Федеральное агентство связи
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)

Кафедра ПМиК

Практическое задание №9-10

по дисциплине «Сетевые базы данных»

“Динамический SQL и PL\SQL” и “SQL инъекции”

Выполнили: студенты группы МГ-211

Стояк Ю.К.

Бурдуковский И.А.

Проверил: Приставка П.А.

Новосибирск, 2023

Оглавление

Задание

- Разработать процедуру, реализующую вывод содержимого таблицы SAL на основании ограничений, задаваемых на поля: SNAME, CITY.
- Предусмотреть возможность задания ограничений только на одно из полей.
- Реализовать возможность использования при формировании ограничений на строки таблицы SAL операторов AND и OR.
- Необходимая для формирования ограничений информация передается в качестве параметров процедуры.

1. Проанализируйте написанное в рамках выполнения лабораторной работы 9 приложение на уязвимость к SQL-инъекциям.
2. В случае обнаруженной уязвимости реализуйте практический пример атаки на приложение
3. Перечислите основные способы устранения уязвимости кода к SQL-инъекциям и в случае необходимости внесите необходимые изменения в код приложения для устранения уязвимостей.

Выполнение

1. Проанализируйте написанное в рамках выполнения лабораторной работы 9 приложение на уязвимость к SQL-инъекциям.
Скрипт:

```
CREATE OR REPLACE PROCEDURE get_sal (scity_in IN VARCHAR2, and_or_in
IN VARCHAR2, sname_in IN VARCHAR2 := NULL)

IS

   TYPE SAL_T IS REF CURSOR;

   sal_cursor SAL_T;

   sal_row sal%ROWTYPE;

   sal_sql VARCHAR2(32767);

BEGIN

      IF sname_in is NULL THEN

         sal_sql := 'SELECT * FROM sal WHERE city = :1 ';

      ELSE

         sal_sql := 'SELECT * FROM sal WHERE city = :1 ' || and_or_in || ' sname =
NVL(:2,sname)';

      END IF;

   OPEN sal_cursor FOR sal_sql

      USING scity_in, sname_in;

      LOOP

         FETCH sal_cursor INTO sal_row;

         EXIT WHEN sal_cursor%NOTFOUND;

         DBMS_OUTPUT.PUT_LINE(sal_row.snum || ' ' || sal_row.sname || ' ' ||
sal_row.city || ' ' || sal_row.comm);

      END LOOP;

   CLOSE sal_cursor;

END get_sal;
```

Уязвимость может быть в строке: sql_query := 'SELECT * FROM sal WHERE city = :1 ' || and_or_in || ' sname = NVL(:2,sname)'; На вход подается строка и нет проверки на то, что в ней ней другого, вредоносного скрипта.

2. В случае обнаруженной уязвимости реализуйте практический пример атаки на приложение.

```
BEGIN
    get_sal('London', 'or 1 = 1 or', 'Anybody');
END;
```

3. Перечислите основные способы устранения уязвимости кода к SQL-инъекциям и в случае необходимости внесите необходимые изменения в код приложения для устранения уязвимостей.

```
CREATE OR REPLACE PROCEDURE get_sal (scity_in IN VARCHAR2, and_or_in
IN VARCHAR2, sname_in IN VARCHAR2 := NULL)
IS
   TYPE SAL_T IS REF CURSOR;
   sal_cursor SAL_T;
   sal_record sal%ROWTYPE;
   sql_query VARCHAR2(32767);
BEGIN
   IF UPPER(and_or_in) = 'OR' THEN
      IF sname_in = NULL THEN
         sql_query := 'SELECT * FROM sal WHERE city = NVL(:1, city)';
      ELSE
         sql_query := 'SELECT * FROM sal WHERE city = NVL(:1, city) OR sname
= :2';
      END IF;
   ELSIF UPPER(and_or_in) = 'AND' THEN
      sql_query := 'SELECT * FROM sal WHERE city = NVL(:1, city) AND sname =
NVL(:2, sname)';
```

```
    END IF;
    IF sql_query is null THEN
          DBMS_OUTPUT.PUT_LINE('Не атакуйте!');
        RETURN;
       END IF;
    OPEN sal_cursor FOR sql_query
       USING scity_in, sname_in;
       LOOP
          FETCH sal_cursor INTO sal_record;
          EXIT WHEN sal_cursor%NOTFOUND;
          DBMS_OUTPUT.PUT_LINE(sal_record.snum || ' ' || sal_record.sname || ' ' ||
sal_record.city || ' ' || sal_record.comm);
       END LOOP;
    CLOSE sal_cursor;
END get_sal;
```

Проверка:

```
  BEGIN
     DBMS_OUTPUT.PUT_LINE('OR:');
     get_sal ('Barcelona', 'OR', 'Rifkin');
     DBMS_OUTPUT.PUT_LINE('AND:');
     get_sal ('Barcelona', 'AND', 'Rifkin');
     DBMS_OUTPUT.PUT_LINE('atact:');
     get_sal ('Barcelona', 'or 1=1 or', 'Rifkin');
  END;
```

Вывод:

OR:
1007 Rifkin Barcelona .15
AND:
1007 Rifkin Barcelona .15
atact:
Не атакуйте!