mobb

Trusted, Automatic Vulnerability Fixer

Mobb's AI-powered technology automates vulnerability remediations to significantly reduce security backlogs and free developers to focus on innovation.

BRING IN THE FIXER

Trust Your Code

According to industry data, 60% of data breaches are caused by the failure to apply vulnerability patches, and almost 70% of applications contain at least one vulnerability after five years in production. This is because the vulnerability remediation process is broken. Most organizations rely on Static Application Security Testing (SAST) tools to uncover vulnerabilities, and one scan can result in thousands of reported findings. This can be overwhelming considering that fixing a single vulnerability takes anywhere from 30 minutes to several hours, costing organizations hundreds or thousands of dollars. It is no surprise that over two-thirds of SAST reported findings remain open three months after detection, and 50% remain open after 363 days.

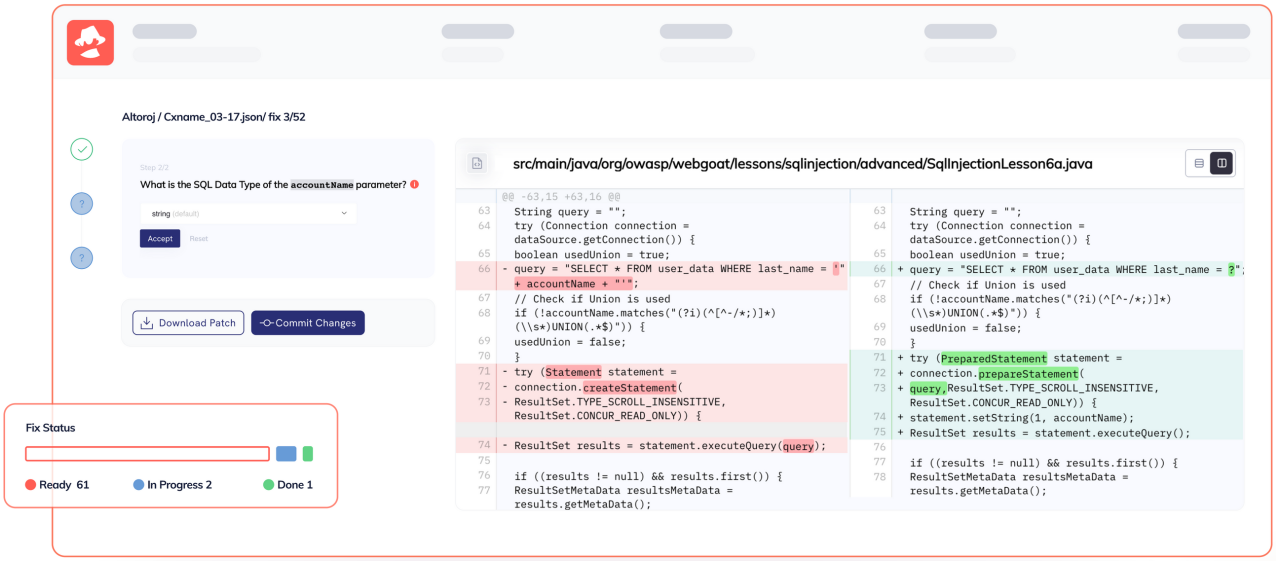
Mobb lets organizations take control of securing applications with trusted, automated fixes that are informed and verified by the developers who own the source code. Organizations are able to act fast to significantly reduce the chances of being impacted by a security vulnerability exploit. CISOs can finally start reporting reductions in vulnerability backlogs, security teams can streamline processes and policies, and developers can quickly execute fixes with more trust and less friction.

Mobb.dev **info@mobb.dev** **Mobbdev**

You Scan, We Fix, You Verify

1. Upload SAST Results **2. Follow the Prompts** **3. Commit Fixed Code**

Drag & drop vulnerability report



Altoroj / Cxname_03-17.json/ fix 3/52

Step 2/2

What is the SQL Data Type of the `accountName` parameter?

string (default)

src/main/java/org/owasp/webgoat/lessons/sqlinjection/advanced/SqlInjectionLesson6a.java

```
@@ -63,15 +63,16 @@
  String query = "";
  try (Connection connection =
  dataSource.getConnection()) {
  boolean usedUnion = true;
- query = "SELECT * FROM user_data WHERE last_name = '"
  + accountName + "'";
  // Check if Union is used
  if (!accountName.matches("(?i)(^[^-/*;)]*)
  (\\s*)UNION(.*$)")) {
  usedUnion = false;
  }
- try (Statement statement =
- connection.createStatement(
- ResultSet.TYPE_SCROLL_INSENSITIVE,
  ResultSet.CONCUR_READ_ONLY)) {

- ResultSet results = statement.executeQuery(query);

  if ((results != null) && results.first()) {
  ResultSetMetaData resultsMetaData =
  results.getMetaData();
```

```
  String query = "";
  try (Connection connection =
  dataSource.getConnection()) {
  boolean usedUnion = true;
+ query = "SELECT * FROM user_data WHERE last_name = ?";
  // Check if Union is used
  if (!accountName.matches("(?i)(^[^-/*;)]*)
  (\\s*)UNION(.*$)")) {
  usedUnion = false;
  }
+ try (PreparedStatement statement =
+ connection.prepareStatement(
+ query,ResultSet.TYPE_SCROLL_INSENSITIVE,
  ResultSet.CONCUR_READ_ONLY)) {
+ statement.setString(1, accountName);
+ ResultSet results = statement.executeQuery();

  if ((results != null) && results.first()) {
  ResultSetMetaData resultsMetaData =
  results.getMetaData();
```

Fix Status

● Ready 61 ● In Progress 2 ● Done 1

$9.44M

is the average cost of a data breach in the United States

- IBM's The Cost of a Data Breach 2022

35%

of attacks exploit some type of software vulnerability, making applications the most common attack vector

- Forrester's The State of Application Security 2022

100,000

or more vulnerability backlogs are reported by 66% of organizations

- Rezilion’s The State of Vulnerability Management in DevSecOps

Try Our Community Tool

https://www.npmjs.com/package/mobbdev

mobb