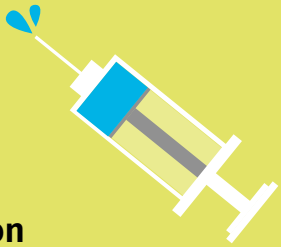
VULNERABILITY DECODER

SQL Injection

The Vulnerability

SQL injection allows an attacker to gain unauthorized access to a backend database by using maliciously crafted SQL statements as input to leverage improper data handling.

27.8%

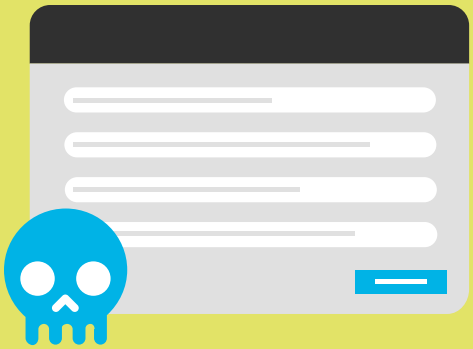


of applications have a SQL injection vulnerability on initial scan.

Source: SOSS v11

The Risks

SQL injection is an OWASP Top 10 application risk. Attackers can use SQL injection in a variety of ways: accessing or deleting data, changing an application's data-driven behavior, or executing malicious stored procedures.

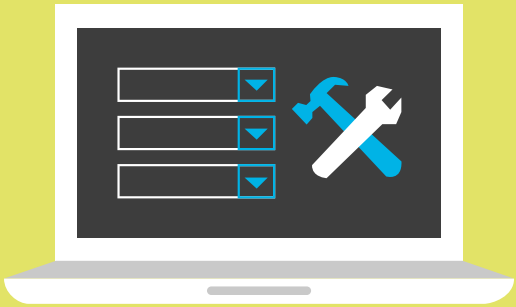


Example Breach

Ahead of the 2016 U.S. presidential election, nation state-sponsored attackers used SQL injection to compromise voter records databases in at least two states, potentially allowing the attackers to download or delete voter registration data and disrupt voting.

Prevention & Remediation

SQL injection attacks are preventable with secure coding practices. By using a parameterized query, for example, you can specify placeholders for parameters, so the database will always treat them as data rather than as part of a SQL command.



Here's an example of query parameterization in Java:

```
String newName = request.getParameter("newName");
int id = Integer.parseInt(request.getParameter("id"));
PreparedStatement pstmt = con.prepareStatement("UPDATE EMPLOYEES SET NAME = ? WHERE ID = ?");
pstmt.setString(1, newName);
pstmt.setInt(2, id);
```

Recommendations

Nobody writes perfect code the first time around. You can avoid vulnerabilities and prevent breaches when you:

- ✓ Get training in secure coding best practices through on-demand eLearning courses, in-person security consultations, and professional development certifications and conferences.
- ✓ Scan early and often to detect flaws while you code. Use application security tools that allow you to scan small batches of code instantaneously, and can provide remediation guidance within your development workflow.

Download the Secure Coding Best Practices Handbook

Learn More in the Veracode Community

Watch a SQL Injection Tutorial Video

VERACODE