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.

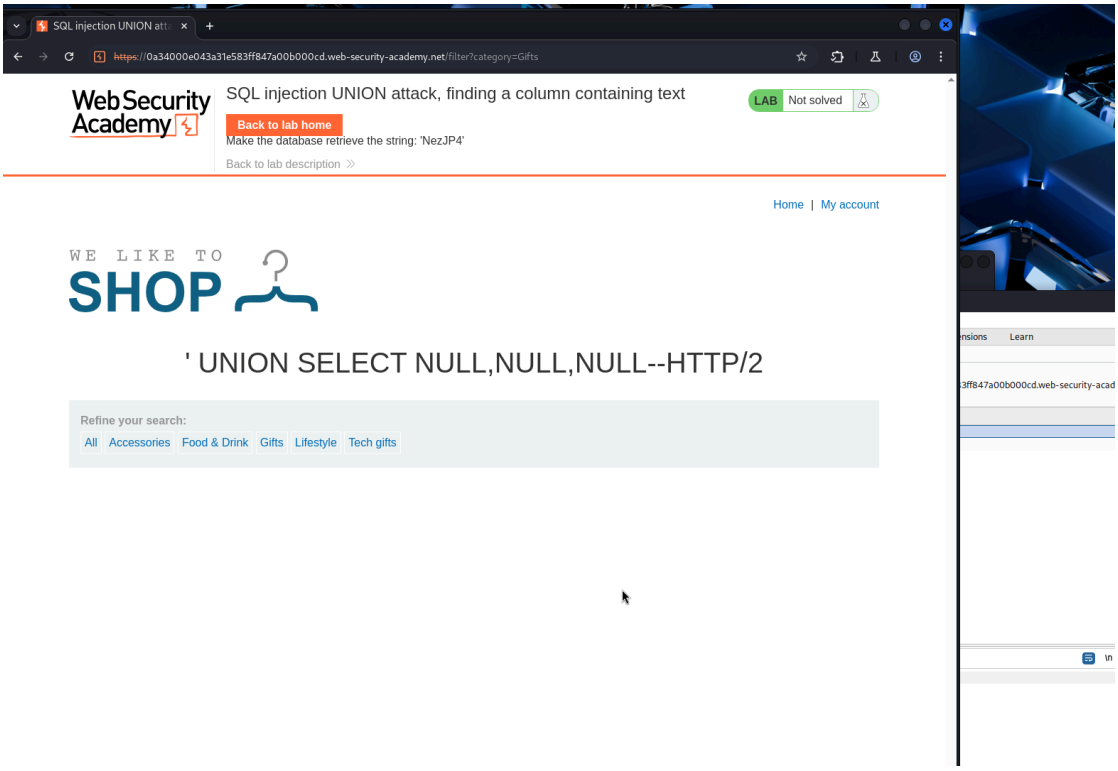
Задача — определить, сколько столбцов возвращает исходный запрос, чтобы правильно построить атаку UNION.

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.

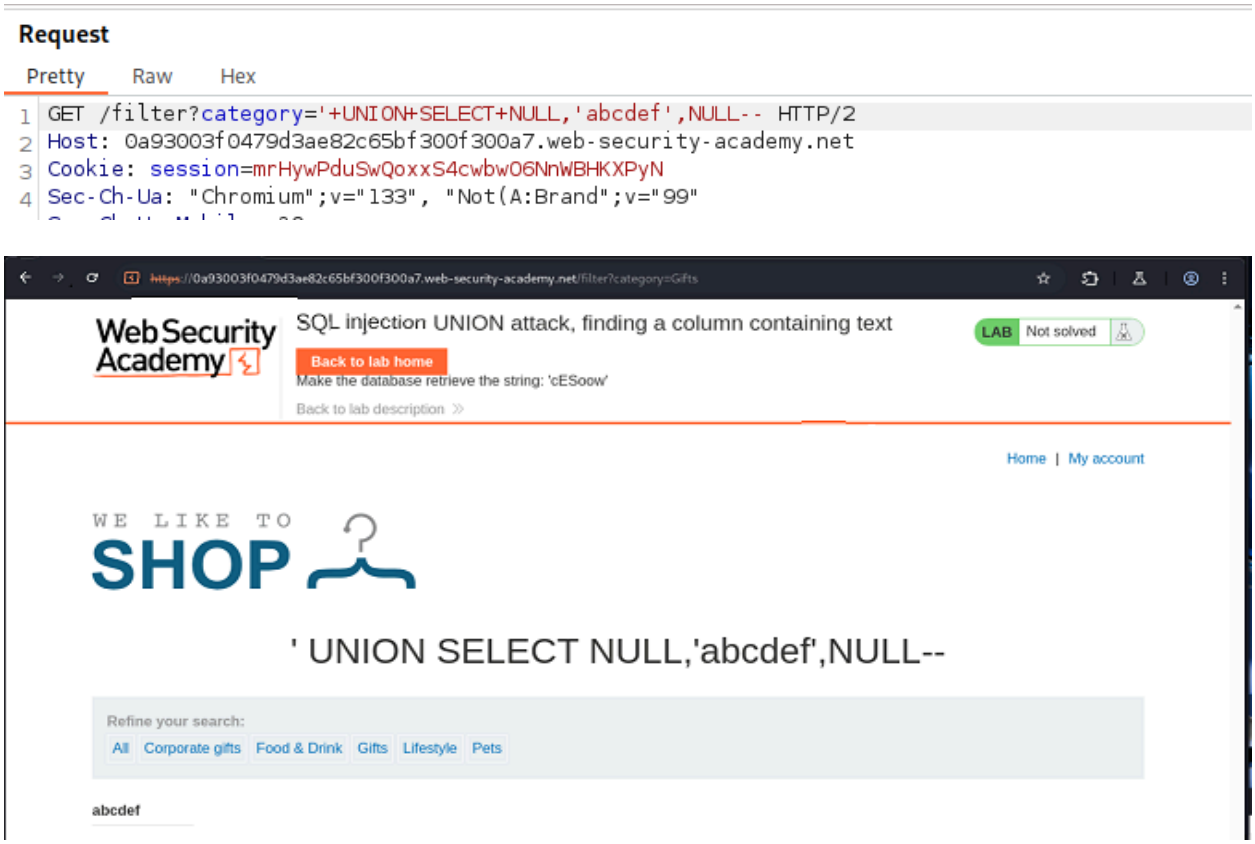
Определим количество столбцов, возвращаемых запросом. запрос возвращает три столбца, используя следующую полезную нагрузку в category параметре. Для этого заменим каждый ноль случайным значением, например (Лаборатория предоставила случайное значение 'cESoow'):

'+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:



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: