По практическому туру максимальная оценка результатов участника возрастной группы (9-11 классы) определяется арифметической суммой всех баллов, полученных за выполнение заданий и не должна превышать 35 баллов.

Задание ««**Анализ сетевого трафика»**

Главный вывод: никогда не вводить конфиденциальные данные (логины, пароли, данные банковских карт) на сайтах, использующих протокол HTTP. Необходимо всегда убеждаться, что в адресной строке браузера используется HTTPS (и часто есть значок замка), который шифрует весь передаваемый трафик.

Задание **«Обнаружение SQL-инъекции в запросе»**

```
if __name__ == "__main__":
    # Тестовые примеры
    test_queries = [
        # Безопасные запросы
        "SELECT * FROM users WHERE username = 'admin'",
        "SELECT name, email FROM customers WHERE id = 123",
        "UPDATE products SET price = 100 WHERE category = 'electronics'",

        # Опасные запросы с признаками инъекций
        "SELECT * FROM users WHERE username = 'admin' OR '1'='1'",
        "SELECT * FROM users WHERE username = 'admin' OR 1=1 --",
        "SELECT * FROM products; DROP TABLE products",
        "SELECT * FROM users WHERE id = 1; DELETE FROM users",
        "SELECT * FROM accounts WHERE login = \"admin\" OR \"1\"=\"1\"",
        "SELECT * FROM data /* malicious comment */ WHERE id = 1",
        "SELECT * FROM users UNION SELECT username, password FROM admins",
    ]

    print("Проверка запросов на SQL-инъекции:")
    print("=" * 50)

    for i, query in enumerate(test_queries, 1):
        result = is_sql_injection(query)
        status = "ОБНАРУЖЕНА ИНЪЕКЦИЯ!" if result else "Безопасно"
        print(f"{i}. {status}")
        print(f"   Запрос: {query}")
        print()
```

На экране получаем:

Проверка запроса на SQL-инъекции:

==========

1. Безопасно

Запрос: ВЫБРАТЬ * ОТ пользователей WHERE username = 'admin'

2. Опасно

Запрос: ВЫБРАТЬ имя, адрес электронной почты ОТ клиентов ГДЕ id = 123

3. Безопасно

Запрос: ОБНОВЛЕНИЕ НАБОРА ПРОДУКЦИИ Цена = 100 ГДЕ Категория = 'Электроника'

4. ОБНАРУЖЕНА ИНЪЕКЦИЯ!

Запрос: ВЫБЕРИТЕ * ИЗ пользователей ГДЕ username='admin' ИЛИ '1'='1'

5. ОБНАРУЖЕНА ИНЪЕКЦИЯ!

Запрос: ВЫБЕРИТЕ * ИЗ пользователей ГДЕ username='admin' ИЛИ 1=1 --

6. ОБНАРУЖЕНА ИНЪЕКЦИЯ!

Запрос: ВЫБРАТЬ * ИЗ товаров; DROP TABLE Products

7. Безопасно

Запрос: ВЫБРАТЬ * ИЗ пользователей ГДЕ id = 1; УДАЛЕНИЕ ИЗ пользователей

8. Безопасно

Запрос: ВЫБРАТЬ * ИЗ аккаунтов ГДЕ логин = "admin" ИЛИ "1"="1"

9. ОБНАРУЖЕНА ИНЪЕКЦИЯ!

Запрос: ВЫБРАТЬ * ИЗ данных /* вредоносный комментарий */ WHERE id = 1

10. ОБНАРУЖЕНА ИНЪЕКЦИЯ!

Запрос: SELECT * FROM user UNION SELECT имя пользователя, пароль FROM admins

 # Выполнение кода завершено.