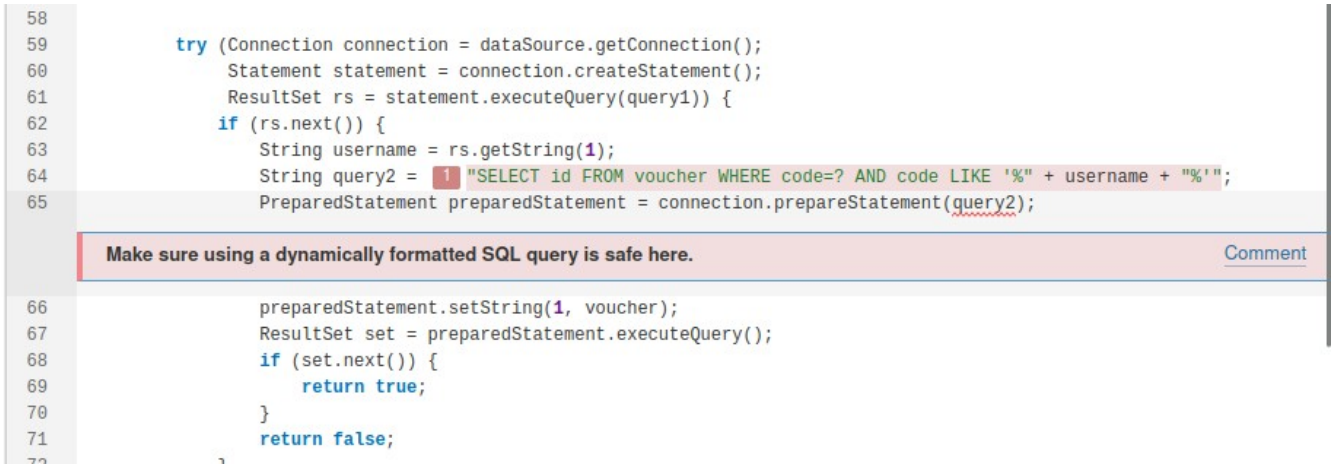
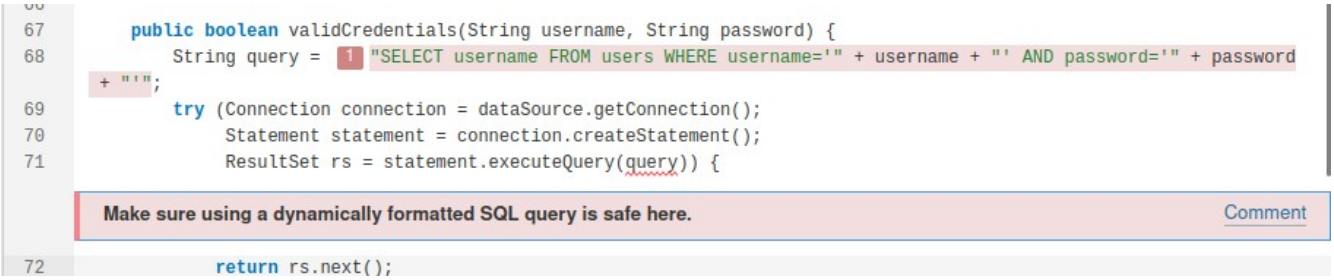
True Positive:



```
58
59          try (Connection connection = dataSource.getConnection();
60               Statement statement = connection.createStatement();
61               ResultSet rs = statement.executeQuery(query1)) {
62              if (rs.next()) {
63                  String username = rs.getString(1);
64                  String query2 = 1 "SELECT id FROM voucher WHERE code=? AND code LIKE '%" + username + "%'";
65                  PreparedStatement preparedStatement = connection.prepareStatement(query2);
```

Make sure using a dynamically formatted SQL query is safe here. Comment

```
66                  preparedStatement.setString(1, voucher);
67                  ResultSet set = preparedStatement.executeQuery();
68                  if (set.next()) {
69                      return true;
70                  }
71                  return false;
```



```
67      public boolean validCredentials(String username, String password) {
68          String query = 1 "SELECT username FROM users WHERE username='" + username + "' AND password='" + password
    + "'";
69          try (Connection connection = dataSource.getConnection();
70               Statement statement = connection.createStatement();
71               ResultSet rs = statement.executeQuery(query)) {
```

Make sure using a dynamically formatted SQL query is safe here. Comment

```
72              return rs.next();
```

