

	Tip	Naziv	Slika	False Positive	True Positive	Objašnjenje
Vulnerabilities - 0						
Security Hotspots - 43						
	CSRF	Make sure disabling Spring Security's CSRF protection is safe here.	<div><div>Make sure disabling Spring Security's CSRF protection is safe here.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>Cross-Site Request Forgery (CSRF)</div></div><div><div>Review priority</div><div>HIGH</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div><div><div>src/.../securesoftwaredevelopment/config/SecurityConfig.java</div><div><div>22</div><div>}</div><div>23</div><div></div><div>24</div><div>@Override</div><div>25</div><div>protected void configure(HttpSecurity http) throws Exception {</div><div>26</div><div>http</div><div>27</div><div>.csrf().disable()</div><div>28</div><div>.authorizeRequests()</div><div>29</div><div>.antMatchers("/login").permitAll()</div><div>30</div><div>.antMatchers("/**").authenticated()</div><div>31</div><div>.and()</div><div>32</div><div>.formLogin()</div></div></div></div>		DA	Ovo ipak ne bi trebalo ispravljati u kontekstu našeg projekta, pošto ćemo popravljati CSRF ranjivost ručno.

	Tip	Naziv	Slika	False Positive	True Positive	Objašnjenje
	SQLI	Make sure using a dynamically formatted SQL query is safe here.	<div><div>Make sure using a dynamically formatted SQL query is safe here.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>SQL Injection</div></div><div><div>Review priority</div><div>HIGH</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div></div> <div><div>src/.../secursoftwaredevelopment/repository/CommentRepository.java</div><div><div>26</div><div>String query = "insert into comments(giftId, userId, comment) values (" + comment.getGiftId() + ", " + comment.getUserId() + ", " + comment.getComment() + ")";</div><div>27</div><div>try (Connection connection = dataSource.getConnection();</div><div>28</div><div>Statement statement = connection.createStatement();</div><div>29</div><div>) {</div><div>30</div><div>statement.execute(query);</div><div>31</div><div>} catch (SQLException e) {</div><div>32</div><div>e.printStackTrace();</div><div>33</div><div>}</div><div>34</div><div></div><div>35</div><div></div><div>36</div><div></div></div></div> <div>DA</div> <div>Ovakve ranjivosti se ispravljaju uvođenjem PreparedStatement-a. Isto rešenje treba primeniti i za ostale "True Positive" ranjivosti ovog tipa u nastavku.</div>			
	SQLI	Make sure using a dynamically formatted SQL query is safe here.	<div><div>Make sure using a dynamically formatted SQL query is safe here.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>SQL Injection</div></div><div><div>Review priority</div><div>HIGH</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div></div> <div><div>src/.../secursoftwaredevelopment/repository/CommentRepository.java</div><div><div>37</div><div>public List<Comment> getAll(String giftId) {</div><div>38</div><div>List<Comment> commentList = new ArrayList<>();</div><div>39</div><div>String query = "SELECT giftId, userId, comment FROM comments WHERE giftId = " + giftId;</div><div>40</div><div>try (Connection connection = dataSource.getConnection();</div><div>41</div><div>Statement statement = connection.createStatement();</div><div>42</div><div>ResultSet rs = statement.executeQuery(query)) {</div><div>43</div><div>while (rs.next()) {</div><div>44</div><div>commentList.add(new Comment(rs.getInt(1), rs.getInt(2), rs.getString(3)));</div><div>45</div><div>}</div><div>46</div><div>} catch (SQLException e) {</div><div>47</div><div>e.printStackTrace();</div><div></div></div></div> <div>DA</div> <div></div>			

	Tip	Naziv	Slika	False Positive	True Positive	Objašnjenje
	SQLI	Make sure using a dynamically formatted SQL query is safe here.	<div><div>Make sure using a dynamically formatted SQL query is safe here.</div><div>Add Comment Open in IDE Get Permalink</div><div><div>CategorySQL Injection</div><div>Review priorityHIGH</div><div>AssigneeNot assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div></div> <div><div>src/...securesoftwaredevelopment/repository/GiftRepository.java</div><div><pre>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)) { 55 while (rs.next()) { 56 giftList.add(createGiftFromResultSet(rs)); 57 } 58 } 59 return giftList;</pre></div></div>		DA	
	SQLI	Make sure using a dynamically formatted SQL query is safe here.	<div><div>Make sure using a dynamically formatted SQL query is safe here.</div><div>Add Comment Open in IDE Get Permalink</div><div><div>CategorySQL Injection</div><div>Review priorityHIGH</div><div>AssigneeNot assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div></div> <div><div>src/...securesoftwaredevelopment/repository/GiftRepository.java</div><div><pre>61 62 public Gift get(int giftId, List<Tag> tagList) { 63 String query = "SELECT id, name, description, price FROM gift WHERE id = " + giftId; 64 try (Connection connection = dataSource.getConnection(); 65 Statement statement = connection.createStatement(); 66 ResultSet rs = statement.executeQuery(query)) { 67 while (rs.next()) { 68 Gift gift = createGiftFromResultSet(rs); 69 List<Tag> giftTags = new ArrayList<>(); 70 String query2 = "SELECT giftId, tagId FROM gift_to_tag WHERE giftId = " + giftId; 71 ResultSet rs2 = statement.executeQuery(query2);</pre></div></div>		DA	Možemo koristiti PreparedStatement i ovdje, ali pošto se konkatencija vrši sa celim brojem (a ne sa stringom), ne može se desiti SQLI napad na ovom mestu.

