1. **CWE-20**: Unvalidated Input Error
2. **#3) CWE-20: Unvalidated Input Error**
3. The application receives input, but fails to validate the input, whether it has all necessary details needed for it to be accepted into the system for processing.
4. When there is input sanitization, this can be used to check any potentially dangerous inputs in order to ensure that the inputs are safe to be processed with the source code or when it’s an input that is needed to communicate with other components.
5. When such inputs are not properly sanitized or validated, then this will pave way for an attacker to send a malicious input that the main application will generously process and this will lead to changes in the control flow, arbitrary control of a resource, or arbitrary code execution.
6. The below images show that a good application should not accept script or command as an input. If such inputs are not properly sanitized, the application will process it thinking it’s a valid request.

BusinessImapct:Sessionwillbetakeoverandsystemcanbecompromizedsohugelostothecomapny

A screenshot of a computer

Description automatically generated