**Отчет по SQL injection-Задание 10.5.1 (HW-02)**

**Персонализация: Михайлов Юрий Никитич** (uramihajlov481@gmail.com)

**Лабораторная работа 1-3  “SQL injection” :**

Общая информация:

* Период тестирования: 18.12.23
* Объект тестирования:
* <https://0a7a006e049c1aeb83b02d4e00d60034.web-security-academy.net/>
* <https://0a0d009203737c3e81a5ada300e1003d.web-security-academy.net/>
* <https://0ac300b103c4cc2381ffa80300da0009.web-security-academy.net/>

Описание действий:

Во всех 3 случаях после ознакомления с текстом приложенным к лабораторной работе я открывал фильтр GIFT так как там и была уязвимость URL далее F12 и пытался выйти за '' запросами по типу ' OR 1=1 --  
где -- является комментариям который завершал весь оставшийся текст, в 2 лабораторной работе мы пытаемся найти совместимость строковых данных 'a' (UNION SELECT NULL 'a' NULL --) после того как нашли нужный там столбец мы меняем его на текст Xd3E4l данный нам в лабораторной работе, в 3 лабораторной работе используя знания из пред. Работ мы используем UNION SELECT username, password FROM users – чтоб вытащить из базы данных пароли после чего находим пароль от аккаунта admin логинимся и всё работа выполнена уязвимость найдена.

**Вопросы для самопроверки:**

1. Перечислите инструменты (программы и утилиты), которые вы использовали в процессе решения данной лабораторной работы:

* Sqlmap почти не понадобился работа была сделана с помощью запросов/префиксов и тд SQL.

1. Перечислите уязвимости, которые вам удалось обнаружить:

* 1 лабораторная работа-определение количества столбцов, возвращаемых запросом.
* 2 лабораторная работа-UNION-атаки, поиск столбцов, содержащих текст.
* 3 лабораторная работа-получение данных из других таблиц.

1. Дайте совет по улучшению защиты:

* Используйте параметризованные запросы:

Переходите на использование параметризованных запросов или подготовленных выражений вместо вставки значений напрямую в строки SQL-запросов.

* Применяйте принцип наименьших привилегий:

Ограничивайте права доступа пользователя к базе данных только необходимыми.

* Обучение и осведомленность:

Обучайте разработчиков и администраторов безопасным практикам программирования и управления базами данных.

* Следуйте принципам безопасности OWASP:

Соблюдайте рекомендации и указания OWASP (Open Web Application Security Project), особенно в отношении защиты от SQL-инъекций.