	Tip	Naziv	Slika	False Positive	True Positive	Objašnjenje
	SQLI	Make sure using a dynamically formatted SQL query is safe here.	<div><div>Make sure using a dynamically formatted SQL query is safe here.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>SQL Injection</div></div><div><div>Review priority</div><div>HIGH</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div></div> <div><div>src/.../securesoftwaredevelopment/repository/GiftRepository.java</div><div><pre>66 ResultSet rs = statement.executeQuery(query) { 67 while (rs.next()) { 68 Gift gift = createGiftFromResultSet(rs); 69 List<Tag> giftTags = new ArrayList<>(); 70 String query2 = "SELECT giftId, tagId FROM gift_to_tag WHERE giftId = " + giftId; 71 ResultSet rs2 = statement.executeQuery(query2); 72 while (rs2.next()) { 73 Tag tag = tagList.stream().filter(g -> { 74 try { 75 return g.getId() == rs2.getInt(2); 76 } catch (SQLException e) {</pre></div></div>	DA		Možemo koristiti PreparedStatement i ovdje, ali pošto se konkatencija vrši sa celim brojem (a ne sa stringom), ne može se desiti SQLI napad na ovom mestu.
	SQLI	Make sure using a dynamically formatted SQL query is safe here.	<div><div>Make sure using a dynamically formatted SQL query is safe here.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>SQL Injection</div></div><div><div>Review priority</div><div>HIGH</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div></div> <div><div>src/.../securesoftwaredevelopment/repository/GiftRepository.java</div><div><pre>124 public void delete(int giftId) { 125 String query = "DELETE FROM gift WHERE id = " + giftId; 126 String query2 = "DELETE FROM ratings WHERE giftId = " + giftId; 127 String query3 = "DELETE FROM comments WHERE giftId = " + giftId; 128 String query4 = "DELETE FROM gift_to_tag WHERE giftId = " + giftId; 129 try (Connection connection = dataSource.getConnection(); 130 Statement statement = connection.createStatement(); 131) { 132 statement.executeUpdate(query); 133 statement.executeUpdate(query2); 134 statement.executeUpdate(query3); 135 statement.executeUpdate(query4); 136 } catch (SQLException e) { 137 e.printStackTrace();</pre></div></div>	DA		Možemo koristiti PreparedStatement i ovdje, ali pošto se konkatencija vrši sa celim brojem (a ne sa stringom), ne može se desiti SQLI napad na ovom mestu.

	Tip	Naziv	Slika	False Positive	True Positive	Objašnjenje
	SQLI	Make sure using a dynamically formatted SQL query is safe here.	<div><div>Make sure using a dynamically formatted SQL query is safe here.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>SQL Injection</div></div><div><div>Review priority</div><div>HIGH</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div><div><div>src/...secursoftwaredevelopment/repository/GiftRepository.java</div><div><div>124</div><div>public void delete(int giftId) {</div><div>125</div><div>String query = "DELETE FROM gift WHERE id = " + giftId;</div><div>126</div><div>String query2 = "DELETE FROM ratings WHERE giftId = " + giftId;</div><div>127</div><div>String query3 = "DELETE FROM comments WHERE giftId = " + giftId;</div><div>128</div><div>String query4 = "DELETE FROM gift_to_tag WHERE giftId = " + giftId;</div><div>129</div><div>try (Connection connection = dataSource.getConnection();</div><div>130</div><div>Statement statement = connection.createStatement();</div><div>131</div><div>) {</div><div>132</div><div>statement.executeUpdate(query);</div><div>133</div><div>statement.executeUpdate(query2);</div><div>134</div><div>statement.executeUpdate(query3);</div><div>135</div><div>statement.executeUpdate(query4);</div><div>136</div><div>} catch (SQLException e) {</div><div>137</div><div>e.printStackTrace();</div><div></div><div>}</div></div></div></div> <div>DA</div> <div>Možemo koristiti PreparedStatement i ovdje, ali pošto se konkatenacija vrši sa celim brojem (a ne sa stringom), ne može se desiti SQLI napad na ovom mestu.</div>			
	SQLI	Make sure using a dynamically formatted SQL query is safe here.	<div><div>Make sure using a dynamically formatted SQL query is safe here.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>SQL Injection</div></div><div><div>Review priority</div><div>HIGH</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div><div><div>src/...secursoftwaredevelopment/repository/GiftRepository.java</div><div><div>124</div><div>public void delete(int giftId) {</div><div>125</div><div>String query = "DELETE FROM gift WHERE id = " + giftId;</div><div>126</div><div>String query2 = "DELETE FROM ratings WHERE giftId = " + giftId;</div><div>127</div><div>String query3 = "DELETE FROM comments WHERE giftId = " + giftId;</div><div>128</div><div>String query4 = "DELETE FROM gift_to_tag WHERE giftId = " + giftId;</div><div>129</div><div>try (Connection connection = dataSource.getConnection();</div><div>130</div><div>Statement statement = connection.createStatement();</div><div>131</div><div>) {</div><div>132</div><div>statement.executeUpdate(query);</div><div>133</div><div>statement.executeUpdate(query2);</div><div>134</div><div>statement.executeUpdate(query3);</div><div>135</div><div>statement.executeUpdate(query4);</div><div>136</div><div>} catch (SQLException e) {</div><div>137</div><div>e.printStackTrace();</div><div></div><div>}</div></div></div></div> <div>DA</div> <div>Možemo koristiti PreparedStatement i ovdje, ali pošto se konkatenacija vrši sa celim brojem (a ne sa stringom), ne može se desiti SQLI napad na ovom mestu.</div>			

