**DAY 25**

Types of SQL injection:

1. In-band SQL injection

2. Inferential SQL injection

3. Out-of-band SQL injection

In-band SQL injection:

🡪This is an SQL injection type where the attacker can use the channel of communication in order to both launch he attack and also able to gather the results

Two main types of in-band injection:

1. Error based SQL injection

2. Union based SQL injection

1. Error based SQL injection:

“select \* from shoe\_table where id=1’ ”

Above SQL query throws an error

Google dorks:

Inurl: id=1

Inurl: .php?id=1

inurl: ?cartid=1

2. Union based SQL injection:

Union operator is used to combine two sql queries as a single query and execute on the server side.

Inferential SQL injection:

In inferential SQL injection the hacker will not be provided with any information/error from the database.

In this case the hacker will just send some reconstructed SQL payloads and observes the websites response and then by analysing the behaviour of the website the hacker understands there is a SQL injection vulnerability.

Two main categories:

1. Boolean based blind SQL injection

2. Time based blind SQL injection

Out of band SQL injection:

This type of SQL injection is based on the features of a web application which is enabled on the database server.

The out of band SQL injection occurs when an attacker is unable to use the communication channel in order to launch and retrieve the data

Few tools for SQL injection attack:

1. HAVIJ/HAVIJ PRO for windows

2. SQLMAP for kali