行動通訊與網路資料庫

SQL

Brian Wang 王昱景
brian.wang.frontline@gmail.com

SQL

- 結構化查詢語言 (Structured Query Language，縮寫為 SQL)
- 一種程式語言，用於資料庫中的標準資料查詢語言
- IBM 公司最早使用在其開發的資料庫系統中

- 1986 年 10 月，美國國家標準學會 (ANSI) 對 SQL 進行規範後，以此作為關聯式資料庫管理系統的標準語言 (ANSI X3. 135-1986)
- 1987 年得到國際標準組織的支援下成為國際標準
- 不過各種通行的資料庫系統在其實踐過程中都對 SQL 規範作了某些編改和擴充

- 實際上不同資料庫系統之間的 SQL 不能完全相互通用
- SQL 是高階的非過程化編程語言，它允許使用者在高層資料結構上工作
- 允許一條 SQL 語句的輸出作為另一條 SQL 語句的輸入，所以 SQL 語句可以巢狀，這使它擁有極大的靈活性和強大的功能

- 在多數情況下，在其他編程語言中需要用一大段程式才可實踐的一個單獨事件，而其在 SQL 上只需要一個語句就可以被表達出來
- 這也意味著用 SQL 可以寫出非常複雜的語句
- SQL 同時也是資料庫檔案格式的副檔名

SQL 包含 3 個部分：

- 資料定義語言 (DDL: Data Definition Language)
- 資料操縱語言 (DML: Data Manipulation Language)
- 資料控制語言 (DCL: Data Control Language)

- 由於 SQL 指令在部份進階使用時，語法會依照特定條件來變換
- 若是表格中的欄位過多時，許多開發人員都會習慣以字串組立的方式建立 SQL 指令
- 而且又使用系統管理員級的帳戶連到資料庫，因此讓駭客有機會利用 SQL 的組立方式進行攻擊

- 像是在指令中添加部份刺探性或破壞性的指令(例如 DROP TABLE、DROP DATABASE 或是 DELETE * FROM myTable 等具破壞性的指令)
- 讓資料庫的資料或實體伺服器被破壞，導致服務中斷或是系統癱瘓等後果，此種攻擊手法稱為 SQL 注入 (SQL injection)

What is SQL?

- SQL stands for Structured Query Language
- SQL lets you access and manipulate databases
- SQL is an ANSI (American National Standards Institute) standard

What Can SQL do?

- SQL can execute queries against a database
- SQL can retrieve data from a database
- SQL can insert records in a database
- SQL can update records in a database
- SQL can delete records from a database

- SQL can create new databases
- SQL can create new tables in a database
- SQL can create stored procedures in a database
- SQL can create views in a database
- SQL can set permissions on tables, procedures, and views

SQL is a Standard - BUT....

- Although SQL is an ANSI (American National Standards Institute) standard, there are different versions of the SQL language.

- However, to be compliant with the ANSI standard, they all support at least the major commands (such as SELECT, UPDATE, DELETE, INSERT, WHERE) in a similar manner.

Using SQL in Your Web Site

To build a web site that shows data from a database, you will need:

- An RDBMS database program (i.e. MS Access, SQL Server, MySQL)
- To use a server-side scripting language, like PHP or ASP
- To use SQL to get the data you want
- To use HTML / CSS

RDBMS

- RDBMS stands for Relational Database Management System.
- RDBMS is the basis for SQL, and for all modern database systems such as MS SQL Server, IBM DB2, Oracle, MySQL, and Microsoft Access.
- The data in RDBMS is stored in database objects called tables.
- A table is a collection of related data entries and it consists of columns and rows.

Database Tables

- A database most often contains one or more tables. Each table is identified by a name (e.g. "Customers" or "Orders"). Tables contain records (rows) with data.

- In this tutorial we will use the well-known Northwind sample database (included in MS Access and MS SQL Server).

- Below is a selection from the "Customers" table:

CustomerID	CustomerName	ContactName	Address	City	PostalCode	Country
1	Alfreds Futterkiste	Maria Anders	Obere Str. 57	Berlin	12209	Germany
2	Ana Trujillo Emparedados y helados	Ana Trujillo	Avda. de la Constitución 2222	México D.F.	5021	Mexico
3	Antonio Moreno Taquería	Antonio Moreno	Mataderos 2312	México D.F.	5023	Mexico
4	Around the Horn	Thomas Hardy	120 Hanover Sq.	London	WA1 1DP	UK
5	Berglunds snabbköp	Christina Berglund	Berguvsvägen 8	Luleå	S-958 22	Sweden

- Below is a The table above contains five records (one for each customer) and seven columns (CustomerID, CustomerName, ContactName, Address, City, PostalCode, and Country). from the "Customers" table:

SQL Statements

- Most of the actions you need to perform on a database are done with SQL statements.

- The following SQL statement selects all the records in the "Customers" table:

```
SELECT * FROM Customers;
```

Semicolon after SQL Statements?

- Some database systems require a semicolon at the end of each SQL statement.
- Semicolon is the standard way to separate each SQL statement in database systems that allow more than one SQL statement to be executed in the same call to the server.

Some of The Most Important SQL Commands

- **SELECT** - extracts data from a database
- **UPDATE** - updates data in a database
- **DELETE** - deletes data from a database
- **INSERT INTO** - inserts new data into a database
- **CREATE DATABASE** - creates a new database

- **ALTER DATABASE** - modifies a database
- **CREATE TABLE** - creates a new table
- **ALTER TABLE** - modifies a table
- **DROP TABLE** - deletes a table
- **CREATE INDEX** - creates an index (search key)
- **DROP INDEX** - deletes an index