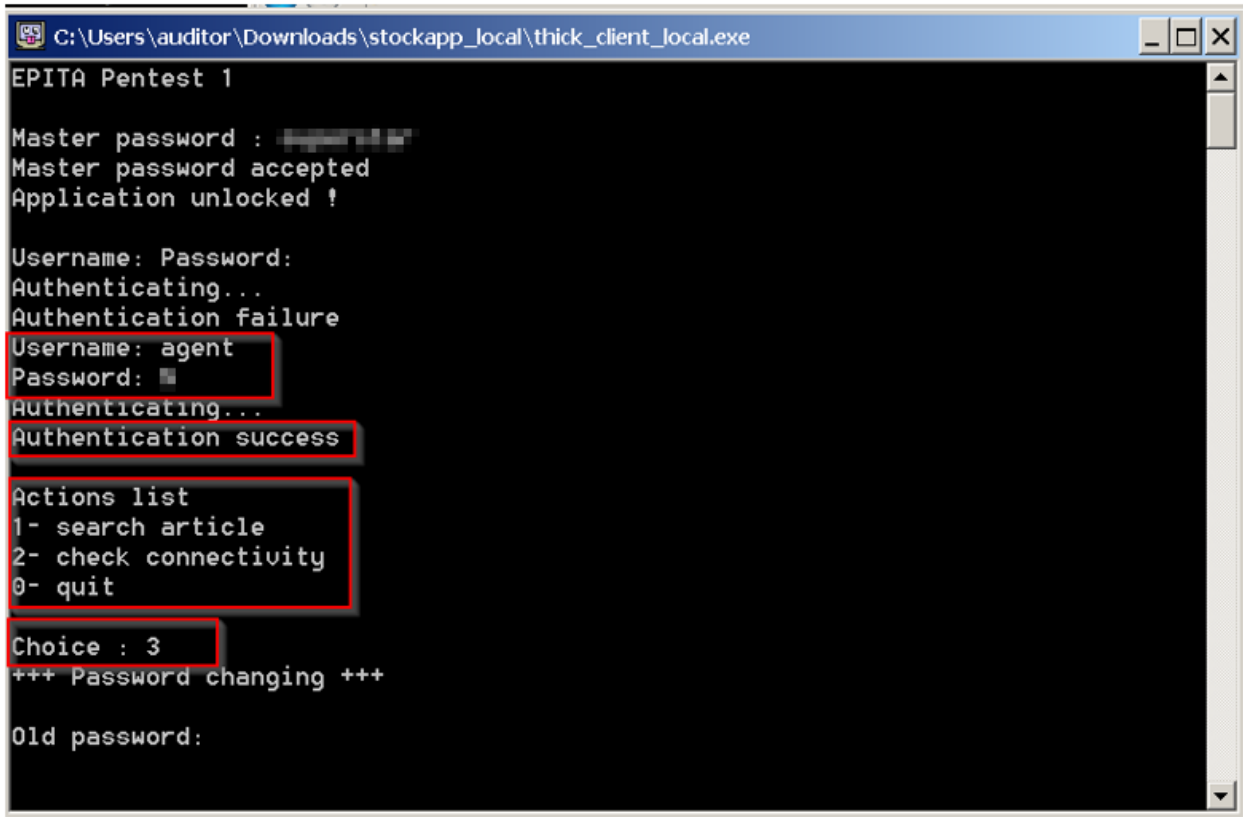
AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:L

### **6.3 Description:**

Access control are not in places for the application. Due to that admin action can be done by non-admin users and privileges which are not required need to be removed

## 6.4 Exploitation:

- Login to the Stockapp as agent
- Here we see only few numbers like 1,2,0
- Now enter number 3 which is not visible and this is a admin only action
- We see password changed even action (number 3) is not visible



```
C:\Users\auditor\Downloads\stockapp_local\thick_client_local.exe
EPITA Pentest 1

Master password : [redacted]
Master password accepted
Application unlocked !

Username: Password:
Authenticating...
Authentication failure
Username: agent
Password: [redacted]
Authenticating...
Authentication success

Actions list
1- search article
2- check connectivity
0- quit

Choice : 3
+++ Password changing +++

Old password:
```

In the above screenshot, number 3 is not shown but after entering 3 it is allowing us to change the password.

