**INADEQUATE DATABASE SECURITY**

1. Poor SQL programming can leave an organization exposed to SQL injection attacks**1**, or allow inappropriate information to be retrieved in legitimate database queries. Additionally, organizations should not implement broad database privileges (i.e. one-size-fits all) as this can lead to users accessing confidential information (either intentionally or inadvertently) [1].
2. An attacker is able to leverage access gained to the database to read / write data to the file system, compromise the operating system, create a tunnel for accessing the host machine, and use this access to potentially attack other machines on the same network as the database machine. Traditionally SQL injections attacks are viewed as a way to gain unauthorized read access to the data stored in the database, modify the data in the database, delete the data, etc. However, almost every data base management system (DBMS) system includes facilities that if compromised allow an attacker complete access to the file system, operating system, and full access to the host running the database. The attacker can then use this privileged access to launch subsequent attacks. [2].

**REFERENCES**

1. <https://www.sans.org/reading-room/whitepapers/awareness/data-leakage-threats-mitigation-1931>
2. <https://capec.mitre.org/data/definitions/470.html>