	Tip	Naziv	Slika	False Positive	True Positive	Objašnjenje
	SQLI	Make sure using a dynamically formatted SQL query is safe here.	<div><div>Make sure using a dynamically formatted SQL query is safe here.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>SQL Injection</div></div><div><div>Review priority</div><div>HIGH</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div><div><div>src/_/securesoftwaredevelopment/repository/GiftRepository.java</div><div><pre>124 public void delete(int giftId) { 125 String query = "DELETE FROM gift WHERE id = " + giftId; 126 String query2 = "DELETE FROM ratings WHERE giftId = " + giftId; 127 String query3 = "DELETE FROM comments WHERE giftId = " + giftId; 128 String query4 = "DELETE FROM gift_to_tag WHERE giftId = " + giftId; 129 try (Connection connection = dataSource.getConnection(); 130 Statement statement = connection.createStatement(); 131) { 132 statement.executeUpdate(query); 133 statement.executeUpdate(query2); 134 statement.executeUpdate(query3); 135 statement.executeUpdate(query4); 136 } catch (SQLException e) { 137 e.printStackTrace(); 138 } 139 }</pre></div></div></div>	DA		Možemo koristiti PreparedStatement i ovdje, ali pošto se konkatencija vrši sa celim brojem (a ne sa stringom), ne može se desiti SQLi napad na ovom mestu.
	SQLI	Make sure using a dynamically formatted SQL query is safe here.	<div><div>Make sure using a dynamically formatted SQL query is safe here.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>SQL Injection</div></div><div><div>Review priority</div><div>HIGH</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div><div><div>src/_/securesoftwaredevelopment/repository/HashedUserRepository.java</div><div><pre>22 23 24 public HashedUser findUser(String username) { 25 String sqlQuery = "select passwordHash, salt, totKey from hashedUsers where username = '" + username + "'"; 26 try (Connection connection = dataSource.getConnection(); 27 Statement statement = connection.createStatement(); 28 ResultSet rs = statement.executeQuery(sqlQuery)) { 29 if (rs.next()) { 30 String passwordHash = rs.getString(1); 31 String salt = rs.getString(2); 32 String totKey = rs.getString(3); 33 return new HashedUser(username, passwordHash, salt, totKey); 34 } 35 } 36 }</pre></div></div></div>		DA	

	Tip	Naziv	Slika	False Positive	True Positive	Objašnjenje
	SQLi	Make sure using a dynamically formatted SQL query is safe here.	<div><div>Make sure using a dynamically formatted SQL query is safe here.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>SQL Injection</div></div><div><div>Review priority</div><div>HIGH</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div></div> <div><div>src/.../securesoftwaredevelopment/repository/PermissionRepository.java</div><div><pre>27 public List<Permission> findByRoleId(int roleId) { 28 List<Permission> permissions = new ArrayList<>(); 29 String query = "SELECT id, name FROM permissions WHERE id IN (SELECT permissionId FROM role_to_permissions WHERE 30 roleId=" + roleId + ")"; 31 try { 32 Connection connection = dataSource.getConnection(); 33 Statement statement = connection.createStatement(); 34 ResultSet rs = statement.executeQuery(query); 35 while (rs.next()) { 36 int id = rs.getInt(1); 37 String name = rs.getString(2); 38 permissions.add(new Permission(id, name)); 39 } 40 } catch (SQLException e) { 41 throw new RuntimeException(e); 42 } 43 }</pre></div></div>	DA		Možemo koristiti PreparedStatement i ovdje, ali pošto se konkatenacija vrši sa celim brojem (a ne sa stringom), ne može se desiti SQLi napad na ovom mestu.
	SQLi	Make sure using a dynamically formatted SQL query is safe here.	<div><div>Make sure using a dynamically formatted SQL query is safe here.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>SQL Injection</div></div><div><div>Review priority</div><div>HIGH</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div></div> <div><div>src/.../securesoftwaredevelopment/repository/PersonRepository.java</div><div><pre>43 List<Person> personList = new ArrayList<>(); 44 String query = "SELECT id, firstName, lastName, email FROM persons WHERE UPPER(firstName) like UPPER('%" + searchTerm + 45 "%') OR UPPER(lastName) like UPPER('%" + searchTerm + "%')"; 46 try { 47 Connection connection = dataSource.getConnection(); 48 Statement statement = connection.createStatement(); 49 ResultSet rs = statement.executeQuery(query); 50 while (rs.next()) { 51 personList.add(createPersonFromResultSet(rs)); 52 } 53 } 54 return personList; 55 }</pre></div></div>	DA		