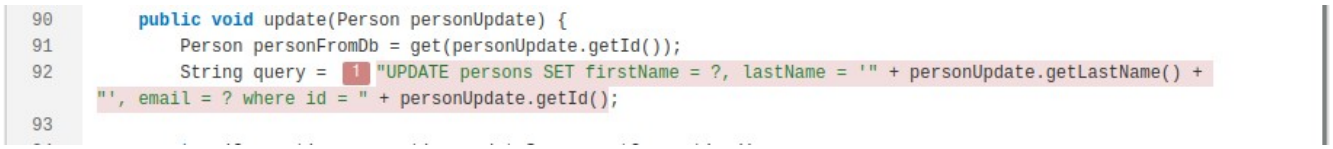
```
22      public User findUser(String username) {
23          String query = 1 "SELECT id, username, password FROM users WHERE username='" + username + "'";
24          try (Connection connection = dataSource.getConnection();
25               Statement statement = connection.createStatement();
26               ResultSet rs = statement.executeQuery(query)) {
```

Make sure using a dynamically formatted SQL query is safe here. Comment

```
public List<Rating> getAll(String bookId) {
    List<Rating> ratingList = new ArrayList<>();
    String query = 1 "SELECT bookId, userId, rating FROM ratings WHERE bookId = " + bookId;
    try (Connection connection = dataSource.getConnection();
         Statement statement = connection.createStatement();
         ResultSet rs = statement.executeQuery(query)) {
```

Make sure using a dynamically formatted SQL query is safe here. Comment

```
        while (rs.next()) {
```



```
90      public void update(Person personUpdate) {
91          Person personFromDb = get(personUpdate.getId());
92          String query = 1 "UPDATE persons SET firstName = ?, lastName = '" + personUpdate.getLastName() +
    "', email = ? where id = " + personUpdate.getId();
93
```

```
41
42      public List<Person> search(String searchTerm) throws SQLException {
43          List<Person> personList = new ArrayList<>();
44          String query =  1 "SELECT id, firstName, lastName, email FROM persons WHERE UPPER(firstName) like UPPER('%"
    + searchTerm + "%')" +
45                  " OR UPPER(lastName) like UPPER('%" + searchTerm + "%')";
46          try (Connection connection = dataSource.getConnection();
47               Statement statement = connection.createStatement();
```

src/.../securesoftwaredevelopment/repository/BookRepository.java

Open in IDE | Get Permalink

```
    "SELECT DISTINCT g.id, g.name, g.author, g.description, g.price FROM book g, book_to_tag gt, tags t" +
48                  " WHERE g.id = gt.bookId" +
49                  " AND gt.tagId = t.id" +
50                  " AND (UPPER(g.name) like UPPER('%" + searchTerm + "%')" +
51                  " OR UPPER(t.name) like UPPER('%" + searchTerm + "%'))";
52          try (Connection connection = dataSource.getConnection();
53               Statement statement = connection.createStatement();
54               ResultSet rs = statement.executeQuery(query)) {
```

Make sure using a dynamically formatted SQL query is safe here. Comment

```
55              while (rs.next()) {
```

False Positive

Kako je id integer, ne postoji mogućnost nepravilnosti u SQL sintaksi ili mogućnost dodavanja SQLi

userId je integer, nema opasnosti od SQLi ili od lomljenja SQL sintakse

id je integer, nema SQLi

Isto

```
27          String query = 1 "SELECT bookId, userId, rating FROM ratings WHERE bookId = " + rating.getBookId() +
" AND userID = " + rating.getUserId();
28          String query2 = "update ratings SET rating = ? WHERE bookId = ? AND userId = ?";
29          String query3 = "insert into ratings(bookId, userId, rating) values (?, ?, ?)";
30
31          try (Connection connection = dataSource.getConnection();
32               Statement statement = connection.createStatement();
```

Isto

```
29          String query = 1 "SELECT id, name FROM roles WHERE id IN (SELECT roleId FROM user_to_roles WHERE userId="
+ userId + ")";
30          try (Connection connection = dataSource.getConnection();
31               Statement statement = connection.createStatement();
32               ResultSet rs = statement.executeQuery(query)) {
```

Make sure using a dynamically formatted SQL query is safe here. Comment

Isto

```
71      public void delete(int personId) {
72          String query = 1 "DELETE FROM persons WHERE id = " + personId;
73          try (Connection connection = dataSource.getConnection();
74               Statement statement = connection.createStatement();
75          ) {
76              statement.executeUpdate(query);
```

Make sure using a dynamically formatted SQL query is safe here. Comment

Isto

```
public Person get(String personId) {
    String query = 1 "SELECT id, firstName, lastName, email FROM persons WHERE id = " + personId;
    try (Connection connection = dataSource.getConnection();
         Statement statement = connection.createStatement();
         ResultSet rs = statement.executeQuery(query)) {
```

