# Vulnerability Report for Insecure Data Storage - Part 4 in DIVA Application

- **Title:** Vulnerability Report for Insecure Data Storage - Part 4 in DIVA Application
- **Severity:** Critical
- **Description:**

  The Diva application stores sensitive data, such as user credentials or personal information, in clear text within a file in external storage. This insecure data storage practice exposes critical information to potential unauthorised access.

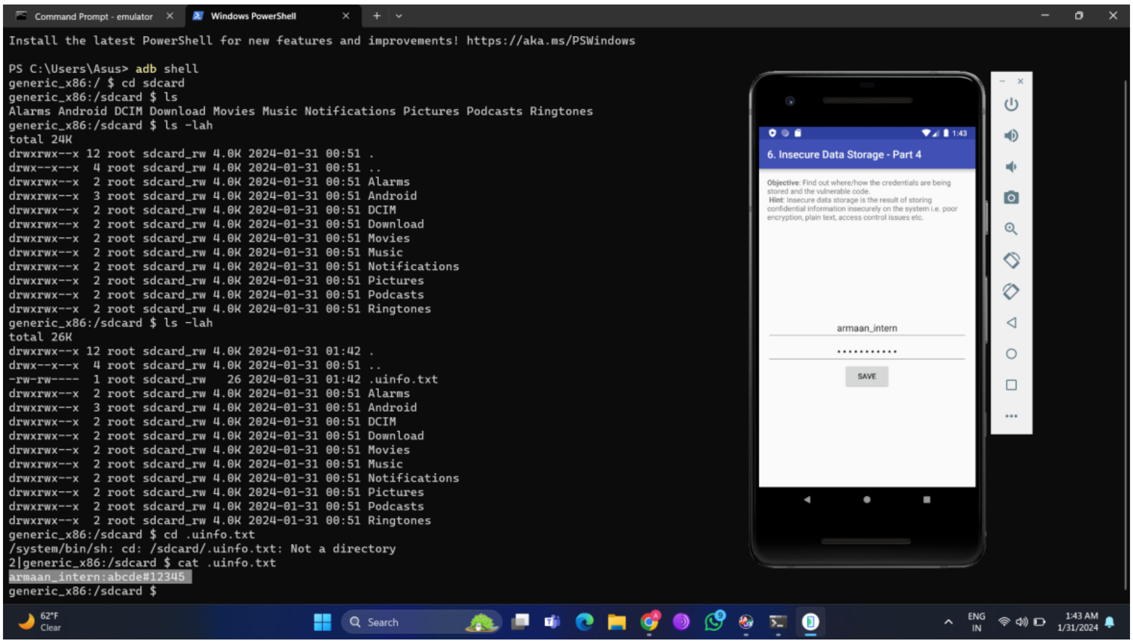
- **Impact:**

  1. Unauthorised Access: An attacker with access to the external storage can easily retrieve and exploit sensitive information.
  2. Credential Exposure: Usernames, passwords, or other authentication tokens stored in clear text are at risk of being compromised.
  3. Data Tampering: Malicious actors may manipulate stored data, leading to potential integrity issues.

- **Steps to Reproduce:**

  1. Login to the application.
  2. Click on the “Insecure Data Storage - Part 4” option.
  3. Enter the username and password in the application.
  4. Open the “diva-beta.apk” file in the jadx application.
  5. In jadx open the ‘jakhar.assem.diva’ folder, present in the ‘Source code’ folder.
  6. Search for ‘InsecureDataStorage4Activity’ file and open it.
  7. Observe that the code states that the username and password is saved as plain sensitive data in a file, in the external storage i.e sdcard.
  8. Open the terminal/cmd and type ‘cd sdcard’.
  9. List the contents of the sdcard by using the command ‘ls -lah’ to list all hidden files.
  10. Observe that the sdcard contains a hidden text file with the name similar to “.uinfo.txt”.
  11. Read this file by using the command ‘cat <file name>’.