## 6.5 Remediation:

- Access control need to be in place
- Give least privileges unless it required

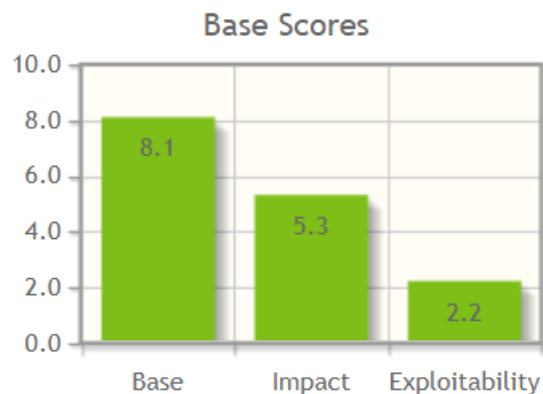
## **7.Secrets present in memory even when not needed:**

### **7.1 Cleartext Storage of Sensitive Information in Memory:**

[CWE - CWE-316: Cleartext Storage of Sensitive Information in Memory \(4.9\) \(mitre.org\)](#)

### **7.2 Base score Metrics:**

- Risk Level: High
- [https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?calculator&version=3.0&vector=\(AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N\)](https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?calculator&version=3.0&vector=(AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N))



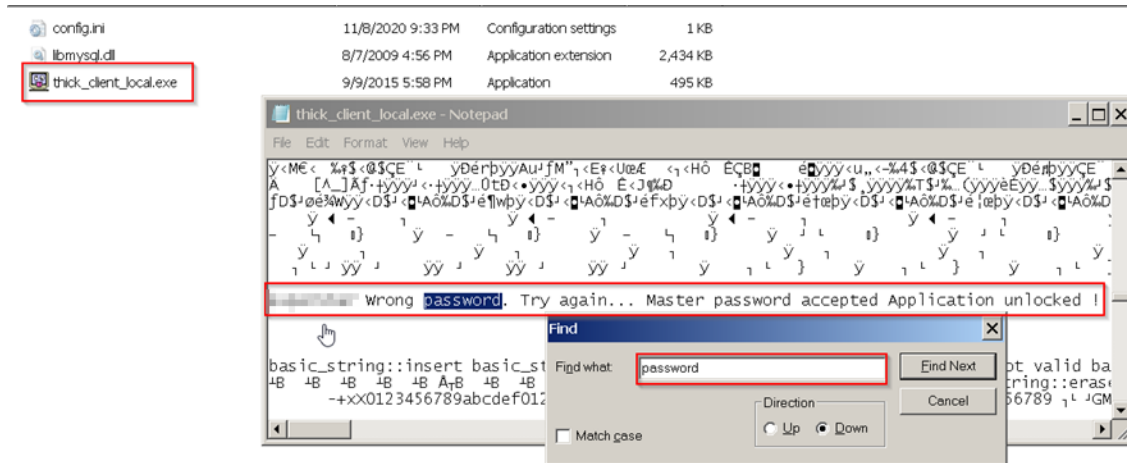
AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:L/A:L

### **7.3 Description:**

In the memory of the application master password is present and by this an attacker can able to use this to take complete control of the application. When we open thick client application using notepad and search using password master password is reveling.

