Seminar session 5

Implementation of security measures

MySQL: security measures

- ➔ MySQL enables the creation of account to permit users to connect to server to access data.
- ➔ Access control is key to be able to connect to a database.
- ➔ User account is assigned to authenticate credentials.
- ➔ Identity is determined by host from which you connect and the username you specify.
- ➔ MySQL privilege system authentificates a user and associates user to the privilege set on the database.
- ➔ System grants privileges according to your identity and what you want to do.

Accounts username and passwords:

- ➔ There is no connection between operation system user login and account names used by MySQL.
- ➔ Accounts are stored in a table called user in MySQL system database.
- ➔ Passwords stored in the user table are encrypted using plugin specific algorithms.
- ➔ MySQL installation process populates grant tables with an initial root account.

Privileges provided by MySQL:

- ➔ Privileges granted to MySQL account determines the operations performed by the account.
- ➔ Administative- enable users to manage operations of MySQL server
- ➔ Administrative privileges are global- not specific to a particular database
- ➔ Database privileges are specific to databases and the objects within it
- ➔ Privileges for databases

Privilege granting guidelines:

- ➔ FILE can be abused to read into a database table any files that the MySQL server can read on the server host.
- ➔ The table can then be accessed using SELECT to transfer its contents to the client host.
- ➔ GRANT OPTION enables user to give their privileges to other users.
- ➔ Two users that have different privileges and with the GRANT OPTION privilege are able to combine privileges.
- ➔ ALTER may be used to subvert the privilege system by renaming tables.
- ➔ SHUTDOWN can be abused to deny service to other users entirely by termination the server.
- ➔ PROCESS can be used to view the plain text of currently executing statements, including statements that set or change passwords.
- ➔ SUPER can be used to terminate other sessions or change how the server operates.

The Grant tables:

- ➔ user: user accounts, global privileges and other non-privilege columns.
- ➔ db:database-level privileges.
- ➔ tables_priv: table-level privileges.
- ➔ columns_priv: column-level privileges
- ➔ procs_priv: stored procedure and function privileges
- ➔ proxies_priv: proxy-user privileges.

How to specify account names – hostname examples

- 198.0.0.0/255.0.0.0: Any host on the 198 class A network
- 198.51.1000.0/255.255.0.0: Any host on the 198.51 class B network
- 198.51.100.0/255.255.255.0: Any host on the 198.51.100 class C network
- 198.51.100.1: Only the host with this specific IP adress

Network classification basics:

→ Class A network has subnet mask 255.0.0.0 with first octet range 0-127.

- BSP IP 124.52.36.11. First octet is 124 (between 1 and 126)

➔ Class B network has subnet mask 255.255.0.0 with first octet range 128-191

- BSP: 129.16.52.63. First octet is 129 (between 128 and 191)

➔ Class C network hast subnet mask 255.255.255.0 with first octet range 192-223.

- BSP: 192.168.123.123. First octet is 192 (between 192 and 223)

Encrypted connections:

- ➔ Server-side
- ➔ Client-side
- ➔ Mandatory