**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.

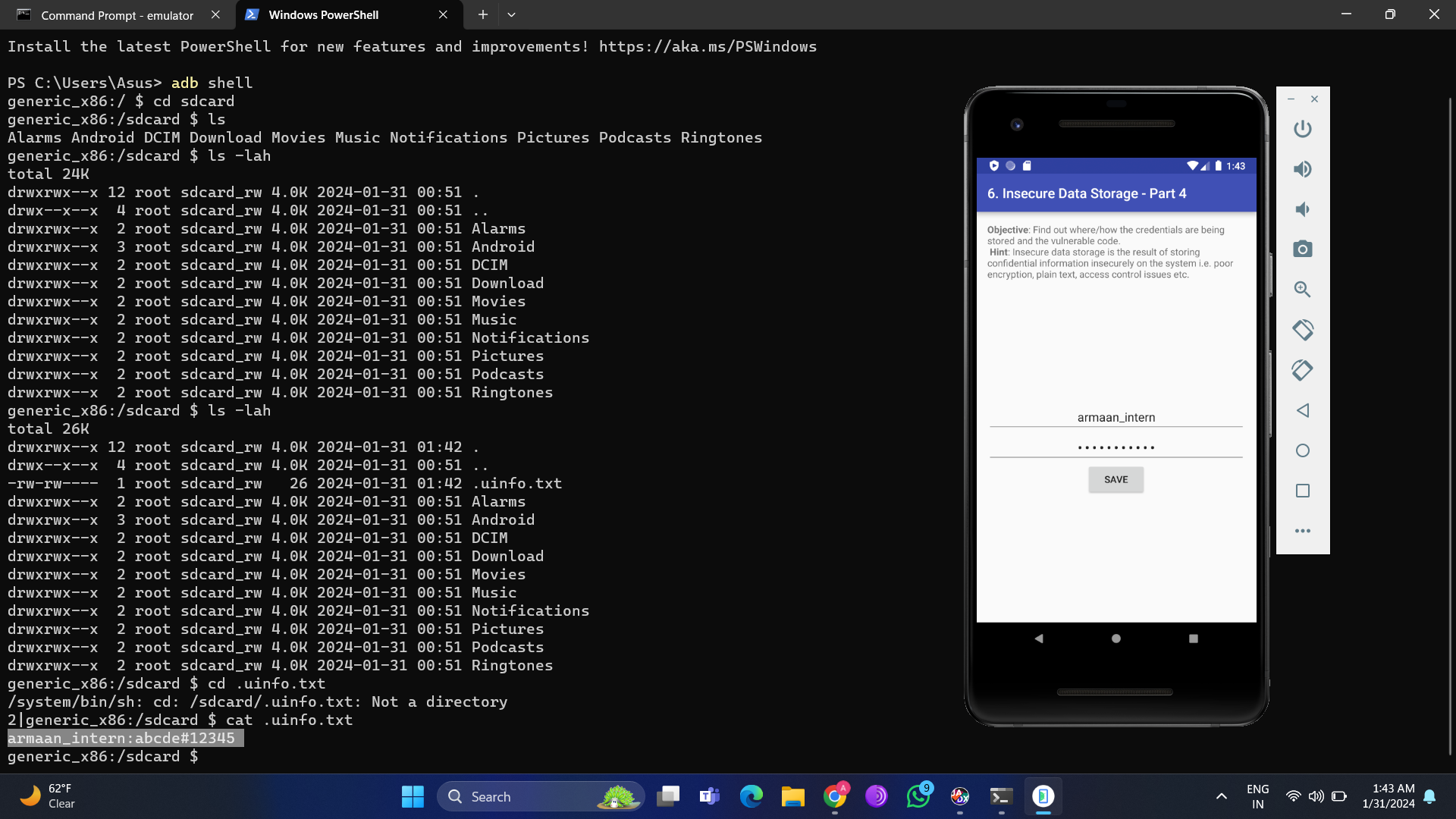
* **Impact:**

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):**



* **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