## 7.4 Exploitation:

- Go to thickclient windows folder and open thickClient using Notepad
- Here you see a lot of junk information
- Ctrl +F to search by keyword “Password” you see password is visible in cleartext



In the above screenshot we see password is visible in the cleartext

## 7.5 Remediation:

- Ensure no password or any sensitive information is placed in the application in cleartext
- Use encryption to secure passwords

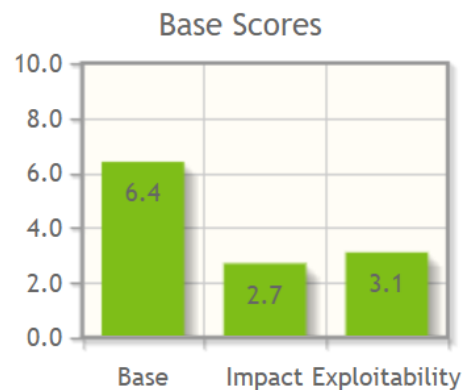
## **8.Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')**

### **8.1 CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')**

<https://cwe.mitre.org/data/definitions/89.html>

#### **8.2 Base Score Metrics:**

- Risk Level: High
- <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N&version=3.1>



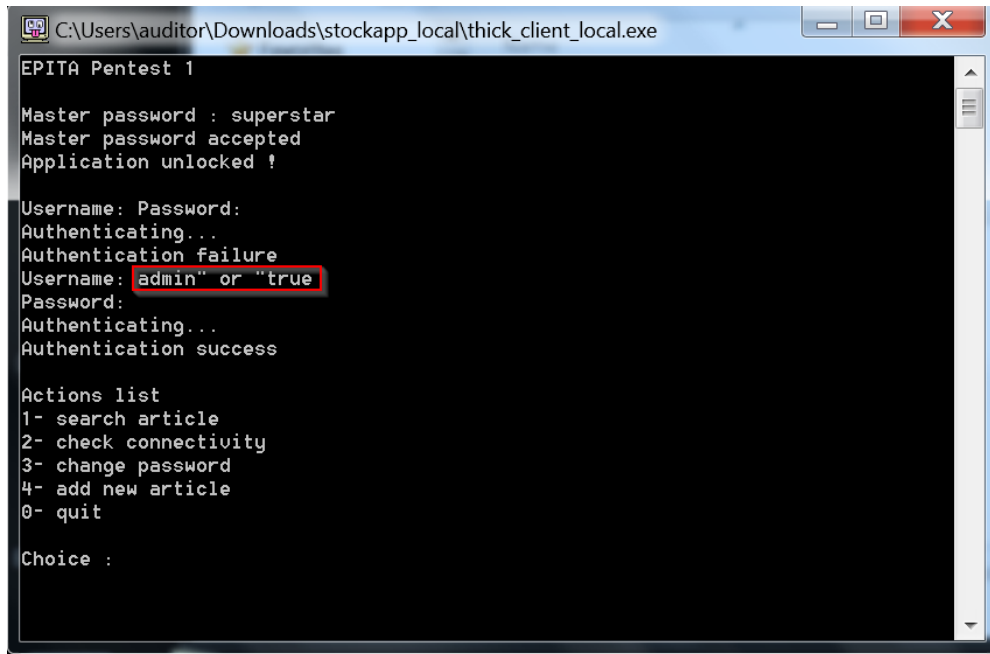
[AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N](https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N&version=3.1)

#### **8.3 Description:**

The software constructs all or part of an SQL command using externally influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.

## 8.4 Exploitation:

- Launch the stock app



```
C:\Users\auditor\Downloads\stockapp_local\thick_client_local.exe
EPITA Pentest 1
Master password : superstar
Master password accepted
Application unlocked !
Username: Password:
Authenticating...
Authentication failure
Username: admin" or "true
Password:
Authenticating...
Authentication success
Actions list
1- search article
2- check connectivity
3- change password
4- add new article
0- quit
Choice :
```

- Enter master password for unlock application.
- For the username use following input: **admin" = "true**
- For the password enter anything or without enter anything(blank)
- Then authentication success.

