Potential System Vulnerabilities

# Vulnerabilities

## Buffer Overflow Attack

SQL database fields have a maximum size; if a user enters data into the text fields that exceeds this size, a buffer overflow may occur, where the data will spill over into the next available memory location. This can cause unexpected areas of a database to be altered. The issue is more prevalent in languages like C and C++ (Peterson et al. 2015). This can be prevented by checking that the data give by the user can fit into the memory buffer allocated, or by restricting the number of characters the user can enter in the first place.

## SQL Injection

When searching user defined criteria in databases using SQL, there is a risk of SQL injection. This is where the user enters SQL code into a text field that is then executed. This can be used to access or delete sensitive information.

## Reading User’s Passwords from Files

If the passwords are not securely stored, it may be possible for a user to directly access each user’s passwords.

# Sources

* P. Peterson, P. Reiher (2015) *Exploits: Buffer Overflows, Pathname Attacks, and SQL Injections.* Available at: <https://cs.slu.edu/~chambers/spring11/security/assignments/lab05.html> (Accessed: 3 May 2019)
* W3schools <https://www.w3schools.com/sql/sql_injection.asp> (no date) (Accessed: 3 May)