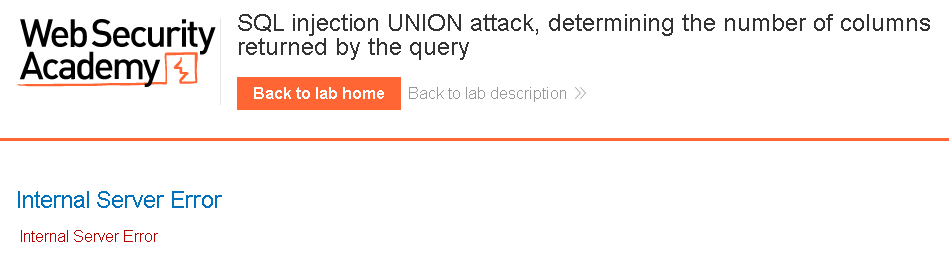
**SF 10.5.1**

[*Лабораторная 1*](https://portswigger.net/web-security/sql-injection/union-attacks/lab-determine-number-of-columns) *- SQL injection UNION attack, determining the number of columns returned by the query*

Используем инструмент Burp Suite.

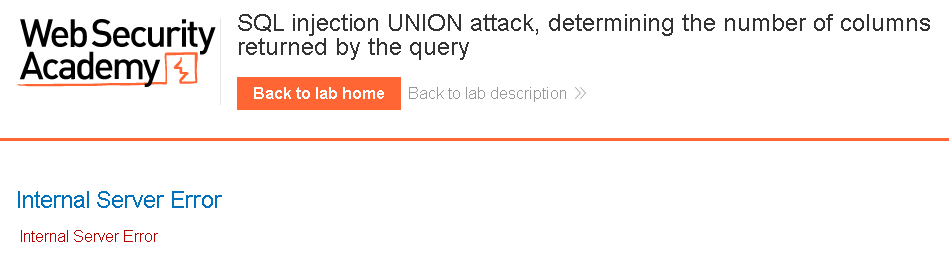
Заходим на <https://0a9d00480344cb6fc0c7fb1500e300aa.web-security-academy.net/filter?category=Tech+gifts>

Изменяем урл на <https://0a9d00480344cb6fc0c7fb1500e300aa.web-security-academy.net/filter?category=>’ и видим ошибку:

