**Министерство науки и высшего образования Российской Федерации**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

**Факультет безопасности информационных технологий**

**Дисциплина:**

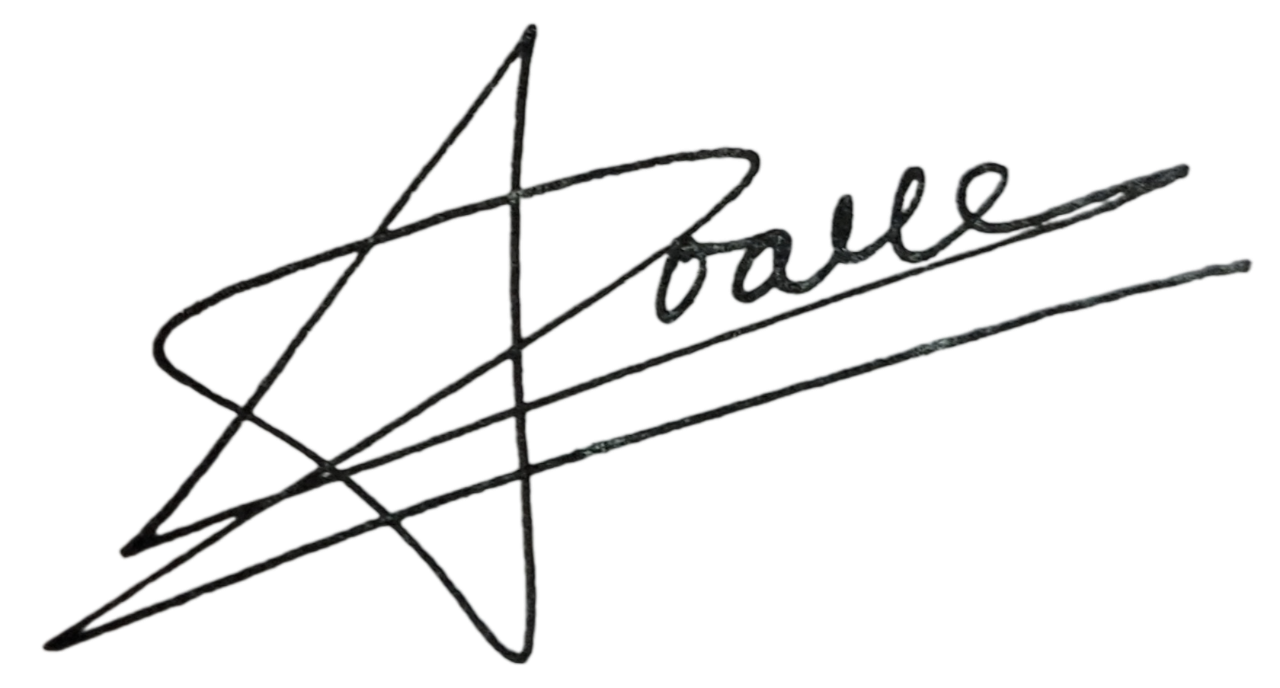
«Информационная безопасность баз данных»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №6**

«SQL-инъекции»

**Выполнили:**

Чу Ван Доан, студент группы N3247

**

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

**Проверил:**

**Волков А.Г.**

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(отметка о выполнении)

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись

Санкт-Петербург

2024 г.

**Содержание**

[Содержание 3](#_heading=h.gjdgxs)

[1](#_heading=h.30j0zll) SQL-инъекции 5

[1.1](#_heading=h.1fob9te) Цель работы 5

[1.2](#_heading=h.3znysh7) Задание 5

[1.3](#_heading=h.1t3h5sf) Ход работы 5

[1.3.1](#_heading=h.4d34og8) Задание 1 5

[1.3.2](#_heading=h.2s8eyo1) Задание 2 6

[1.3.3](#_heading=h.17dp8vu) Задание 3 6

[Заключение 8](#_heading=h.3rdcrjn)

# SQL-инъекции

## Цель работы

Получение навыков SQL-инъекций.

## Задание

### Задание 1: В случае объединения таблиц покажите, как злоумышленник может узнать количество столбцов второй таблицы.

### Задание 2: Предложите подход для получения структуры базы данных (включая название столбцов таблицы).

### Задание 3:  Покажите пример использования подготовленных параметров для вашего любимого языка программирования.

## Ход работы

### Задание 1

Создадим таблицу students.

Graphical user interface, text

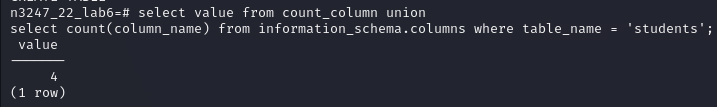
Description automatically generated

1. Создание таблицы students



1. Создание таблицы count\_column

Узнаем количество столбцов таблицы с помощью information\_schema.columns.



1. Поиск количества column

### Задание 2

С помощью information.columns, мы можем узнать структуру базы данных.

Text

Description automatically generated

1. Подход для получения структуры базы данных

### Задание 3

Создадим таблицу info\_user.

Text

Description automatically generated

1. Создание таблицы info\_user

Text

Description automatically generated

1. Код

A screenshot of a computer

Description automatically generated with medium confidence

1. Результат использования подготовленных параметров для Python

Text

Description automatically generated

1. Результат использования подготовленных параметров для Python

В этом примере мы используем библиотеку ‘psycopg2’ для подключения к PostgreSQL, создаём курсор и выполняем подготовленный запрос с использованием параметров (‘%s’). Затем мы передаем кортеж с данными для вставки (‘username’ и ‘password’) в качестве второго аргумента метода ‘execute’. Это предотвращает SQL-инъекцию и делает код более читаемым и безопасным.

**Заключение**

В ходе выполнения лабораторной работы был изучен теоретический материал по SQL-инъекциям. Приобретенные знания были применены на практике в СУБД PostgreSQL.