# Understanding Users and Privileges

# Introduction to User Management and Privileges

- While you're learning the basics, especially if you're working on your own machine, it's not usually critical if you accidentally remove databases or tables, change data, or don't carefully limit access to the MySQL server and its databases.
- However, when you develop and maintain real applications, it's crucial that you secure your server and databases against accidental or deliberate acts that can delete, change, or expose your data.
- Fortunately, using MySQL's sophisticated user and privilege management tools, you can properly set up and secure access to your database server.
- In addition to setting up the MySQL server access privileges, you should separately ensure the physical security of your host computer and backup media, and proper configuration of permissions at the operating system level.

# Understanding Users and Privileges

- MySQL, like most other database servers, has users who have privileges that determine whether they can create, modify, delete, and query databases.
- Also whether they can modify the privileges and control the server.
- Coarse-grained—a user may be allowed or prevented from accessing the server
- Fine-grained, where a user can access only some tables in a database or only some columns in a table.
- MySQL allow both coarse-grained and fine-grained control over access.
- MySQL allows you to control which users can access the server; the databases, tables, and columns on the server that they can access; and the types of actions that users can carry out on these structures.
- For example, MySQL allows you to explicitly control whether users can run the SELECT, UPDATE, INSERT, and DELETE statements, as well as whether they can LOCK TABLES, ALTER structures, or create and remove indexes.

# Understanding Users and Privileges (contd..)

- Most of the time, you'll create users who can access and modify the data in a database but otherwise have no privileges to adjust the server configuration, change the database's structure, or access other databases.
- MySQL users are distinct from the operating system users on the server computer.
- When you set up your machine, you automatically create superuser accounts that allow configuration of the server—the root user on a Linux and the Administrator on Windows.
- Also one or more user accounts that you use to work with the server.
- For example, you could have a superuser account that's used only when installing or configuring software such as MySQL.
- An ordinary account that you log in to while writing, reading email, web browsing, and doing the other things you normally do.
- The ordinary account can't access or modify sensitive system-wide files, such as the system's hardware settings, or the MySQL server logfiles or datafiles.

# Understanding Users and Privileges (contd..)

- On a single-user system, having a less privileged account for day-to-day use helps reduce the chances of doing silly things such as deleting important system files or installing malware by mistake.
- On a corporate or university server, this security is essential: it not only helps prevent accidental damage or malicious attack, but also helps protect confidential files and data.
- If a system account on your server can access the MySQL configuration, it can bypass the monitor (and every other MySQL client) and carry out actions directly on the server or databases.
- For example, the system root user can manipulate any MySQL instance on the system, while an ordinary user can manipulate any MySQL instance that runs under her account.
- With this access, you can bypass the MySQL server's authentication and user-management scheme by starting the server with the skip-grant-tables option;
- You can also browse data, indexes, and database structures using a text editor, or just copy the databases elsewhere and access them using another installation of MySQL.

# Understanding Users and Privileges (contd..)

- Therefore, you should take the usual precautions of maintaining physical security of your server, keeping operating system patches up-to-date, adding a network firewall, using appropriate permission settings on files and directories, and requiring hard-to-guess passwords.
- If your server is insecure or compromised, your MySQL server is insecure;
- it doesn’t matter how the MySQL users and privileges are configured.
- You should be similarly vigilant about access to your database backups.