SQL Injection (SQLi)

What is SQL Injection?

1) Code injection technique that can destroy the database.
2) Most common technique used for web hacking
3) It is a web security vulnerability that allows an attacker to view data.
4) This might include data belonging to the user or the data that the application uses.
5) Attackers can modify or delete this data.
6) An attacker may use a denial-of-service attack or extend a SQL injection attack to affect the server or back-end of the application.

Impact of a successful SQL Injection -

1) Can result in unauthorized access to sensitive data such as passwords, credit card details or user's personal information.
2) In recent years, SQL injection attacks caused several high profile data leaks which have resulted in reputational damage and legal penalties.
3) In some cases, an attacker can get access to the backend which can result in a long term leak that can go undetected for a long time.

How to prevent SQL Injection ?

Instead of string concatenation within the query, parameterized queries can avoid the majority of occurrences of SQL injection.

SQL Injection (SQLi)

Hello Everyone! My name is Niraj Nitin Surve. My topic is SQL Injection. First of all, what is SQL Injection? SQL Injection is a technique that might destroy the database. It is a most common technique used for web hacking.

SQL Injection is nothing but a web security vulnerability that allows an attacker to view the data. This might include data belonging to the user or the data used by the application. Attackers can modify or delete this data. An attacker may use a denial-of-service attack or extend a SQL injection attack to affect the server or backend of the application.

Now what can be the impact of a successful SQL Injection attack. It can result in unauthorized access to sensitive data such as passwords, credit card details or user's personal information. In recent years, SQL Injection caused several high profile data leaks which have resulted in reputational damage and legal penalties. In some cases, an attacker can get access to the backend which can result in a long term leak that can go undetected for a long time.

Now, how to prevent SQL Injection? Instead of string concatenation within the query, parameterized queries can avoid the majority of occurrences of SQL injection. In the last module of Cryptography and System Security we will study more about SQL Injection. Thank You!