- ## PoC (Proof of Concept):



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

PS C:\Users\Asus> adb shell
generic_x86:/ $ cd sdcard
generic_x86:/sdcard $ ls
Alarms Android DCIM Download Movies Music Notifications Pictures Podcasts Ringtones
generic_x86:/sdcard $ ls -lah
total 24K
drwxrwx--x 12 root sdcard_rw 4.0K 2024-01-31 00:51 .
drwx--x--x  4 root sdcard_rw 4.0K 2024-01-31 00:51 ..
drwxrwx--x  2 root sdcard_rw 4.0K 2024-01-31 00:51 Alarms
drwxrwx--x  3 root sdcard_rw 4.0K 2024-01-31 00:51 Android
drwxrwx--x  2 root sdcard_rw 4.0K 2024-01-31 00:51 DCIM
drwxrwx--x  2 root sdcard_rw 4.0K 2024-01-31 00:51 Download
drwxrwx--x  2 root sdcard_rw 4.0K 2024-01-31 00:51 Movies
drwxrwx--x  2 root sdcard_rw 4.0K 2024-01-31 00:51 Music
drwxrwx--x  2 root sdcard_rw 4.0K 2024-01-31 00:51 Notifications
drwxrwx--x  2 root sdcard_rw 4.0K 2024-01-31 00:51 Pictures
drwxrwx--x  2 root sdcard_rw 4.0K 2024-01-31 00:51 Podcasts
drwxrwx--x  2 root sdcard_rw 4.0K 2024-01-31 00:51 Ringtones
generic_x86:/sdcard $ ls -lah
total 26K
drwxrwx--x 12 root sdcard_rw 4.0K 2024-01-31 01:42 .
drwx--x--x  4 root sdcard_rw 4.0K 2024-01-31 00:51 ..
-rw-rw----  1 root sdcard_rw   26 2024-01-31 01:42 .uinfo.txt
drwxrwx--x  2 root sdcard_rw 4.0K 2024-01-31 00:51 Alarms
drwxrwx--x  3 root sdcard_rw 4.0K 2024-01-31 00:51 Android
drwxrwx--x  2 root sdcard_rw 4.0K 2024-01-31 00:51 DCIM
drwxrwx--x  2 root sdcard_rw 4.0K 2024-01-31 00:51 Download
drwxrwx--x  2 root sdcard_rw 4.0K 2024-01-31 00:51 Movies
drwxrwx--x  2 root sdcard_rw 4.0K 2024-01-31 00:51 Music
drwxrwx--x  2 root sdcard_rw 4.0K 2024-01-31 00:51 Notifications
drwxrwx--x  2 root sdcard_rw 4.0K 2024-01-31 00:51 Pictures
drwxrwx--x  2 root sdcard_rw 4.0K 2024-01-31 00:51 Podcasts
drwxrwx--x  2 root sdcard_rw 4.0K 2024-01-31 00:51 Ringtones
generic_x86:/sdcard $ cd .uinfo.txt
/system/bin/sh: cd: /sdcard/.uinfo.txt: Not a directory
2|generic_x86:/sdcard $ cat .uinfo.txt
armaan_intern:abcde#12345
generic_x86:/sdcard $
```

1:43

6. Insecure Data Storage - Part 4

**Objective**: Find out where/how the credentials are being stored and the vulnerable code.
**Hint**: Insecure data storage is the result of storing confidential information insecurely on the system i.e. poor encryption, plain text, access control issues etc.

armaan_intern

•••••••••••

SAVE

- ## Remediation:

  1. Encryption: Implement strong encryption algorithms to protect sensitive data before storing it in external storage.
  2. Key Management: Ensure secure key management practices to safeguard encryption keys.
  3. Secure File Permissions: Restrict access permissions for the file containing sensitive data to authorised entities only.
  4. Use Internal Storage: Whenever possible, store sensitive data in the application's internal storage, which is more secure than external storage.

- ## CWE (Common Weakness Enumeration):

  1. CWE-256: Plaintext Storage of a Password
  2. CWE-313: Cleartext Storage in a File or on Disk
  3. CWE-311: Missing Encryption of Sensitive Data