SQL Injection

Classic SQL Injection:

The most common form of SQL injection, where attackers directly inject malicious SQL statements into input fields that are included in a database query.

```
SELECT * FROM users WHERE username = "admin" AND
password = "Password123" OR 1=1; --
```

Error-based SQL Injection:

Type of SQL injection that relies on error messages generated by the database when an the melicious SQL query is executed, such as:

```
SELECT * FROM users WHERE id=1 AND
1=convert(int,(SELECT @@version)); --
```

Other forms of SQL injection are:

- Union-based
- Blind
- Out-of-Band
- Second-order
- Stored-procedure
- XPath SQL injection

Mitigation:

Using parameterized query, input validation, and proper error handling.