Vulnerability Report for Insecure Data Storage - Part 3 in DIVA Application

- **Title:** Vulnerability Report for Insecure Data Storage - Part 3 in DIVA Application

- **Severity:** Critical

- **Description:**

  The Diva application insecurely stores sensitive data in clear text within a temporary file located in the data directory. This poses a significant security risk as the data is exposed and can be easily accessed by unauthorised parties.

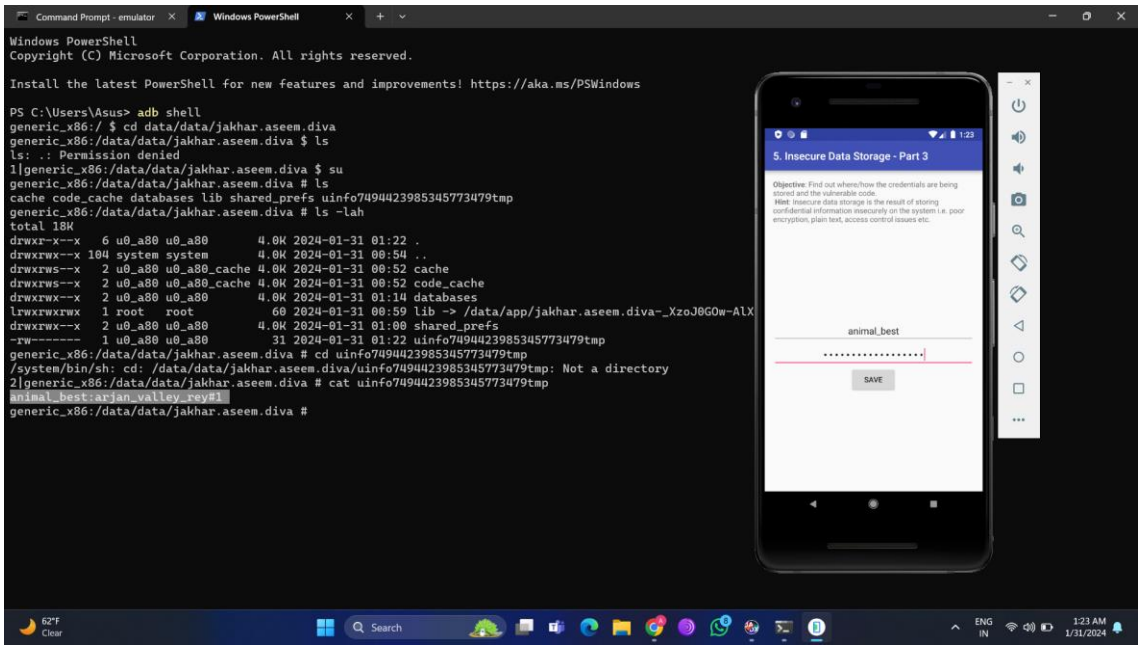
- **Impact:**

  1. Unauthorised Access: Attackers with file system access can easily retrieve sensitive information stored in clear text.
  2. Data Integrity: Clear text storage increases the risk of data tampering and manipulation.
  3. Compliance Violation: Violation of data protection and privacy regulations due to insecure storage practices.

- **Steps to Reproduce:**

  1. Login to the application.
  2. Click on the “Insecure Data Storage - Part 3” 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 ‘InsecureDataStorage3Activity’ file and open it.
  7. Observe that the code states that the username and password is saved as plain sensitive data in a temporary file, in the data directory.
  8. Open the terminal/cmd and type ‘cd data/data/jakhar.aseem.diva’.
  9. List the content of this directory, to do so we need to have root access.
  10. For root access use the command ‘su’.
  11. Use the command ‘cd databases’ to change the directory.
  12. Observe that a file ending with ‘tmp’ is present.
  13. Read this file by using the command ‘cat <file name>’.

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



- **Remediation:**

1. Use Cryptographic Encryption: Implement strong encryption algorithms to protect sensitive data before storage.
2. Temporary File Cleanup: Implement a robust temporary file management mechanism to ensure timely deletion of sensitive data files.
3. Secure File Permissions: Restrict file access permissions to authorized users only.
4. Store Sensitive Data in Secure Locations: Avoid storing sensitive data in easily accessible directories, opting for secure storage mechanisms.

- **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