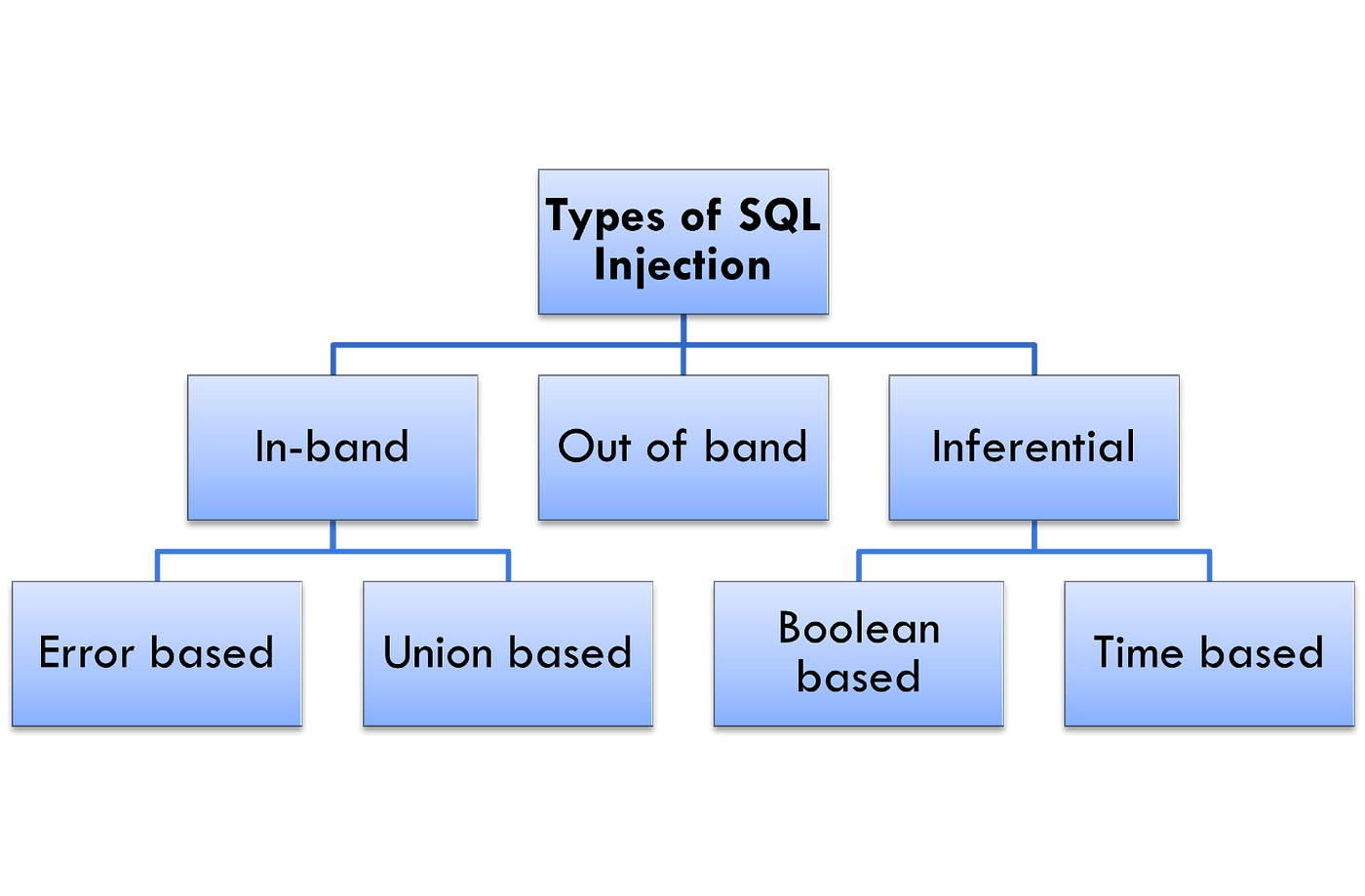
Collaborative Development: SQL Injection and how to protect against it.