	Tip	Naziv	Slika	False Positive	True Positive	Objašnjenje
	SQLI	Make sure using a dynamically formatted SQL query is safe here.	<div><div>Make sure using a dynamically formatted SQL query is safe here.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>SQL Injection</div></div><div><div>Review priority</div><div>HIGH</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div></div> <div><div>src/...securesoftwaredevelopment/repository/PersonRepository.java</div><div><pre>55 56 public Person get(String personId) { 57 String query = "SELECT id, firstName, lastName, email FROM persons WHERE id = " + personId; 58 try (Connection connection = dataSource.getConnection(); 59 Statement statement = connection.createStatement(); 60 ResultSet rs = statement.executeQuery(query)) { 61 while (rs.next()) { 62 return createPersonFromResultSet(rs); 63 } 64 } catch (SQLException e) { 65 e.printStackTrace(); 66 } 67 }</pre></div></div>		DA	
	SQLI	Make sure using a dynamically formatted SQL query is safe here.	<div><div>Make sure using a dynamically formatted SQL query is safe here.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>SQL Injection</div></div><div><div>Review priority</div><div>HIGH</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div></div> <div><div>src/...securesoftwaredevelopment/repository/PersonRepository.java</div><div><pre>71 72 public void delete(int personId) { 73 String query = "DELETE FROM persons WHERE id = " + personId; 74 try (Connection connection = dataSource.getConnection(); 75 Statement statement = connection.createStatement(); 76) { 77 statement.executeUpdate(query); 78 } catch (SQLException e) { 79 e.printStackTrace(); 80 } 81 }</pre></div></div>		DA	Možemo koristiti PreparedStatement i ovdje, ali pošto se konkatencija vrši sa celim brojem (a ne sa stringom), ne može se desiti SQLI napad na ovom mestu.

	Tip	Naziv	Slika	False Positive	True Positive	Objašnjenje
	SQLI	Make sure using a dynamically formatted SQL query is safe here.	<div><div>Make sure using a dynamically formatted SQL query is safe here.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>SQL Injection</div></div><div><div>Review priority</div><div>HIGH</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div></div> <div><div>src/.../securesoftwaredevelopment/repository/PersonRepository.java</div><div><pre>90 public void update(Person personUpdate) { 91 Person personFromDb = get(personUpdate.getId()); 92 String query = "UPDATE persons SET firstName = ?, lastName = ? + personUpdate.getLastName() + ", email = ? where id = " 93 + personUpdate.getId(); 94 95 try {Connection connection = dataSource.getConnection(); 96 PreparedStatement statement = connection.prepareStatement(query); 97 } { 98 String firstName = personUpdate.getFirstName() != null ? personUpdate.getFirstName() : personFromDb.getFirstName(); 99 String email = personUpdate.getEmail() != null ? personUpdate.getEmail() : personFromDb.getEmail(); 100 statement.setString(1, firstName); 101 statement.setString(2, email); 102 }</pre></div></div>		DA	
	SQLI	Make sure using a dynamically formatted SQL query is safe here.	<div><div>Make sure using a dynamically formatted SQL query is safe here.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>SQL Injection</div></div><div><div>Review priority</div><div>HIGH</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div></div> <div><div>src/.../securesoftwaredevelopment/repository/RatingRepository.java</div><div><pre>26 public void createOrUpdate(Rating rating) { 27 String query = "SELECT giftId, userId, rating FROM ratings WHERE giftId = ? + rating.getGiftId() + ? AND userId = ? + 28 rating.getUserId(); 29 String query2 = "update ratings SET rating = ? WHERE giftId = ? AND userId = ?"; 30 String query3 = "insert into ratings(giftId, userId, rating) values (?, ?, ?)"; 31 32 try {Connection connection = dataSource.getConnection(); 33 Statement statement = connection.createStatement(); 34 ResultSet rs = statement.executeQuery(query); 35 } { 36 if (rs.next()) { 37 PreparedStatement preparedStatement = connection.prepareStatement(query2); 38 preparedStatement.setInt(1, rating.getRating()); 39 preparedStatement.setInt(2, rating.getGiftId()); 40 } 41 }</pre></div></div>		DA	Možemo koristiti PreparedStatement i ovdje, ali pošto se konkatencija vrši sa celim brojem (a ne sa stringom), ne može se desiti SQLI napad na ovom mestu.

