

Hard Coded Password in code – not a good practice

1. כל מי שרואה את הקוד רואה את הסיסמה
2. הסיסמה דולפת ל Git כששומרים את הקוד
3. אי אפשר להחליף סיסמה בלי לקמפל את הקוד מחדש
4. סיכון אבטחה חמור לפי OWASP (Open Web Application Security) Project שהוא ארגון בינלאומי ללא מטרות רווח שמתמקד באבטחת אפליקציות תוכנה)

דוגמה לא טובה – סיסמה בקוד

1. `string user = "abc@gmail.com";`
2. **`string pass = "abcd1234";`**
3. `SmtplibClient smtp = new SmtplibClient(...);`
4. `smtp.Credentials = new NetworkCredential(user, pass);`
5. ✓ קל מידי לגנוב את הסיסמה

פתרון 1 - הכנסת סיסמה ב TextBox בצורה מוסתרת

1. המשתמש מכניס סיסמה בזמן ריצה
 2. יתרונות: הסיסמה לא נשמרת בשום קובץ וניתן לשנות את הערך בזמן ריצה מבלי לקמפל מחדש את הקוד
 3. חסרונות: המשתמש צריך להקליד כל פעם (מתאים יותר לסיסמת כניסה למערכת)
 4. דוגמה:
- ```
textBoxPass.PasswordChar = '*'; //masking can be done in properties also
```
- 
- ```
string pass = textBoxPass.Text; //get the password entered by the user
```

פתרון 2 – משתנה סביבה Environment Variable

1. מוגדר כמשתנה סביבה במערכת ההפעלה של המחשב
2. יתרונות: לא נמצא בקוד ולא ב GIT וניתן לשנות אותו מבלי לקמפל מחדש את הקוד
3. חסרונות: יש צורך להגדיר ידנית בכל מחשב שרצה עליו התוכנה אבל מבחינת אבטחה מומלץ ע"י OWASP

פתרון 2 – משתנה סביבה Environment Variable

הוספת משתנה סביבה חדש:

1. לחץ Start

2. חפש: Edit the system environment variables

3. בחלון → לחץ על: ...Environment Variables

תראה שני אזורים:

- User variables (למשתמש הנוכחי בלבד)
- System variables (לכל המשתמשים — דורש אדמין)

4. לחץ New...

5. מלא:

• *Variable name*:

APP_PASS

• *Variable value*:

לדוגמה: abcd1234

6. שמור → OK

⚠ לאחר השמירה לפעמים צריך להפעיל מחדש את Visual Studio כדי שהמשתנה ייקלט.

פתרון 2 – משתנה סביבה Environment Variable

טעינת משתנה הסביבה לקוד של C#:

```
string pass = Environment.GetEnvironmentVariable("APP_PASS");  
if (string.IsNullOrEmpty(pass))  
{  
    MessageBox.Show("Environment variable APP_PASS is not set!");  
}
```

פתרון 3 – App.Config

1. זה קובץ הגדרות (קונפגורציה) שנשמר ליד האפליקציה (ב bin)
2. יתרונות: ניתן לשנות אותו בצורה נוחה מבלי לקמפל מחדש את הקוד
3. חסרון: הסיסמה גלויה אם לא מוצפנת ולכן מסוכן להכניס ל GIT
4. ניתן להכניס ל GIT בלי בעיה אם לא מדובר במידע רגיש
5. ניתן לשמור בו מידע רגיש בתנאי שלא שומרים את הקובץ ב GIT ע"י הוספת App.config לקובץ .gitignore. ואז App.config לא ישמר ב GIT
6. במקרה שהקובץ לא נשמר ב git כדאי להכניס ל GIT את הקובץ App.sample.config שהוא בעצם template (<add key="APP_PASS" value="REPLACE_ME"/>) שצריך לשנות לו את השם ל App.config ולעדכן בו את ה value הנכון

פתרון 3 – App.Config

הוספת Item חדש (key/value) ל App.config:

אם הקובץ לא קיים, מוסיפים חדש לפרויקט:

Right-click project → **Add** → **New Item** → *Application Configuration File*

לאחר מכן מוסיפים סקשן appSettings ומוסיפים Item חדש (key/value):

```
<?xml version="1.0" encoding="utf-8" ?>
```

```
<configuration>
```

```
  <appSettings>
```

```
    <add key="APP_PASS" value="abcd1234" />
```

```
  </appSettings>
```

```
</configuration>
```


פתרון 3 – App.Config

טעינת value לפי key מה- App.config מתוך קוד C#:

```
using System.Configuration;
string pass = ConfigurationManager.AppSettings["APP_PASS"];
if (string.IsNullOrEmpty(pass))
{
    MessageBox.Show("Key 'APP_PASS' not found in App.config");
}
```

פתרון 4 – שמירת הסיסמה בצורה מוצפנת בתוך קובץ או DB

1. הסיסמה נשמרת מוצפנת בתוך קובץ או DB
2. הכי בטוח מקומית
3. דורש הצפנה ופיענוח. דורש ניהול מפתחות לפעמים
4. נראה בהמשך

השוואה בין השיטות

1. TextBox with mask - הכי בטוח מצד אחסון אבל לא נוח לסיסמאות ארוכות שאי אפשר לזכור (כמו App_PASS).
2. Environment Variable - מאובטח יחסית, כי זה הגדרות פיר מחשב.
3. App.config - נוח לשינויים, אבל מסוכן כששומרים מידע רגיש (במקרה של מידע רגיש עדיף לא לשמור ב GIT).
4. Encryption - הכי מאובטח אבל הכי מורכב. נראה בהמשך.

תרגיל

תקן את התרגיל הקודם שבו שמרת APP_PASS בצורת Hard Coded בקוד, כך שיהיה ניתן לשלוף את הסיסמה לפי התנאים הבאים:

1. טעינת הסיסמה מהמשתמש ע"י TextBox with masking.
2. במידה והסיסמה לא הוזנה ע"י המשתמש טען אותה ממשתנה סביבה בשם APP_PASS.
3. במידה והסיסמה לא קיימת במשתנה סביבה טען אותה מתוך קובץ App.config.
4. במידה והסיסמה לא הוזנה בשום שלב, הצג הודעה מתאימה. במידה והצלחת לשלוף את הסיסמה המשך את הקוד כרגיל ושלח את המיל.