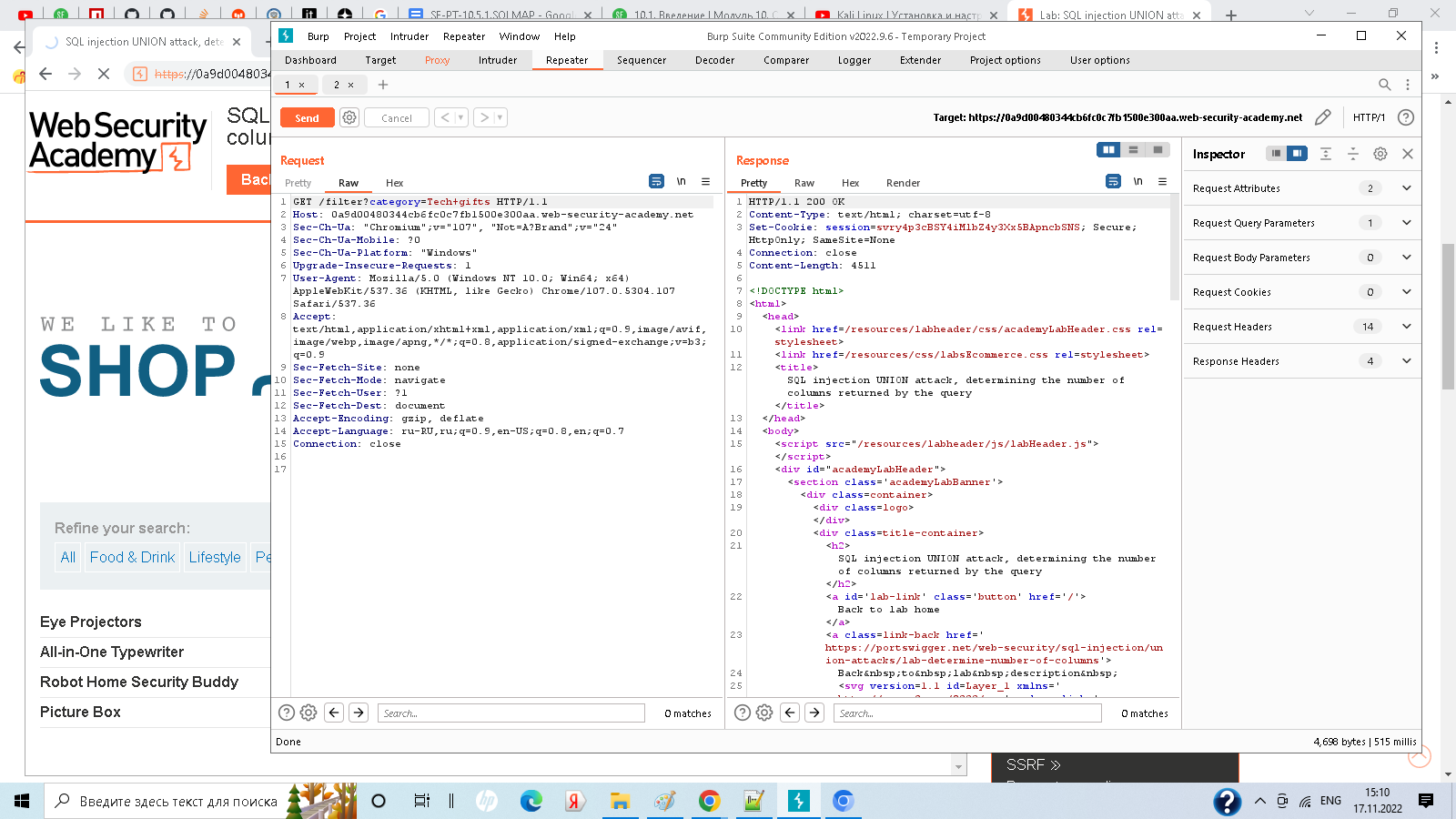


Допишем запрос UNION:

[https://0a9d00480344cb6fc0c7fb1500e300aa.web-security-academy.net/filter?category=%27%20UNION%20select%20NILL%20–](https://0a9d00480344cb6fc0c7fb1500e300aa.web-security-academy.net/filter?category=%27%20UNION%20select%20NILL%20%E2%80%93), видим ту же ошибку:



Открываем Burp Suite, идем на закладку Proxy, включаем прокси. Предварительно приостановила антивирусник.

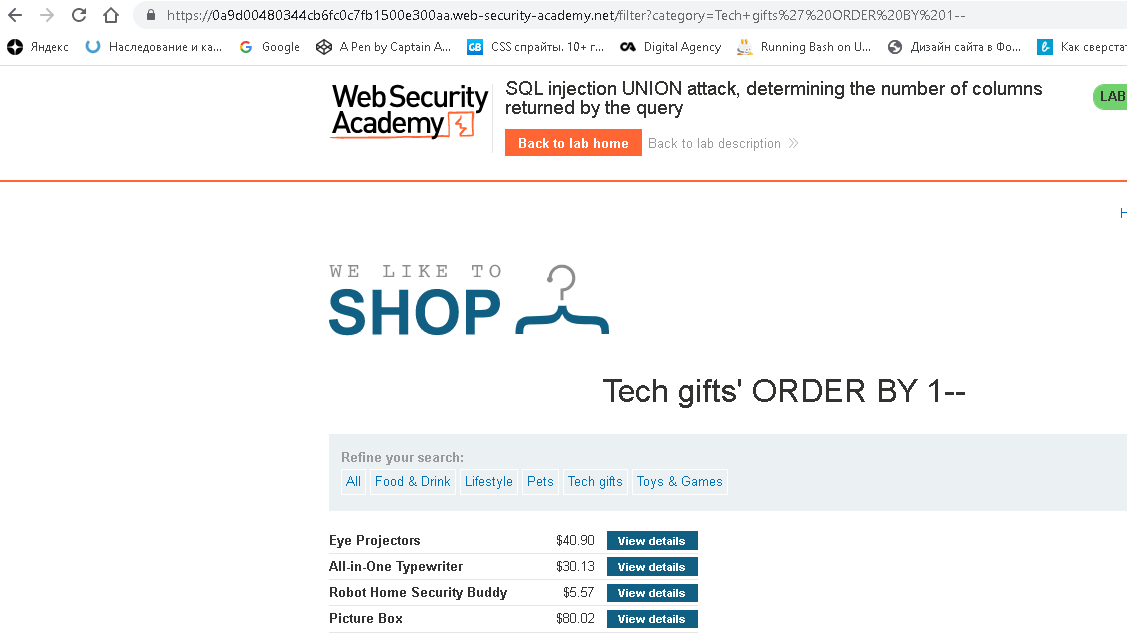


В поле **Request** в первой строке поэтапно каждый раз добавляем запрос(см.выделено цветом):

