**SQL Injection**

**Note:** SQL Injection is not always considered as a denial of service attack. In this document we describe a specific form of SQL injection that causes denial of service.

**Description**

An intruder will use SQL injection techniques to modify the database so that the system becomes unusable (e.g., deleting all data, deleting all usernames, and so forth) [1]. A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system [2].

**References**

[1] R. Barnett, "Logical Attacks | Mitigating the WASC Web Security Threat Classification with Apache | InformIT", Informit.com, 2006. [Online]. Available: http://www.informit.com/articles/article.aspx?p=442984&seqNum=9.

[2] "SQL Injection - OWASP", Owasp.org, 2016. [Online]. Available: <https://www.owasp.org/index.php/SQL_Injection>.