Vulnerability Report for Access Control Issues – Part 3 in DIVA Application

- **Title:** Vulnerability Report for Access Control Issues – Part 3 in DIVA Application

- **Severity:** Critical

- **Description:**

  The Diva application suffers from a critical access control issue where an attacker can bypass the PIN entry requirement and access sensitive credentials from outside the application. This vulnerability enables unauthorised users to retrieve sensitive information without the necessary authentication.

- **Impact:**

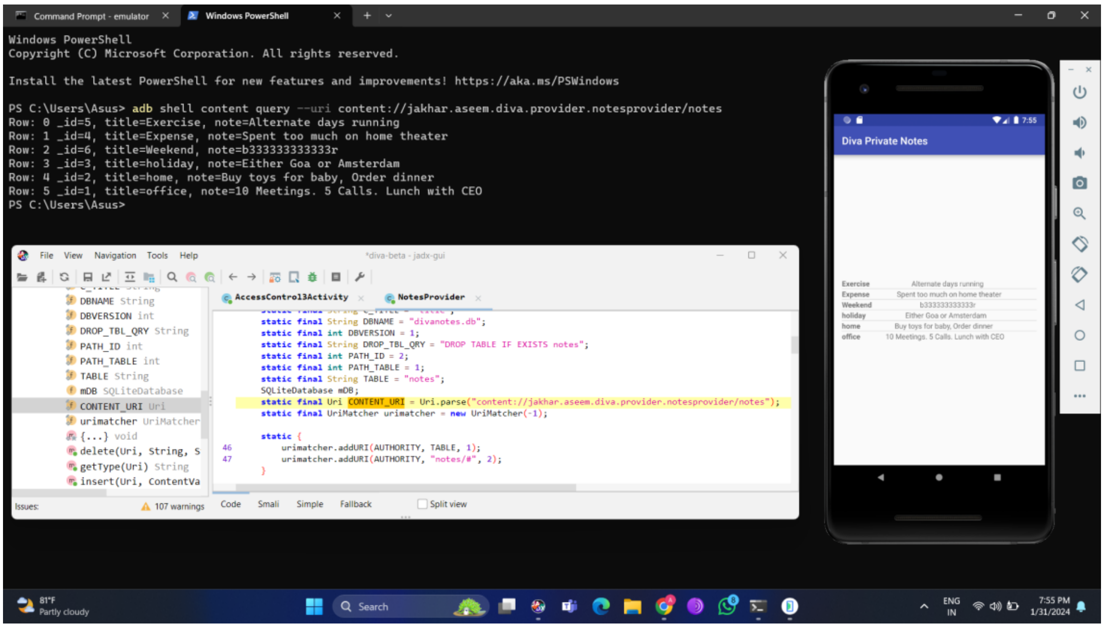
  1. Unauthorised Access: Attackers can access sensitive credentials without a PIN, compromising the security of user accounts.
  2. Data Leakage: The exposure of sensitive information through content URIs may lead to data leakage and potential misuse.
  3. Privacy Violation: Users' private information is at risk of unauthorised access and exploitation.

- **Steps to Reproduce:**

  1. Login to the application.
  2. Click on the “Access Control Issues – Part 3” option.
  3. Enter a pin number, eg: 1234, and click on the “Create/Change pin” button.
  4. Click on the “Go to Private Notes”. It asks for a pin to access the private notes.
  5. Close the application.
  6. Open the “diva-beta.apk” file in the jadx application.
  7. In jadx open the ‘jakhar.assem.diva’ folder, present in the ‘Source code’ folder.
  8. Open the “AccessControl3NotesActivity” file in the ‘Source code’ folder.
  9. The code states that the pin numbers are being provided by the content providers..
  10. Open the “NotesProvider” file present in the ‘Resources’ folder.

11. Search for “Content_URI” in the file and copy the URI.
12. Open the terminal/cmd and use the command “adb shell content query –uri content://<Content_URI>”.
13. This automatically opens the application and shows the credentials.

- **PoC (Proof of Concept):**



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Asus> adb shell content query --uri content://jakhar.aseem.diva.provider.notesprovider/notes
Row: 0 _id=5, title=Exercise, note=Alternate days running
Row: 1 _id=4, title=Expense, note=Spent too much on home theater
Row: 2 _id=6, title=Weekend, note=b333333333333r
Row: 3 _id=3, title=holiday, note=Either Goa or Amsterdam
Row: 4 _id=2, title=home, note=Buy toys for baby, Order dinner
Row: 5 _id=1, title=office, note=10 Meetings. 5 Calls. Lunch with CEO
PS C:\Users\Asus>
```

```java
    static final String DBNAME = "divanotes.db";
    static final int DBVERSION = 1;
    static final String DROP_TBL_QRY = "DROP TABLE IF EXISTS notes";
    static final int PATH_ID = 2;
    static final int PATH_TABLE = 1;
    static final String TABLE = "notes";
    SQLiteDatabase mDB;
    static final Uri CONTENT_URI = Uri.parse("content://jakhar.aseem.diva.provider.notesprovider/notes");
    static final UriMatcher urimatcher = new UriMatcher(-1);

    static {
        urimatcher.addURI(AUTHORITY, TABLE, 1);
        urimatcher.addURI(AUTHORITY, "notes/#", 2);
    }
```

- **Remediation:**

1. Implement Proper Access Controls: Review and enhance access controls to ensure that sensitive operations, like accessing credentials, require appropriate authentication, such as the PIN.

2. Use Secure Storage Mechanisms: Employ secure storage mechanisms that prevent unauthorised access, even when content URIs are known.

3. Encrypt Sensitive Data: Encrypt sensitive data, including credentials, to add an extra layer of protection against unauthorised access.

- **CWE (Common Weakness Enumeration):**

1. CWE-284: Improper Access Control
2. CWE-923: Improper Restriction of Communication to Log Files