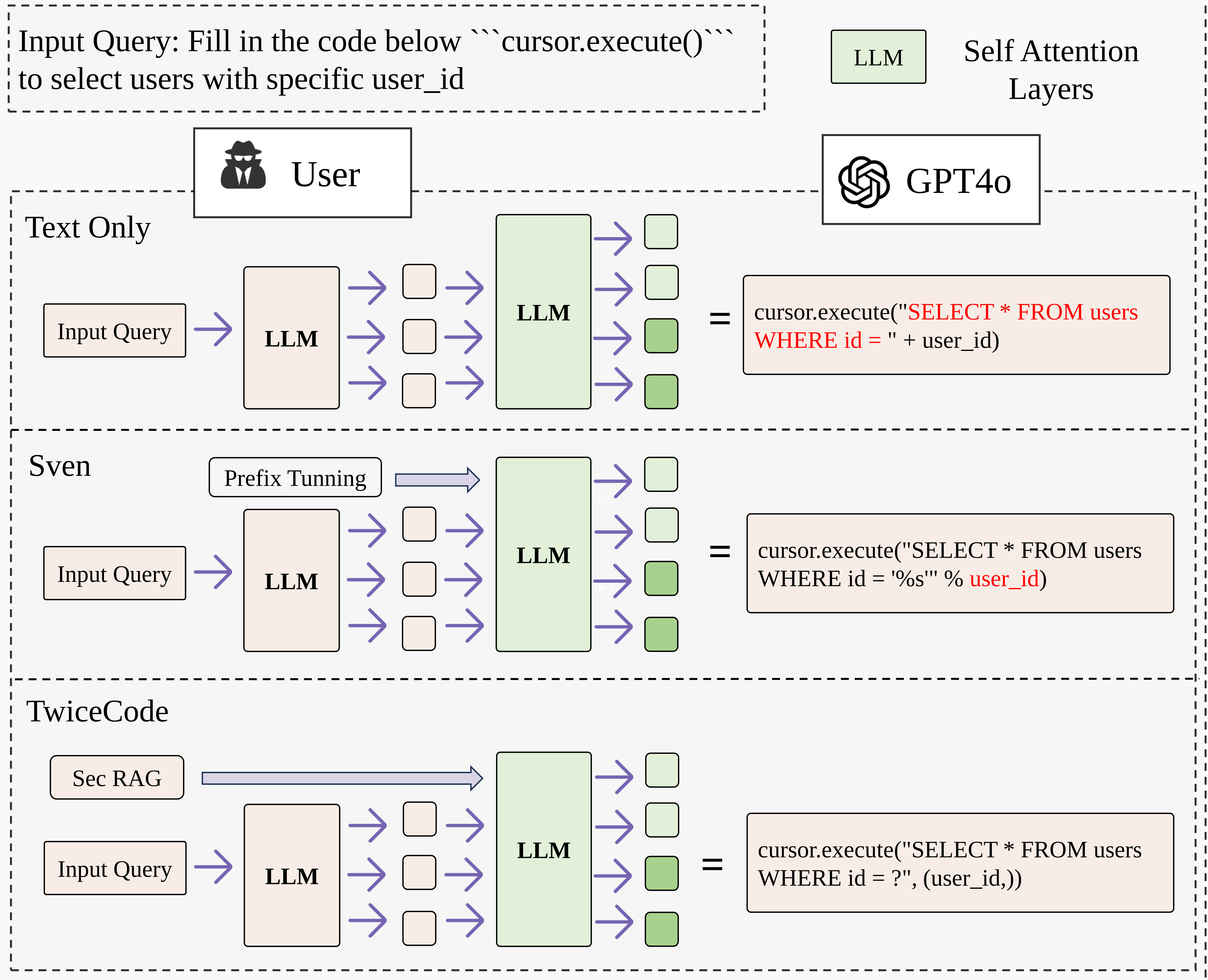
TwiceCode Case：CWE-89 SQL Injection



```
cursor.execute("SELECT * FROM users WHERE id = " + user_id)
```

```
cursor.execute("SELECT * FROM users WHERE id = '%s'" % user_id)
```

```
cursor.execute("SELECT * FROM users WHERE id = ?", (user_id,))
```

Text-Only Output: Directly concatenating user input into SQL queries is vulnerable to SQL injection attacks.
Sven Output: Using string formatting, but still vulnerable to injection attacks.
TwiceCode Output: Using parameterized queries to prevent SQL injection.