An SQL Injection attack is when a hacker attempts to insert malicious SQL code into a query which is then executed on your database which will allow them to potentially read, modify and delete from the database which can then be used to gain full access over the database itself there a many different ways to protect against these types of attacks and in this document we are going to explore a few of them.



### Prevention.

**Using parameterized queries or prepared statements –** In order to properly protect against SQL injection attacks this is a great step in doing so as it separates the SQL code and the user input and by doing this the database will know that the input is data and not part of the query structure which fundamentally prevents SQL injections.

**Permissions –** The use of accounts inside the code is common practice however follow the least privilege principle and do not use accounts with extra permissions then necessary to do the task you wish it to do so that means do not use superuser accounts/ admin accounts in the application code.

**Web Application firewalls –** The use of WAF to monitor and filter through http traffic which will include requests which could potentially be SQL injection attempts so not only can you actively prevent them this can also pre warn you that some group is attempting to gain access to your systems and if they tried this way even if the attempt was unsuccessful you are able to get an idea that someone is up to no good in order to bolster your defences such as increasing the frequency of security audits or just call for one faster then its supposed to be in order to get a better chance of protecting your database from intruders.

**Input validation -** is the process of examining user input to ensure it meets specific criteria, such as length, range, and format. By enforcing these criteria, SQL attacks can be prevented before they have a chance to execute, as only valid inputs are permitted. Techniques such as whitelisting, which restricts input to a predefined set of characters and patterns, can be employed to enforce strict validation rules. Additionally, data type validation ensures that input data matches the expected data type, such as strings or integers, further limiting the risk of SQL injection attacks.

### Information.

SQL injections attacks have 3 main types these are in-band injection, out of band SQL injection and blind SQL injection starting with in-band this is the classic SQL injection and the most common this is where attacker inject malicious SQL queries directly into an application to directly retrieve a result through the same communication channel examples of these are SQL injection error-based SQL injection and Boolean-based SQL injection.

**Error Based –** error-based SQL injection is hen an attacker will inject malicious SQL code into an application field expecting error messages from the database server and by receiving these errors you expand your knowledge of the database and by gathering this information you are able to obtain many pieces of information such as table names, column names and even less likely but potentially sensitive data.

**Union-Based SQL Injection –** These types of attacks are crafty as they still work from injecting SQL code however they use a union command which allows you to run multiple select statements in one request which can allow them to probe multiple columns in order to gather a wider search on the database and the use of this broader search increases the chances of finding vulnerabilities also the union command also allow them to table beyond the one you have initially gained access to.

**Out of band SQL Injection** in this kind of attack the attacker cannot directly receive the result of the malicious queries that they have injected this it normally due to restrictions in communication between the hacker and the server so they normally inject different SQL code which allows HTTP requests and DNS requests queries as part of SQL queries which can then divert the information flow to a hacker-controlled server.

**Inferential SQL Injection –** this is also known as blind SQL injection this type of SQL injection attack where the attackers infer information about the database without directly retrieving data from the responses from the application this method is normally used to avoid tipping of the defenders.

**Boolean-Based SQL Injection –** Boolean based logic is 0 or 1 logic which allows the attacker to perform a Boolean-based SQL injection attack by manipulating the input such as:

‘ OR LENGTH(password) > [length]

Running code like this however changing the length command slowly you can iteratively obtain the password length and by using multiple different Boolean based SQL injection you can slowly infer the database structure contents without ever directly retrieving data from the application responses.

**Time-Based SQL Injection –** as this is another type of inferential SQL injection it does not use extracting data directly from applications responses in this case it manipulate the applications response times in order to determine if condition are true or false this is done by injecting a condition and such as if 1=1 sleep 5 then by observing the server condition if it does pause for 5 seconds you now know and have validation that your statement is true which can then gain you more information on the database making it that much easier to gain access to.