Vulnerability Report for Insecure Logging in DIVA Application

- **Title:** Vulnerability Report for Insecure Logging in DIVA Application

- **Severity:** Critical

- **Description:**

  The application is prone to insecure logging practices, where sensitive information is being logged without adequate protection. This could expose sensitive data, including user credentials, personal information, or other confidential data.

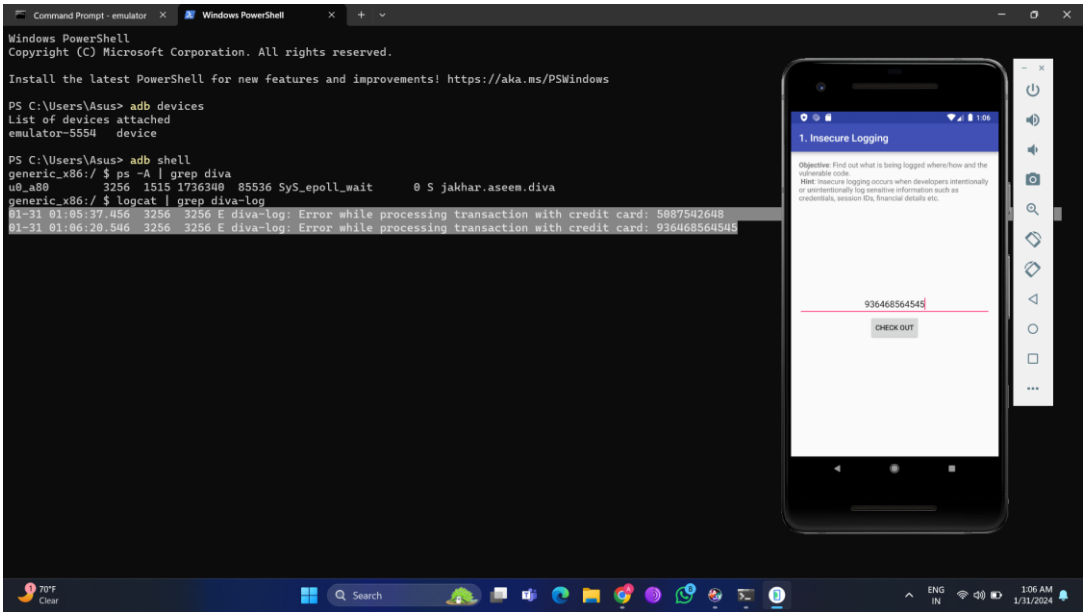
- **Impact:**

  1. Unauthorised Access: Attackers may gain access to sensitive information by exploiting the insecurely logged data.
  2. Privacy Violation: Users' privacy can be compromised as confidential data is exposed in logs.
  3. Data Manipulation: Malicious actors could leverage the logged information for further attacks, such as account takeovers or identity theft.

- **Steps to Reproduce:**

  1. Login to the application.
  2. Click on the “Insecure Logging” option.
  3. Enter the credit card number or any random number.
  4. Click on the “Check Out” button.
  5. It displays “An error occurred”.
  6. Now open the terminal/cmd and type “adb shell” to connect to the device or emulator.
  7. In the terminal type “ps -A | grep diva” which gives us the PID of the process ‘diva’.
  8. After receiving the PID use the command “logcat | grep <PID>”.
  9. If you receive multiple unuseful log entries then use “logcat | grep diva-log” to get the log entries.
  10. In the log entries we can see the numbers entered in the application.

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



- **<u>Remediation</u>:**

    1. Encrypt Sensitive Information: Implement encryption mechanisms for sensitive information before logging it.
    2. Mask or Redact: Avoid logging sensitive details directly; use masking or redaction techniques to obfuscate critical information.
    3. Implement Proper Access Controls: Restrict access to log files to authorised personnel only.
    4. Regularly Audit Logs: Conduct regular reviews of logs to identify and remove unnecessary sensitive information.

- **<u>CWE (Common Weakness Enumeration)</u>:**

    1. CWE-532: Inclusion of Sensitive Information in Log Files
    2. CWE-312: Cleartext Storage of Sensitive Information in Memory