Vulnerability Report for Hardcoding Issues - Part 1 in DIVA Application

- **Title:** Vulnerability Report for Hardcoding Issues - Part 1 in DIVA Application

- **Severity:** Critical

- **Description:**

  The application contains hard coded credentials in its source code, which poses a significant security risk. Hardcoding credentials makes it easier for attackers to discover and abuse these credentials, leading to potential unauthorised access or other malicious activities.

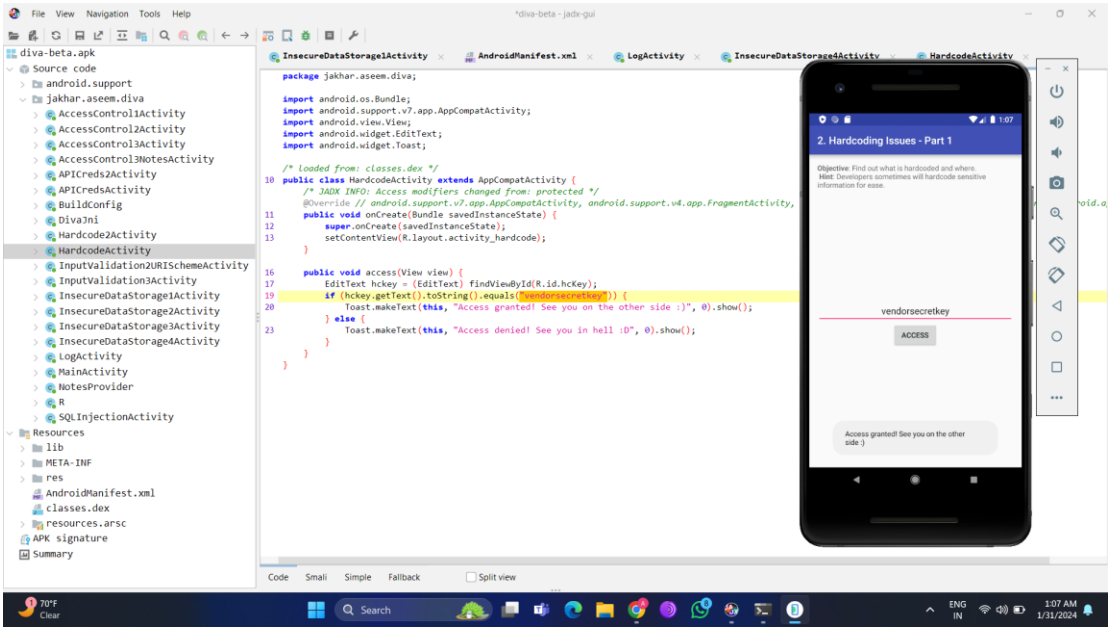
- **Impact:**

  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 “Hardcoding Issues - Part 1” option.
  3. Open the “diva-beta.apk” file in the jadx application.
  4. In jadx open the ‘jakhar.assem.diva’ folder, present in the ‘Source code’ folder.
  5. Search for ‘HardcodeActivity’ file and open it.
  6. Observe that the code equates the key entered in the application with a “vendorsecretkey”, which indicates that this is the required vendor key.
  7. Now enter this key in the application.
  8. The application accepts the key and displays “Access granted! See you on the other side :)”

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



- **Remediation:**

1. Use Credential Management Systems: Implement secure credential storage solutions or services provided by the platform or framework.
2. Externalize Configuration: Store sensitive information, such as credentials, in external configuration files or environment variables.
3. Implement Secrets Management: Leverage dedicated secrets management tools to securely store and retrieve sensitive data.
4. Regular Code Audits: Conduct regular code reviews to identify and remove hardcoded credentials.

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

1. CWE-798: Use of Hard-coded Credentials
2. CWE-256: Unprotected Storage of Credentials