	Tip	Naziv	Slika	False Positive	True Positive	Objašnjenje
	SQLI	Make sure using a dynamically formatted SQL query is safe here.	<div><div>Make sure using a dynamically formatted SQL query is safe here.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>SQL Injection</div></div><div><div>Review priority</div><div>HIGH</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div></div> <div><div>src/...securesoftwaredevelopment/repository/RatingRepository.java</div><div><pre>53 public List<Rating> getAll(String giftId) { 54 List<Rating> ratingList = new ArrayList<>(); 55 String query = "SELECT giftId, userId, rating FROM ratings WHERE giftId = " + giftId; 56 try (Connection connection = dataSource.getConnection(); 57 Statement statement = connection.createStatement(); 58 ResultSet rs = statement.executeQuery(query)) { 59 while (rs.next()) { 60 ratingList.add(new Rating(rs.getInt(1), rs.getInt(2), rs.getInt(3))); 61 } 62 } catch (SQLException e) { 63 e.printStackTrace(); 64 } 65 }</pre></div></div>		DA	
	SQLI	Make sure using a dynamically formatted SQL query is safe here.	<div><div>Make sure using a dynamically formatted SQL query is safe here.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>SQL Injection</div></div><div><div>Review priority</div><div>HIGH</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div></div> <div><div>src/...securesoftwaredevelopment/repository/RoleRepository.java</div><div><pre>27 public List<Role> findByUserId(int userId) { 28 List<Role> roles = new ArrayList<>(); 29 String query = "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)) { 33 while (rs.next()) { 34 int id = rs.getInt(1); 35 String name = rs.getString(2); 36 roles.add(new Role(id, name)); 37 } 38 } 39 }</pre></div></div>		DA	Možemo koristiti PreparedStatement i ovdje, ali pošto se konkatencija vrši sa celim brojem (a ne sa stringom), ne može se desiti SQLI napad na ovom mestu.

	Tip	Naziv	Slika	False Positive	True Positive	Objašnjenje
	SQLI	Make sure using a dynamically formatted SQL query is safe here.	<div><div>Make sure using a dynamically formatted SQL query is safe here.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>SQL Injection</div></div><div><div>Review priority</div><div>HIGH</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div></div> <div><div>src/.../securesoftwaredevelopment/repository/UserRepository.java</div><div><pre>24 25 26 public User findUser(String username) { 27 String query = "SELECT id, username, password FROM users WHERE username='" + username + "'"; 28 try (Connection connection = dataSource.getConnection(); 29 Statement statement = connection.createStatement(); 30 ResultSet rs = statement.executeQuery(query)) { 31 if (rs.next()) { 32 int id = rs.getInt(1); 33 String username1 = rs.getString(2); 34 String password = rs.getString(3); 35 return new User(id, username1, password); 36 } 37 } 38 }</pre></div></div>		DA	
	SQLI	Make sure using a dynamically formatted SQL query is safe here.	<div><div>Make sure using a dynamically formatted SQL query is safe here.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>SQL Injection</div></div><div><div>Review priority</div><div>HIGH</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div></div> <div><div>src/.../securesoftwaredevelopment/repository/UserRepository.java</div><div><pre>41 42 43 public boolean validCredentials(String username, String password) { 44 String query = "SELECT username FROM users WHERE username='" + username + "' AND password='" + password + "'"; 45 try (Connection connection = dataSource.getConnection(); 46 Statement statement = connection.createStatement(); 47 ResultSet rs = statement.executeQuery(query)) { 48 return rs.next(); 49 } catch (SQLException e) { 50 e.printStackTrace(); 51 } 52 return false; 53 }</pre></div></div>		DA	

	Tip	Naziv	Slika	False Positive	True Positive	Objašnjenje
	SQLI	Make sure using a dynamically formatted SQL query is safe here.	<div><div><div><div>Make sure using a dynamically formatted SQL query is safe here.</div><div><div>Add Comment</div><div>Open in IDE</div><div> Get Permalink</div></div></div><div><div>Category</div><div>SQL Injection</div></div><div><div>Review priority</div><div>HIGH</div></div><div><div>Assignee</div><div>Not assigned </div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div><div></div></div></div><div><div>src/.../securesoftwaredevelopment/repository/UserRepository.java </div><div><div></div><pre>54 public void delete(int userId) { 55 String query = "DELETE FROM users WHERE id = " + userId; 56 try (Connection connection = dataSource.getConnection(); 57 Statement statement = connection.createStatement(); 58) { 59 statement.executeUpdate(query); 60 } catch (SQLException e) { 61 e.printStackTrace(); 62 } 63 } 64 }</pre></div></div></div>	DA		Možemo koristiti PreparedStatement i ovde, ali pošto se konkatencija vrši sa celim brojem (a ne sa stringom), ne može se desiti SQLi napad na ovom mestu.
	Insecure Configuration	Make sure this debug feature is deactivated before delivering the code in production.	<div><div><div><div>Make sure this debug feature is deactivated before delivering the code in production.</div><div><div>Add Comment</div><div>Open in IDE</div><div> Get Permalink</div></div></div><div><div>Category</div><div>Insecure Configuration</div></div><div><div>Review priority</div><div>LOW</div></div><div><div>Assignee</div><div>Not assigned </div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div><div></div></div></div><div><div>src/.../securesoftwaredevelopment/repository/CommentRepository.java </div><div><div></div><pre>28 try (Connection connection = dataSource.getConnection(); 29 Statement statement = connection.createStatement(); 30) { 31 statement.execute(query); 32 } catch (SQLException e) { 33 e.printStackTrace(); 34 } 35 } 36 37 public List<Comment> getAll(String giftId) { 38 List<Comment> commentList = new ArrayList<>();</pre></div></div></div>	DA		Ovakva ranjivost ispravlja se logovanjem greške. U suprotnom, napadač može zloupotrebiti podatke koji bi se ispisali. Isto rešenje treba primeniti i za ostale "True Positive" ranjivosti u nastavku.