## 8.5 Recommendations:

- Use of Prepared Statements (with Parameterized Queries)
- Use of Properly Constructed Stored Procedures
- Allow-list Input Validation
- Escaping All User Supplied Input
- Reference  
[https://cheatsheetseries.owasp.org/cheatsheets/SQL\\_Injection\\_Prevention\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html)

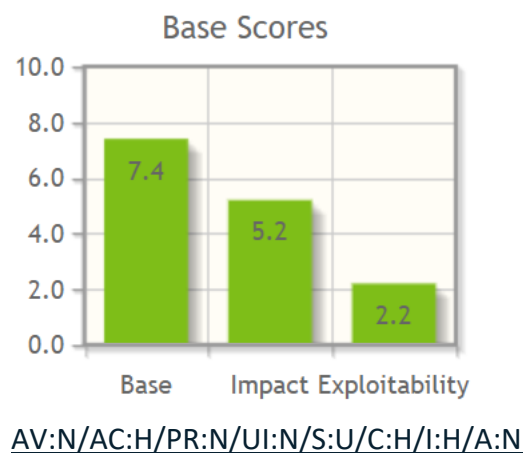
## **9. Network traffic not encrypted:**

### **9.1 CWE-523: Unprotected Transport of Credentials**

<https://cwe.mitre.org/data/definitions/523.html>

#### **9.2 Base Score Metrics:**

- **Risk Level : High**
- <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N&version=3.1>



#### **9.3 Description:**

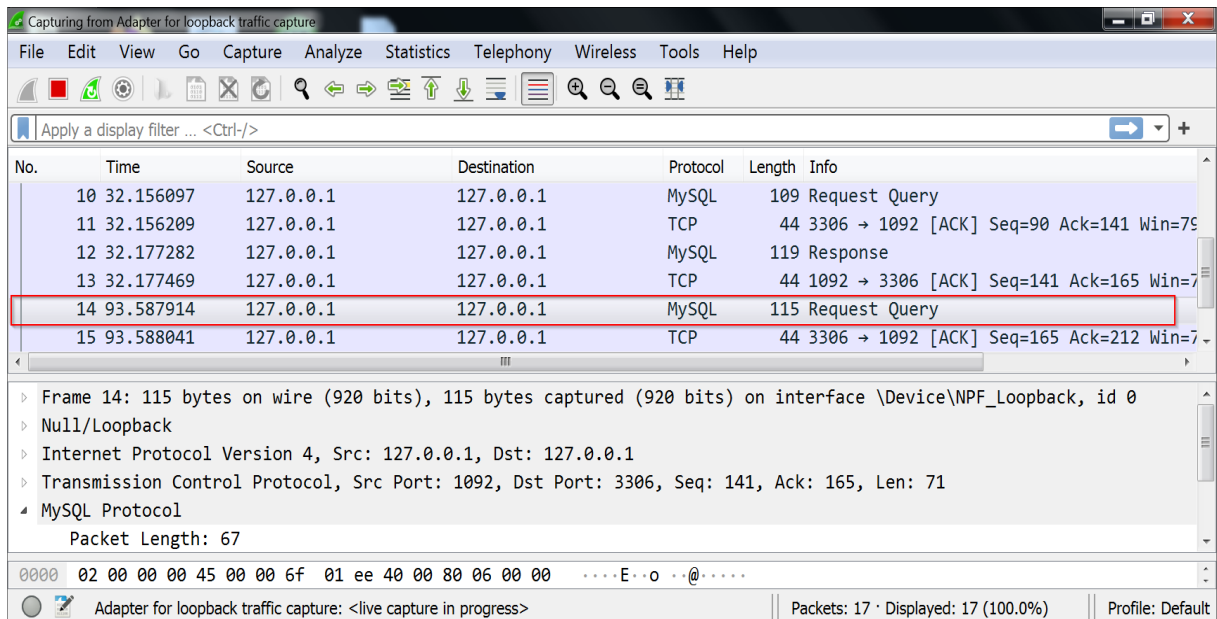
Login pages do not use adequate measures to secure the username and password while they are in transport from the client to the server. The attacker can monitor network traffics and they can steal the user credentials.

