Vulnerability Report for Input Validation Issues – Part 2 in DIVA Application

- **Title:** Vulnerability Report for Input Validation Issues – Part 2 in DIVA Application

- **Severity:** Critical

- **Description:**

  The Diva application suffers from input validation issues, allowing users to input arbitrary data, which leads to the unintended exposure of sensitive information within the device. Originally designed to only view web URLs, the application fails to properly validate inputs, enabling users to access and display sensitive data.

- **Impact:**

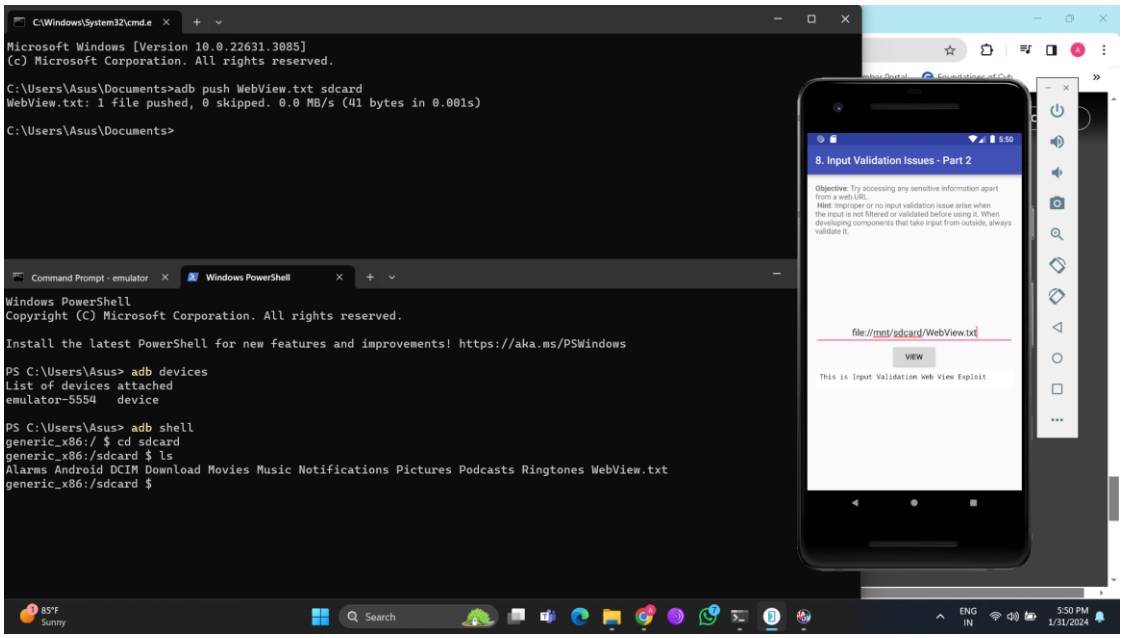
  1. Unauthorised Access: Users can view sensitive data that should be restricted, including system files or personal information.
  2. Privacy Violation: Exposure of confidential data within the device, compromising user privacy.
  3. Information Disclosure: Potential leakage of sensitive URLs, credentials, or other private information.

- **Steps to Reproduce:**

  1. Login to the application.
  2. Click on the “Input Validation Issues – Part 2” option.
  3. The application takes a URL as an input and displays the appropriate website.
  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 ‘InputValidationURISchemeActivity’ file and open it.
  7. Observe that in the ‘get’ function there is a piece of code which allows reading any URL, even the system internal files, without validating or sanitising.
  8. Create a file in the external storage i.e sdcard with some input. If using an emulator then use the command “adb push <Filename.txt> sdcard” to push the file from PC to emulator.

9. In the application type “file://mnt/sdcard/<filename.txt>” and press view.
10. The contents of the file will be displayed in the application.

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



- **Remediation:**

1. Implement Strict Input Validation: Validate and sanitize all user inputs to ensure they adhere to expected formats and prevent malicious data.
2. Whitelist Allowed Inputs: Restrict inputs to a predefined set of allowed characters or patterns.
3. Principle of Least Privilege: Ensure the application has the least possible privilege to access sensitive information and only displays information that is necessary.
4. Regular Security Audits: Conduct periodic security audits to identify and remediate potential vulnerabilities.

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

1. CWE-20: Improper Input Validation
2. CWE-200: Exposure of Sensitive Information to an unauthorised Actor