	Tip	Naziv	Slika	False Positive	True Positive	Objašnjenje
	Insecure Configuration	Make sure this debug feature is deactivated before delivering the code in production.	<div><div>Make sure this debug feature is deactivated before delivering the code in production.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>Insecure Configuration</div></div><div><div>Review priority</div><div>LOW</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div><div><div>src/.../securesoftwaredevelopment/repository/CommentRepository.java</div><div><pre>42 ResultSet rs = statement.executeQuery(query)) { 43 while (rs.next()) { 44 commentList.add(new Comment(rs.getInt(1), rs.getInt(2), rs.getString(3))); 45 } 46 } catch (SQLException e) { 47 e.printStackTrace(); 48 } 49 return commentList; 50 } 51 } 52 }</pre></div></div></div>		DA	
	Insecure Configuration	Make sure this debug feature is deactivated before delivering the code in production.	<div><div>Make sure this debug feature is deactivated before delivering the code in production.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>Insecure Configuration</div></div><div><div>Review priority</div><div>LOW</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div><div><div>src/.../securesoftwaredevelopment/repository/GiftRepository.java</div><div><pre>35 while (rs.next()) { 36 Gift gift = createGiftFromResultSet(rs); 37 giftList.add(gift); 38 } 39 } catch (SQLException e) { 40 e.printStackTrace(); 41 } 42 return giftList; 43 } 44 } 45 public List<Gift> search(String searchTerm) throws SQLException {</pre></div></div></div>		DA	

	Tip	Naziv	Slika	False Positive	True Positive	Objašnjenje
	Insecure Configuration	Make sure this debug feature is deactivated before delivering the code in production.	<div><div>Make sure this debug feature is deactivated before delivering the code in production.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>Insecure Configuration</div><div>Review priority</div><div>LOW</div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div><div><div>src/.../securesoftwaredevelopment/repository/GiftRepository.java</div><div><pre>81 82 } 83 gift.setTags(giftTags); 84 return gift; 85 } catch (SQLException e) { 86 e.printStackTrace(); 87 } 88 89 return null; 90 } 91</pre></div></div></div>		DA	
	Insecure Configuration	Make sure this debug feature is deactivated before delivering the code in production.	<div><div>Make sure this debug feature is deactivated before delivering the code in production.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>Insecure Configuration</div><div>Review priority</div><div>LOW</div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div><div><div>src/.../securesoftwaredevelopment/repository/GiftRepository.java</div><div><pre>109 110 } { 111 statement2.setInt(1, (int) finalId); 112 statement2.setInt(2, tag.getId()); 113 statement2.executeUpdate(); 114 } catch (SQLException e) { 115 e.printStackTrace(); 116 } 117 }); 118 } catch (SQLException e) { 119 e.printStackTrace(); 120 } </pre></div></div></div>		DA	

	Tip	Naziv	Slika	False Positive	True Positive	Objašnjenje
	Insecure Configuration	Make sure this debug feature is deactivated before delivering the code in production.	<div>Make sure this debug feature is deactivated before delivering the code in production.</div> <div><div>Add CommentOpen in IDEGet Permalink</div><div>CategoryInsecure Configuration</div><div>Review priorityLOW</div><div>AssigneeNot assigned</div><div>Status: To review This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div> <div>src:/.../securesoftwaredevelopment/repository/GiftRepository.java</div> <div><pre>114 e.printStackTrace(); 115 } 116 }); 117 } 118 } catch (SQLException e) { 119 e.printStackTrace(); 120 } 121 return id; 122 } 123 124 public void delete(int giftId) {</pre></div>		DA	
	Insecure Configuration	Make sure this debug feature is deactivated before delivering the code in production.	<div>Make sure this debug feature is deactivated before delivering the code in production.</div> <div><div>Add CommentOpen in IDEGet Permalink</div><div>CategoryInsecure Configuration</div><div>Review priorityLOW</div><div>AssigneeNot assigned</div><div>Status: To review This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div> <div>src:/.../securesoftwaredevelopment/repository/GiftRepository.java</div> <div><pre>132 statement.executeUpdate(query); 133 statement.executeUpdate(query2); 134 statement.executeUpdate(query3); 135 statement.executeUpdate(query4); 136 } catch (SQLException e) { 137 e.printStackTrace(); 138 } 139 } 140 141 private Gift createGiftFromResultSet(ResultSet rs) throws SQLException { 142 int id = rs.getInt(1);</pre></div>		DA	

	Tip	Naziv	Slika	False Positive	True Positive	Objašnjenje
	Insecure Configuration	Make sure this debug feature is deactivated before delivering the code in production.	<div>Make sure this debug feature is deactivated before delivering the code in production. <a>Add Comment <a>Open in IDE <a>Get Permalink</div> <div>Category Insecure Configuration</div> <div>Review priority LOW</div> <div>Assignee Not assigned <a></div> <div>Status: To review This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div> <div>src/.../securesoftwaredevelopment/repository/HashedUserRepository.java</div> <div><pre>30 String salt = rs.getString(2); 31 String totpKey = rs.getString(3); 32 return new HashedUser(username, passwordHash, salt, totpKey); 33 } 34 } catch (SQLException e) { 35 e.printStackTrace(); 36 } 37 return null; 38 } 39 40 public void saveTotpKey(String username, String totpKey) {</pre></div>		DA	
	Insecure Configuration	Make sure this debug feature is deactivated before delivering the code in production.	<div>Make sure this debug feature is deactivated before delivering the code in production. <a>Add Comment <a>Open in IDE <a>Get Permalink</div> <div>Category Insecure Configuration</div> <div>Review priority LOW</div> <div>Assignee Not assigned <a></div> <div>Status: To review This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div> <div>src/.../securesoftwaredevelopment/repository/HashedUserRepository.java</div> <div><pre>44 statement.setString(1, totpKey); 45 statement.setString(2, username); 46 47 statement.executeUpdate(); 48 } catch (SQLException e) { 49 e.printStackTrace(); 50 } 51 } 52 } 53</pre></div>		DA	