GET /filter?category=Tech gifts’+UNION+select+NULL,+NULL,+NULL–

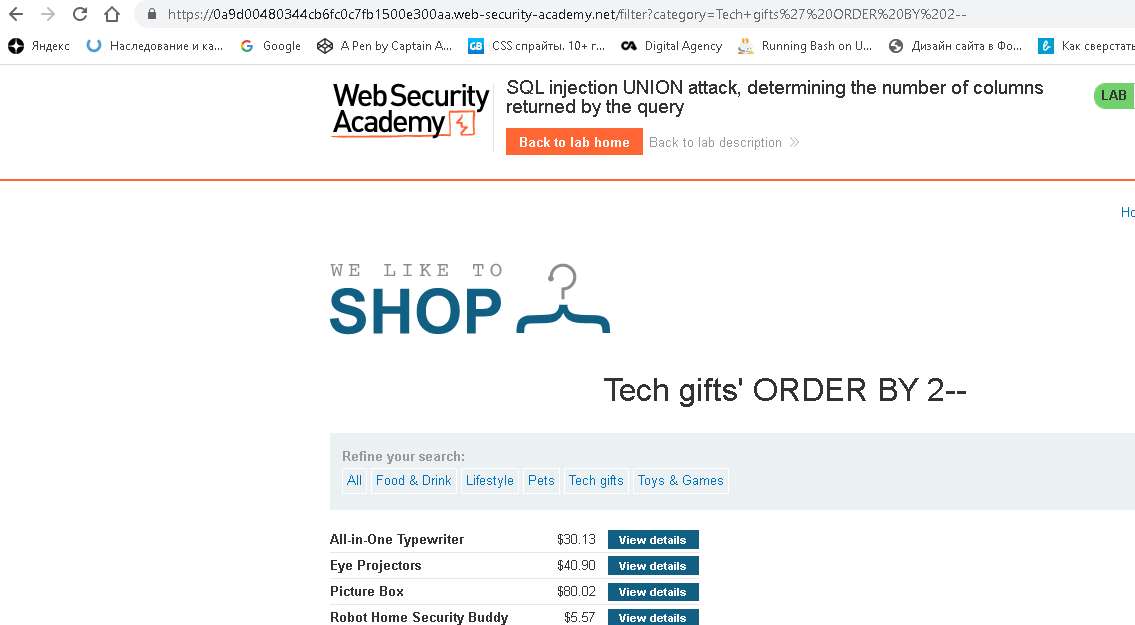
и в поле **Response** смотрим не ушла ли ошибка **Internal Server Error**.

Ошибка ушла при 3\*NULL. Проверим 4 или 3 колонки в результате, указывая в урле поочередно ORDER BY 1– и, проверяя вывелись ли колонки.



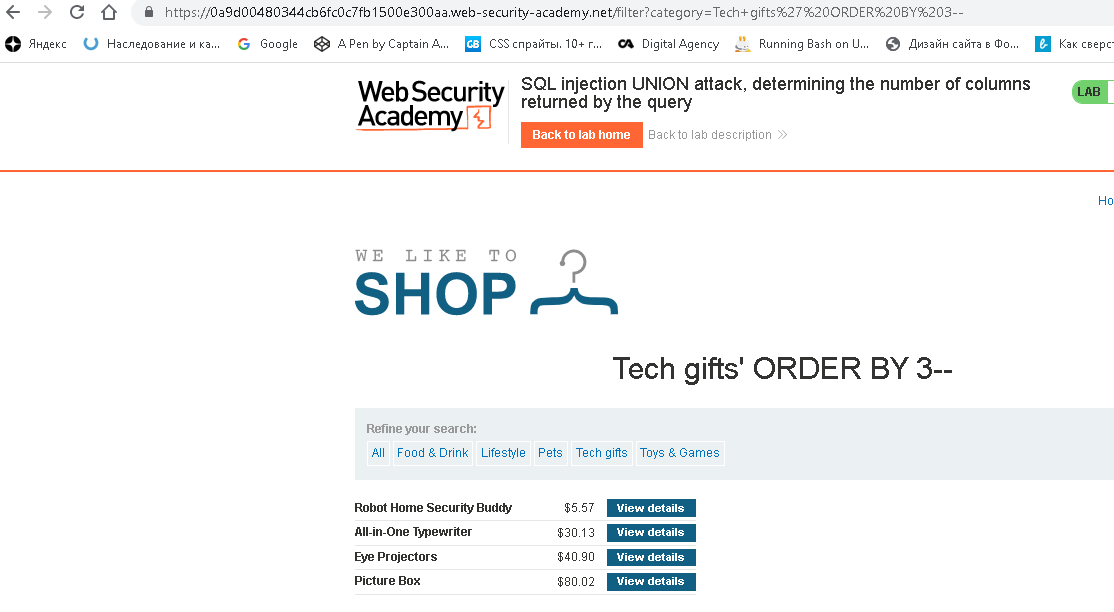
В урле прописываем ORDER BY 2–

(таблица есть)



