FB.LDAP\_INJECTION

Ошибка "The query could be vulnerable to LDAP injection" указывает на потенциальную уязвимость вашего кода к атаке LDAP-инъекции. Это означает, что ваш запрос к LDAP-серверу формируется таким образом, что злоумышленник может внедрить вредоносный код или изменить его выполнение, используя специально сформированные строки.

LDAP (Lightweight Directory Access Protocol) инъекция аналогична SQL-инъекции, но применяется к LDAP-запросам. Злоумышленник может внедрять команды LDAP в ваш запрос, чтобы получить несанкционированный доступ к данным, выполнить поддельные запросы или воздействовать на работу LDAP-сервера.

Таблица №1 – Основные характеристики детектора FB.LDAP\_INJECTION

|  |  |
| --- | --- |
| Категория критичности | Minor |
| Надежность | Unknown |
| Источник | SpotBugs |
| Тип ошибки | LDAP Injection |
| CWE | CWE90 |
| CVE | --- |
| Возможные последствия | Обход аутентификации; утечка конфиденциальных данных из LDAP-каталога; выполнение несанкционированных запросов |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Потенциально небезопасное | Корректная конструкция |
| public static void incorrectTest(String username, String password) {  try {  String filter = "(uid=" + username + ")"; // ОШИБКА: конкатенация без экранирования  LdapContext ctx = new InitialLdapContext();  SearchControls ctrl = new SearchControls();  ctrl.setSearchScope(SearchControls.SUBTREE\_SCOPE);  NamingEnumeration<SearchResult> res = ctx.search("ou=users,dc=example,dc=com", filter, ctrl);  if (res.hasMore()) {  System.out.println("User found (VULNERABLE TO LDAP INJECTION)");  } else {  System.out.println("User not found");  }  } catch (Exception e) {  e.printStackTrace();  }  } | public static void correctTest(String username, String password) {  try {  String sanitizedUsername = LdapEncoder.filterEncode(username); // Экранирование специальных символов  String filter = "(uid=" + sanitizedUsername + ")";  LdapContext ctx = new InitialLdapContext();  SearchControls ctrl = new SearchControls();  ctrl.setSearchScope(SearchControls.SUBTREE\_SCOPE);  NamingEnumeration<SearchResult> res = ctx.search("ou=users,dc=example,dc=com", filter, ctrl);  if (res.hasMore()) {  System.out.println("User found (SECURE)");  } else {  System.out.println("User not found");  }  } catch (Exception e) {  e.printStackTrace();  }  } |