	Tip	Naziv	Slika	False Positive	True Positive	Objašnjenje
	Insecure Configuration	Make sure this debug feature is deactivated before delivering the code in production.	<div>Make sure this debug feature is deactivated before delivering the code in production.</div> <div><div>Add CommentOpen in IDEGet Permalink</div><div><div>CategoryInsecure Configuration</div><div>Review priorityLOW</div><div>AssigneeNot assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div></div> <div><div>src/.../securesoftwaredevelopment/repository/PermissionRepository.java</div><div><pre>34 int id = rs.getInt(1); 35 String name = rs.getString(2); 36 permissions.add(new Permission(id, name)); 37 } 38 } catch (SQLException e) { 39 e.printStackTrace(); 40 } 41 return permissions; 42 } 43 } 44 }</pre></div></div> <td></td> <td>DA</td> <td></td>		DA	
	Insecure Configuration	Make sure this debug feature is deactivated before delivering the code in production.	<div>Make sure this debug feature is deactivated before delivering the code in production.</div> <div><div>Add CommentOpen in IDEGet Permalink</div><div><div>CategoryInsecure Configuration</div><div>Review priorityLOW</div><div>AssigneeNot assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div></div> <div><div>src/.../securesoftwaredevelopment/repository/PersonRepository.java</div><div><pre>32 ResultSet rs = statement.executeQuery(query)) { 33 while (rs.next()) { 34 personList.add(createPersonFromResultSet(rs)); 35 } 36 } catch (SQLException e) { 37 e.printStackTrace(); 38 } 39 return personList; 40 } 41 } 42 public List<Person> search(String searchTerm) throws SQLException {</pre></div></div> <td></td> <td>DA</td> <td></td>		DA	

	Tip	Naziv	Slika	False Positive	True Positive	Objašnjenje
	Insecure Configuration	Make sure this debug feature is deactivated before delivering the code in production.	<div><div>Make sure this debug feature is deactivated before delivering the code in production.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>Insecure Configuration</div></div><div><div>Review priority</div><div>LOW</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div></div> <div><div>src/.../securesoftwaredevelopment/repository/PersonRepository.java</div><div><pre>60 ResultSet rs = statement.executeQuery(query)) { 61 while (rs.next()) { 62 return createPersonFromResultSet(rs); 63 } 64 } catch (SQLException e) { 65 e.printStackTrace(); 66 } 67 return null; 68 } 69 }</pre></div></div> <td></td> <td>DA</td> <td></td>		DA	
	Insecure Configuration	Make sure this debug feature is deactivated before delivering the code in production.	<div><div>Make sure this debug feature is deactivated before delivering the code in production.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>Insecure Configuration</div></div><div><div>Review priority</div><div>LOW</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div></div> <div><div>src/.../securesoftwaredevelopment/repository/PersonRepository.java</div><div><pre>73 try (Connection connection = dataSource.getConnection(); 74 Statement statement = connection.createStatement(); 75) { 76 statement.executeUpdate(query); 77 } catch (SQLException e) { 78 e.printStackTrace(); 79 } 80 } 81 82 private Person createPersonFromResultSet(ResultSet rs) throws SQLException { 83 int id = rs.getInt(1);</pre></div></div> <td></td> <td>DA</td> <td></td>		DA	

	Tip	Naziv	Slika	False Positive	True Positive	Objašnjenje
	Insecure Configuration	Make sure this debug feature is deactivated before delivering the code in production.	<div><div>Make sure this debug feature is deactivated before delivering the code in production.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>Insecure Configuration</div></div><div><div>Review priority</div><div>LOW</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div><div><div>src/.../securesoftwaredevelopment/repository/PersonRepository.java</div><div><pre>98 String email = personUpdate.getEmail() != null ? personUpdate.getEmail() : personFromDb.getEmail(); 99 statement.setString(1, firstName); 100 statement.setString(2, email); 101 statement.executeUpdate(); 102 } catch (SQLException e) { 103 e.printStackTrace(); 104 } 105 } 106 } 107</pre></div></div></div>		DA	
	Insecure Configuration	Make sure this debug feature is deactivated before delivering the code in production.	<div><div>Make sure this debug feature is deactivated before delivering the code in production.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>Insecure Configuration</div></div><div><div>Review priority</div><div>LOW</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div><div><div>src/.../securesoftwaredevelopment/repository/RatingRepository.java</div><div><pre>44 preparedStatement.setInt(2, rating.getUserId()); 45 preparedStatement.setInt(3, rating.getRating()); 46 preparedStatement.executeUpdate(); 47 } 48 } catch (SQLException e) { 49 e.printStackTrace(); 50 } 51 } 52 53 public List<Rating> getAll(String giftId) { 54 List<Rating> ratingList = new ArrayList<>(); </pre></div></div></div>		DA	

