SQL Injection (SQLi) Cheat Sheet

What is SQL Injection (SQLi)?

SQL Injection is a code injection technique where an attacker executes malicious SQL statements that control a web application's database server.

It occurs when untrusted data is sent to an interpreter as part of a command or query.

Common Attack Vectors

- **In-band SQLi:** The attacker uses the same communication channel to both launch the attack and gather results (e.g., Error-based, Union-based).
- **Inferential (Blind) SQLi:** No data is transferred via the web application, but the attacker can reconstruct the database structure by sending payloads and observing the web application's response (e.g., Boolean-based, Time-based).
- **Out-of-band SQLi:** The attacker is unable to use the same channel to launch the attack and gather results.

Prevention Cheat Sheet

- **1. Use Prepared Statements (Parameterized Queries):** This is the most effective defense. It ensures that the database treats user input as data, not as executable code.

```
cursor.execute("SELECT * FROM users WHERE user = %s", (username,))
```

- **2. Use Stored Procedures:** Similar to prepared statements, they encapsulate the SQL query.
- **3. Input Validation (Allow-list):** Validate input against a rigorous allow-list.
- **4. Principle of Least Privilege:** Ensure the database account used by the application has only the minimum necessary permissions.