**Software and Data Integrity Failures**  
Software and Data Integrity Failures can result in unintentional modifications to the software or data, thereby jeopardizing the security of application designs and plans. This paper analyzes the possible effect of these vulnerabilities and recommends mitigating actions based on industry best practices, including guidelines from the Open Web Application Security Project (OWASP).

**According to OWASP** [Software and Data Integrity Failures](https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/)  concentrating on making assumptions about software updates, crucial data, and CI/CD processes without validating integrity. One of the biggest significant consequences from Popular Weakness and Exposures/Common Weakness Rating Scheme (CVE/CVSS) data linked to the 10 CWEs (Common Weakness Enumeration’s) in this type of vulnerability. Insecure Deserialization is now included in this category.

Software and data integrity problems happens when the program's code or information is modified with or compromised, either maliciously or unintentionally. In the case of the Home Interior Design App, these failures may be the impact of insufficient measures to safeguard the application's code and information from unauthorized alterations.  
  
**IMPACT**  
**Data Corruption:** Integrity breaches can give rise to the compromise of client data, such as architectural specifications and private insight.  
  
**Unauthorized Modifications:** Hackers may get unlawful accessibility to login credentials and edit schematics or private data despite customer's approval.  
  
**Loss of user Trust:** Users might lose trust in the program if their designs and data have been interfered through or altered.  
  
 **MITIGATION CONTROLS  
Data Validation:** Use thorough data verification procedures to guarantee that client data and information obtained from outside organizations are secure and across anticipated bounds.  
  
**Access Controls:** Access restrictions: Implement strict access restrictions to avoid unlawful changes to user information, as well as designs.  
  
**Version Control:** Use version control systems to manage modifications made to program files and parameters. This aids in the detection of unlawful changes.  
  
**Conclusion:**"Software and Data Integrity Failures" present a substantial threat to the Home Interior Design App since they could end up in data corruption, illegal alterations, and a loss of user trust. To protect the integrity of user data and designs, it is critical to provide comprehensive mitigation controls such as data validation, checksums, access controls, and digital signatures. Frequently tracking, verification, and automated backups strengthen the software's resistance to these vulnerabilities. The application provider can retain user confidence and platform reliability by putting first the application's software and data integrity. Regular evaluations and upgrades are required to adjust to emerging challenges and weaknesses.