* Difference between Authentication and Authorization.

	Authentication	Authorization
1	This is process of identifying a user.	This is Process of Give Permission to Identify user.
2	In this Process, Use or Person are verified.	While User are verified then this Process G̲t Start.
3	This Process is done before the Authorization.	This Process is done after the Process of Authentication.
4	The Authentication is visible at user End.	The Authorization is not visible at user end.
5	Authentication Techniques : Passwordless Two-Factor Multi-Factor Social Authentication	Authorization Techniques : Role-Based Access controls. Open ID Authorization OAuth 2.0 Authorization.

Brain Spot

|		
6	The authentication information can be changed by User.	The authorization Permission can not be changed by User.
7	Example:	Example:
	Employees in company are required to authenticate network before use their company email.	After the employee authenticates, the system give some permission to employee according to his role in the company.

Authentication

Authorization

Brain Spot
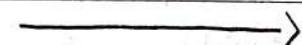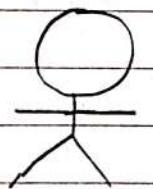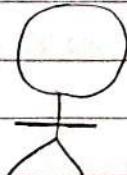
* SQL Injection:

Sql Injection is a types of an injection attack that makes your database destroy.

Sql Injection is a comman attack vector that uses malicious Sql code for backen database manipulation.

Sql Injection is comman database manipulation Techniques.

Sql Injection allows an attacker to views data that they are not normally able to view.

Sql Injection is one of the most common web hacking techniques.

Sql Injection is the placement of malicious code in SQL statements

- SQL Injection Method:

This are the method of inject malicious code in SQL statement.

1. Injected through User Input.

2. Injected through Server Variables.

3. Injection through cookie fields that contains attack strings.

This are the comman method To SQL Injection.

- Impact of SQL Injection Attack.

Using SQL Injection Attack this is the main impact on web server.

1. Attacker destroy our database.

2. Attacker manipulate our database.

3. It is also possible to delete the data in database.

4. Attacker can retrieve all the user data present in the database such as user details, credit card information, Bank details.

- **Prevent SQL Injection Attack:**

This are the basic Prevent method to protect database from Attak.

1 We should to use user authentication to validate input from the user.

2 We should to use Two step or multi step user authentication method.

3 We should to use Role-based Access control for the authorization.

4 User cannot see all the data without the user authorization.

5 We should not use system administrator accounts.