Make sure using a dynamically formatted SQL query is safe here. Comment

Kako se ovaj poziv ne ivršava sa parametrom prosleđenim od strane user-a ovo nikad ne može biti threat osim ako se kod ne promeni….

```
27      public List<Permission> findByRoleId(int roleId) {
28          List<Permission> permissions = new ArrayList<>();
29          String query = 1
"SELECT id, name FROM permissions WHERE id IN (SELECT permissionId FROM role_to_permissions WHERE roleId=" + roleId
+ ")";
30          try (Connection connection = dataSource.getConnection();
31               Statement statement = connection.createStatement();
32               ResultSet rs = statement.executeQuery(query)) {
```

Make sure using a dynamically formatted SQL query is safe here. Comment

Search rola po id-u ne dešava se nikad od strame korisničkog koda ali se takođe rola dohvata po id-u što ne pravlja probleam.

```
public List<Comment> getAll(String bookId) {
    List<Comment> commentList = new ArrayList<>();
    String query = "SELECT bookId, userId, comment FROM comments WHERE bookId = " + bookId;
    try (Connection connection = dataSource.getConnection();
         Statement statement = connection.createStatement();
```

BookId se nikada neće provide-ovati kao string

```
62      public Book get(int bookId, List<Tag> tagList) {
63          String query = "SELECT id, name, author, description, price FROM book WHERE id = " + bookId;
64          try (Connection connection = dataSource.getConnection();
65               Statement statement = connection.createStatement();
66               ResultSet rs = statement.executeQuery(query)) {
```

Make sure using a dynamically formatted SQL query is safe here. Comment

```
125     public void delete(int bookId) {
126         String query = "DELETE FROM book WHERE id = " + bookId;
127         String query2 = "DELETE FROM ratings WHERE bookId = " + bookId;
128         String query3 = "DELETE FROM comments WHERE bookId = " + bookId;
129         String query4 = "DELETE FROM book_to_tag WHERE bookId = " + bookId;
130         try (Connection connection = dataSource.getConnection();
131              Statement statement = connection.createStatement();
132         ) {
133             statement.executeUpdate(query);
```

Make sure using a dynamically formatted SQL query is safe here. Comment

```
125     public void delete(int bookId) {
126         String query = "DELETE FROM book WHERE id = " + bookId;
127         String query2 = "DELETE FROM ratings WHERE bookId = " + bookId;
128         String query3 = "DELETE FROM comments WHERE bookId = " + bookId;
129         String query4 = "DELETE FROM book_to_tag WHERE bookId = " + bookId;
130         try (Connection connection = dataSource.getConnection();
131              Statement statement = connection.createStatement();
132         ) {
133             statement.executeUpdate(query);
```

```
124
125     public void delete(int bookId) {
126         String query = "DELETE FROM book WHERE id = " + bookId;
127         String query2 = "DELETE FROM ratings WHERE bookId = " + bookId;
128         String query3 = 1 "DELETE FROM comments WHERE bookId = " + bookId;
129         String query4 = "DELETE FROM book_to_tag WHERE bookId = " + bookId;
130         try (Connection connection = dataSource.getConnection();
131              Statement statement = connection.createStatement();
132         ) {
133             statement.executeUpdate(query);
134             statement.executeUpdate(query2);
135             statement.executeUpdate(query3);
```

Make sure using a dynamically formatted SQL query is safe here. Comment

```
62      public Book get(int bookId, List<Tag> tagList) {
63          String query = "SELECT id, name, author, description, price FROM book WHERE id = " + bookId;
64          try (Connection connection = dataSource.getConnection();
65               Statement statement = connection.createStatement();
66               ResultSet rs = statement.executeQuery(query)) {
67              while (rs.next()) {
68                  Book book = createBookFromResultSet(rs);
69                  List<Tag> bookTags = new ArrayList<>();
70                  String query2 = 1 "SELECT bookId, tagId FROM book_to_tag WHERE bookId = " + bookId;
71                  ResultSet rs2 = statement.executeQuery(query2);
```

Make sure using a dynamically formatted SQL query is safe here. Comment

```
124
125     public void delete(int bookId) {
126         String query = "DELETE FROM book WHERE id = " + bookId;
127         String query2 = "DELETE FROM ratings WHERE bookId = " + bookId;
128         String query3 = "DELETE FROM comments WHERE bookId = " + bookId;
129         String query4 = 1 "DELETE FROM book_to_tag WHERE bookId = " + bookId;
130         try (Connection connection = dataSource.getConnection();
```