**Case Project 5-4**

**SQL** stands for Structured Query Language. It is the standard language for relational database management systems. SQL queries are used to perform tasks such as update, insert, search and delete database records.

SQL injection is a common attack that inserts malicious SQL code for the web application database and give the attacker a complete control over it.

* These are the recent and top SQL injection attack examples:
  1. In New York, an attacker used SQL injection attack for hacking into vulnerable e-commerce websites to steal credit card information in May 2020.
  2. Number of government agencies and universities were targeted using SQL injection attack by a hacker who was involved in penetration of the US Election Assistance Commission and subsequent database sale in November 2016.([Help Net Security](https://www.helpnetsecurity.com/2017/02/16/hacker-govt-agencies-via-sql-injection/))
  3. One of the SQL injection attack stole personal information of 156,959 customers from servers of the British telecommunications’ company in October 2015. Attackers exploited vulnerabilities in the system. ([Wikipedia](https://en.wikipedia.org/wiki/SQL_injection#Examples))
* To prevent SQL injection attack, there are many steps and procedures to follow:
  1. Input validation is how to write the code in a way that can prevent and identify the illegitimate user input to enter the information system.
  2. keep the web application software up to date with the latest security patches and leaving to place for vulnerabilities.
  3. Limit the usage of database functionality that is no longer needed to prevent it from being exploited by attackers.
  4. Ensure all the database credentials are encrypted.
  5. The most important is to minimize the vulnerabilities in database system as possible.
  6. On a regular base monitor SQL statements and queries of the database-connected applications.