	Tip	Naziv	Slika	False Positive	True Positive	Objašnjenje
	Insecure Configuration	Make sure this debug feature is deactivated before delivering the code in production.	<div>Make sure this debug feature is deactivated before delivering the code in production.</div> <div><div>Add CommentOpen in IDEGet Permalink</div><div><div>CategoryInsecure Configuration</div><div>Review priorityLOW</div><div>AssigneeNot assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div></div> <div><div>src/.../securesoftwaredevelopment/repository/RatingRepository.java</div><div><pre>58 ResultSet rs = statement.executeQuery(query)) { 59 while (rs.next()) { 60 ratingList.add(new Rating(rs.getInt(1), rs.getInt(2), rs.getInt(3))); 61 } 62 } catch (SQLException e) { 63 e.printStackTrace(); 64 } 65 return ratingList; 66 } 67 } 68 }</pre></div></div> <td></td> <td>DA</td> <td></td>		DA	
	Insecure Configuration	Make sure this debug feature is deactivated before delivering the code in production.	<div>Make sure this debug feature is deactivated before delivering the code in production.</div> <div><div>Add CommentOpen in IDEGet Permalink</div><div><div>CategoryInsecure Configuration</div><div>Review priorityLOW</div><div>AssigneeNot assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div></div> <div><div>src/.../securesoftwaredevelopment/repository/RoleRepository.java</div><div><pre>34 int id = rs.getInt(1); 35 String name = rs.getString(2); 36 roles.add(new Role(id, name)); 37 } 38 } catch (SQLException e) { 39 e.printStackTrace(); 40 } 41 } 42 return roles; 43 } 44 }</pre></div></div> <td></td> <td>DA</td> <td></td>		DA	

	Tip	Naziv	Slika	False Positive	True Positive	Objašnjenje
	Insecure Configuration	Make sure this debug feature is deactivated before delivering the code in production.	<div><div>Make sure this debug feature is deactivated before delivering the code in production.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>Insecure Configuration</div></div><div><div>Review priority</div><div>LOW</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div><div><div>src/.../securesoftwaredevelopment/repository/TagRepository.java</div><div><pre>30 ResultSet rs = statement.executeQuery(query)) { 31 while (rs.next()) { 32 tagList.add(new Tag(rs.getInt(1), rs.getString(2))); 33 } 34 } catch (SQLException e) { 35 e.printStackTrace(); 36 } 37 return tagList; 38 } 39 } 40 }</pre></div></div></div>		DA	
	Insecure Configuration	Make sure this debug feature is deactivated before delivering the code in production.	<div><div>Make sure this debug feature is deactivated before delivering the code in production.</div><div><div>Add Comment</div><div>Open in IDE</div><div>Get Permalink</div></div><div><div>Category</div><div>Insecure Configuration</div></div><div><div>Review priority</div><div>LOW</div></div><div><div>Assignee</div><div>Not assigned</div></div><div><div>Status: To review</div><div>This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div></div><div><div>src/.../securesoftwaredevelopment/repository/UserRepository.java</div><div><pre>32 String username = rs.getString(2); 33 String password = rs.getString(3); 34 return new User(id, username, password); 35 } 36 } catch (SQLException e) { 37 e.printStackTrace(); 38 } 39 return null; 40 } 41 } 42 public boolean validCredentials(String username, String password) {</pre></div></div></div>		DA	

	Tip	Naziv	Slika	False Positive	True Positive	Objašnjenje
	Insecure Configuration	Make sure this debug feature is deactivated before delivering the code in production.	<div>Make sure this debug feature is deactivated before delivering the code in production. Add Comment Open in IDE Get Permalink</div> <div>Category Insecure Configuration</div> <div>Review priority LOW</div> <div>Assignee Not assigned ✎</div> <div>Status: To review This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div> <div>src/.../securesoftwaredevelopment/repository/UserRepository.java</div> <div><pre>44 try (Connection connection = dataSource.getConnection(); 45 Statement statement = connection.createStatement(); 46 ResultSet rs = statement.executeQuery(query)) { 47 return rs.next(); 48 } catch (SQLException e) { 49 e.printStackTrace(); 50 } 51 return false; 52 } 53 54 public void delete(int userId) {</pre></div>		DA	
	Insecure Configuration	Make sure this debug feature is deactivated before delivering the code in production.	<div>Make sure this debug feature is deactivated before delivering the code in production. Add Comment Open in IDE Get Permalink</div> <div>Category Insecure Configuration</div> <div>Review priority LOW</div> <div>Assignee Not assigned ✎</div> <div>Status: To review This Security Hotspot needs to be reviewed to assess whether the code poses a risk.</div> <div>src/.../securesoftwaredevelopment/repository/UserRepository.java</div> <div><pre>56 try (Connection connection = dataSource.getConnection(); 57 Statement statement = connection.createStatement(); 58) { 59 statement.executeUpdate(query); 60 } catch (SQLException e) { 61 e.printStackTrace(); 62 } 63 } 64 } 65</pre></div>		DA	