#### **9.4 Exploitation**

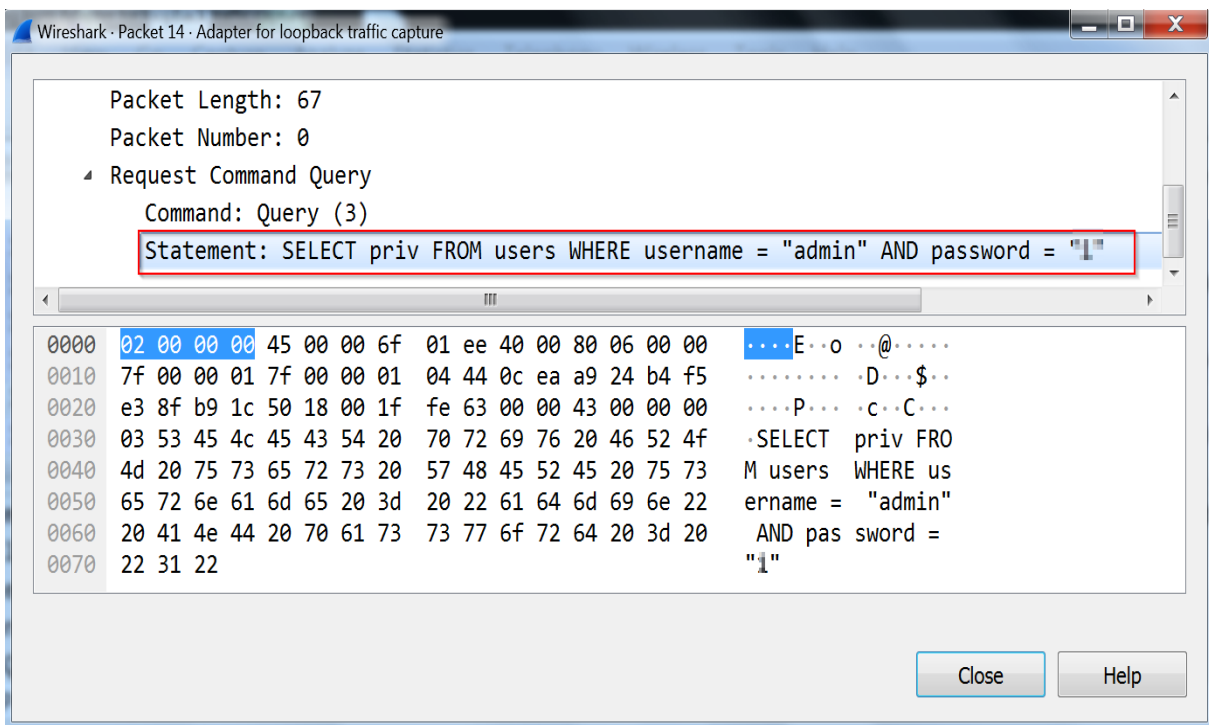
1. Launch Wireshark and right click on Adapter for loopback traffic capture and start capture.
2. Then launch thick\_client\_local application.
3. Login to stockapp with username and password.



4. Click on the protocol that contains MySQL. (Request query)



5. Then Username and password will be visible.



## 9.5 Recommendations:

- using hashed passwords over the transport
- Use certificates signed by a trusted CA provider.
- Use strong, industry standard cipher suites with appropriate key lengths.
- Encrypted Connection TLS Protocols and Ciphers.
- Reference <https://dev.mysql.com/doc/mysql-security-excerpt/5.7/en/encrypted-connections.html>

