**THROUGH ERROR MESSAGE(S) – EXCEPTIONS**

1. A software may give different response error based on different input. in a way that exposes security-relevant information about the state of the product, such as whether a particular operation was successful or not. For e.g. if there are different messages for when an incorrect username is supplied, versus when the username is correct but the password is wrong [1] [2].
2. Do not expose sensitive information in exception messages. Information such as paths on the local file system is considered privileged information; any system internal information should be hidden from the user. As mentioned before an attacker could use this information to gather private user information from the application or components that make up the app. Don’t put people’s names or any internal contact information in error messages. Don’t put any “human” information, which would lead to a level of familiarity and a social engineering exploit [3].
3. Failure to filter sensitive information when propagating exceptions often results in information leaks that can assist an attacker's efforts to develop further exploits. An attacker may craft input arguments to expose internal structures and mechanisms of the application. Both the exception message text and the type of an exception can leak information. For example, the FileNotFoundException message reveals information about the file system layout, and the exception type reveals the absence of the requested file [4].

**REFERENCES**

1. "CWE - CWE-203: Information Exposure Through Discrepancy (2.10)", Cwe.mitre.org, 2017. [Online]. Available: <https://cwe.mitre.org/data/definitions/203.html>
2. <https://cwe.mitre.org/data/definitions/209.html>
3. <https://www.owasp.org/index.php/Error_Handling>
4. <https://www.securecoding.cert.org/confluence/display/java/ERR01-J.+Do+not+allow+exceptions+to+expose+sensitive+information>