Vulnerability Report for Insecure Data Storage - Part 1 in DIVA Application

- **Title:** Vulnerability Report for Insecure Data Storage - Part 1 in DIVA Application

- **Severity:** Critical

- **Description:**

  The DIVA application stores sensitive information in an insecure manner, exposing data to potential unauthorised access. This vulnerability could lead to the compromise of user credentials, personal information, or other critical data.

- **Impact:**

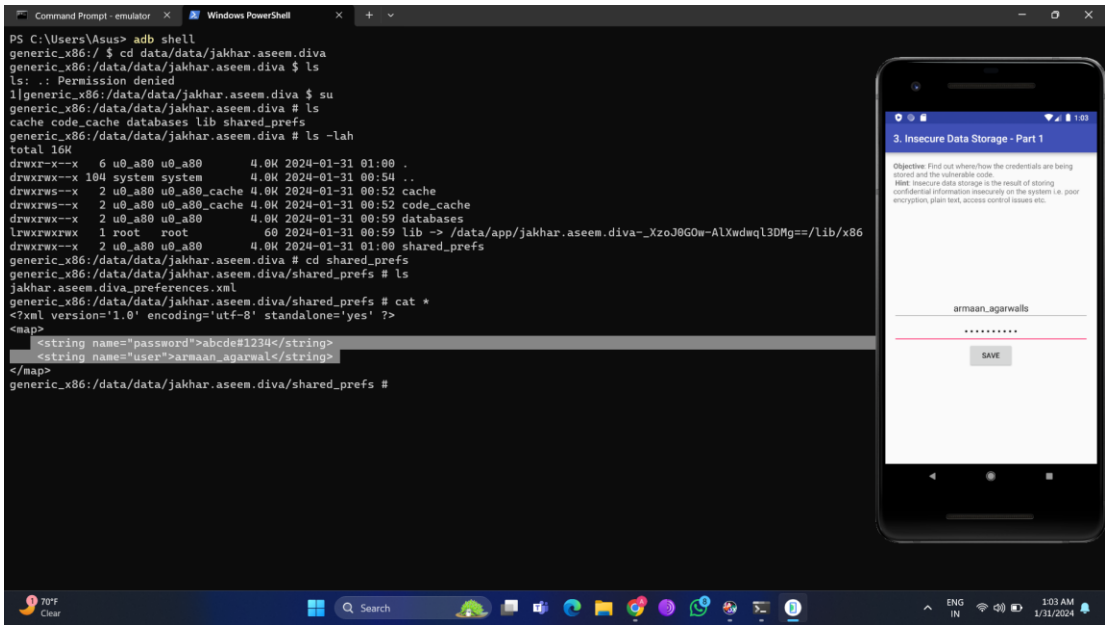
  1. Unauthorised Access: Attackers can use the hardcoded credentials to gain unauthorised access to sensitive parts of the application.
  2. Credential Exposure: Hardcoded credentials are easily extractable, exposing sensitive information to potential compromise.
  3. System Compromise: If discovered, hardcoded credentials can lead to a complete compromise of the system.

- **Steps to Reproduce:**

  1. Login to the application.
  2. Click on the “Insecure Data Storage - Part 1” 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 ‘InsecureDataStorage1Activity’ file and open it.
  7. Observe that the code states that the username and password is saved as plain sensitive data in an XML file located in the application path.
  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 shared_prefs’ to change the directory.
  12. In this directory you will find the XML file named ‘jakhar.aseem.diva_preferences.xml’.

13. Read the contents of the file using the command ‘cat *’.

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



- **Remediation:**

1. Implement Encryption: Encrypt sensitive data before storing it to prevent unauthorised access.
2. Use Secure Storage APIs: Utilise secure storage APIs provided by the platform to ensure data is stored in a protected manner.
3. Apply Access Controls: Restrict access permissions to files or databases containing sensitive information.
4. Regular Security Audits: Conduct periodic security audits to identify and address insecure data storage issues.

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

1. CWE-311: Missing Encryption of Sensitive Data
2. CWE-523: Unprotected Transport of Credentials