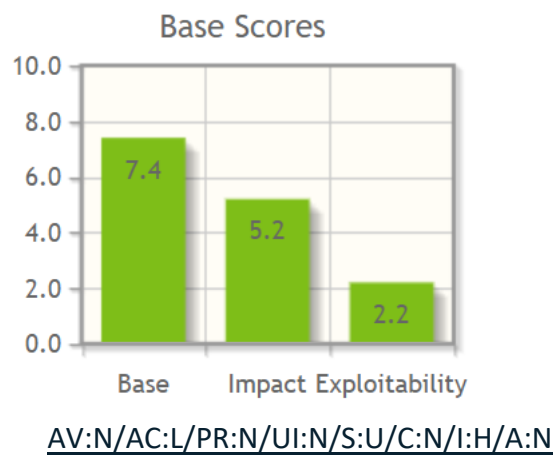
## **10. Weak passwords accepted:**

### **10.1 CWE-521: Weak Password Requirements**

<https://cwe.mitre.org/data/definitions/521.html>

### **10.2 Base Score Metrics:**

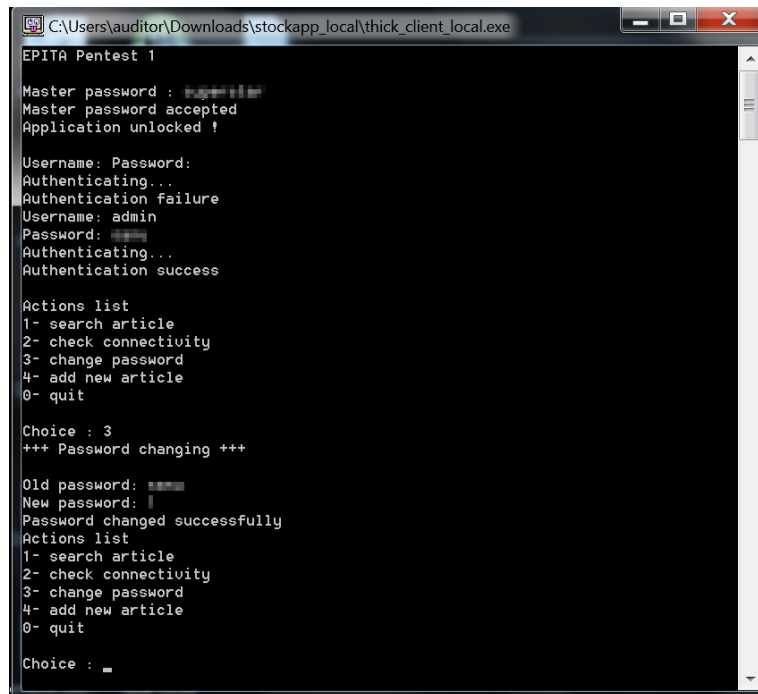
- Risk level: High
- <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N&version=3.1>



### **10.3 Description:**

The product does not require that users should have strong passwords, which makes it easier for attackers to compromise user accounts.

## 10.4 Exploitation:



```
C:\Users\auditor\Downloads\stockapp_local\thick_client_local.exe
EPITA Pentest 1

Master password : ****
Master password accepted
Application unlocked !

Username: Password:
Authenticating...
Authentication failure
Username: admin
Password: ****
Authenticating...
Authentication success

Actions list
1- search article
2- check connectivity
3- change password
4- add new article
0- quit

Choice : 3
+++ Password changing +++

Old password: ****
New password: 1
Password changed successfully
Actions list
1- search article
2- check connectivity
3- change password
4- add new article
0- quit

Choice : 1
```

- 1.Launch stockapp and while enter passwords it accepts weak passwords.
- 2.While changing the password it accepts just 1-digit character also.

## 10.5 Recommendations:

- Use long passwords include special characters, lowercase, uppercase, numbers (mixed characters)
- Can specify the following standards and other rules for passwords:
  - Minimum and maximum length
  - Character restrictions
  - Frequency of password reuse
  - Disallowed usernames or user IDs
  - Specify a minimum password age
- Reference <https://www.ibm.com/docs/en/spim/2.0.0?topic=administration-password-policies>