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: студентs группы МГ-211

Стояк Ю.К.

Бурдуковский И.А.

Проверил: Приставка П.А.

Новосибирск, 2023

Оглавление

[Задание 3](#_Toc96693268)

[Выполнение 4](#_Toc96693269)

# 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!