HARDCODED\_PASSWORD

Этот детектор указывает на использование встроенных в программу фиксированных паролей, что небезопасно.

Таблица №1 – Основные характеристики детектора HARDCODED\_PASSWORD

|  |  |
| --- | --- |
| Категория критичности | Undefined |
| Надежность | Low |
| Источник | SvEng |
| Тип ошибки | Hardcoded Credentials |
| CWE | CWE-259 |
| CVE | --- |
| Возможные последствия | Компрометация учетных данных, несанкционированный доступ к системе, сложность ротации паролей |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Потенциально небезопасное | Корректная конструкция |
| public static void incorrectTest() {  String username = "admin";  String password = "P@ssw0rd123!"; // ОШИБКА: пароль в открытом виде  authenticate(username, password);  } | public static void correctTest() {  String username = "admin";  String password = System.getenv("DB\_PASSWORD"); // Безопасно: из переменных окружения  if (password != null) {  authenticate(username, password);  } else {  System.err.println("Пароль не установлен в переменных окружения");  }  } |