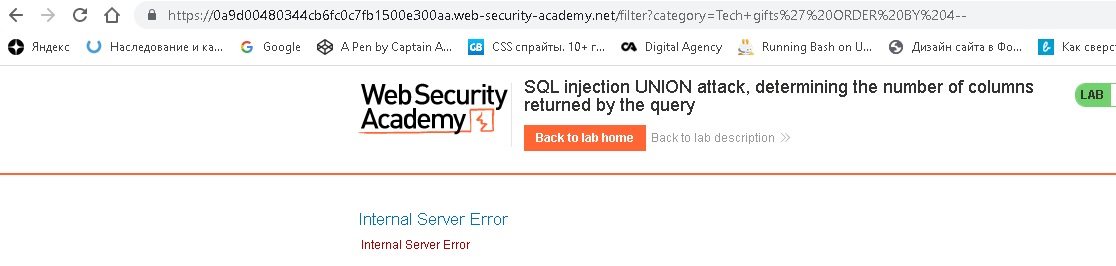
В урле прописываем ORDER BY 3–

(таблица есть)



В урле прописываем ORDER BY 4–

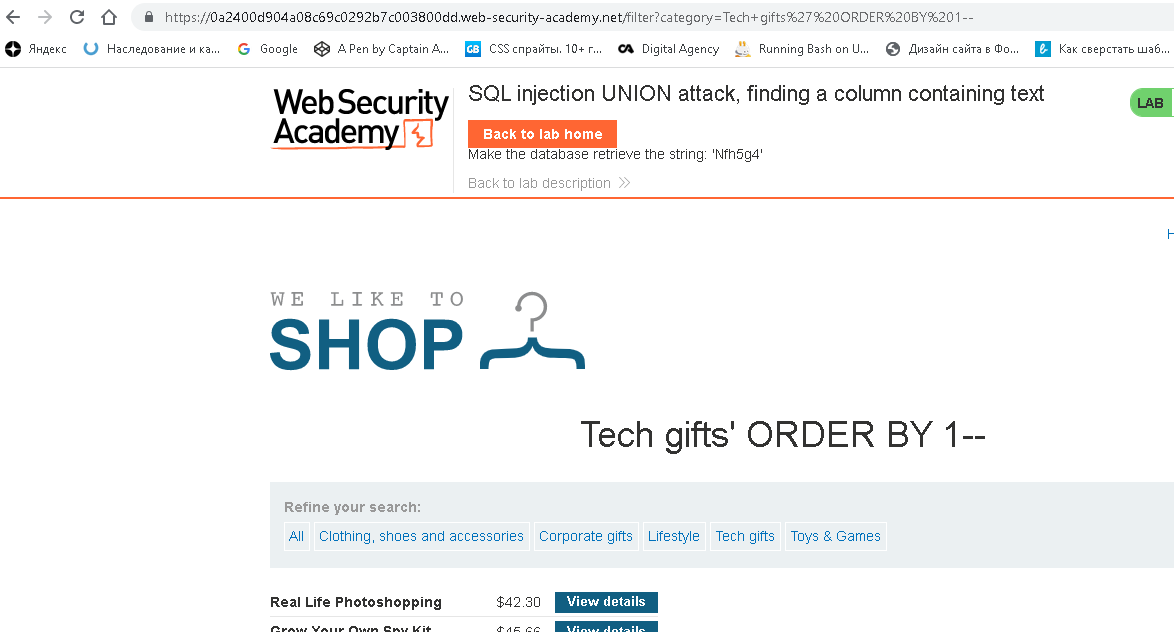
Видим ошибку, тк 4 колонки не существует:



**Итак, всего 3 колонки.**

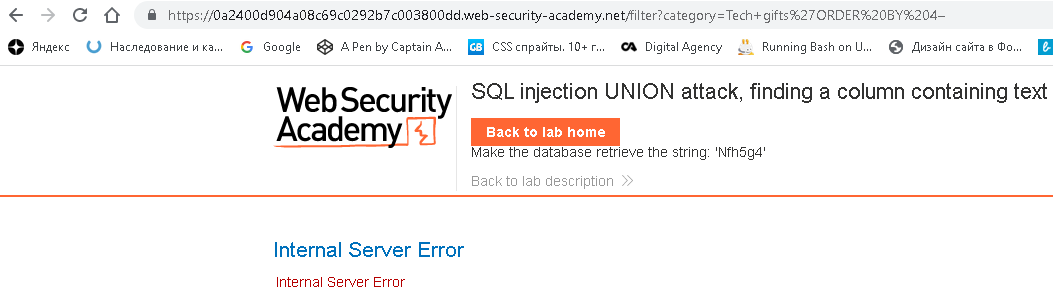
* [Лабораторная 2](https://portswigger.net/web-security/sql-injection/union-attacks/lab-find-column-containing-text) Lab: SQL injection UNION attack, finding a column containing text

Добавим в урл ORDER BY 1–



Потом ORDER BY 2– (есть таблица), ORDER BY 3– (есть таблица).

Когда добавляем ORDER BY 4–, получаем ошибку:

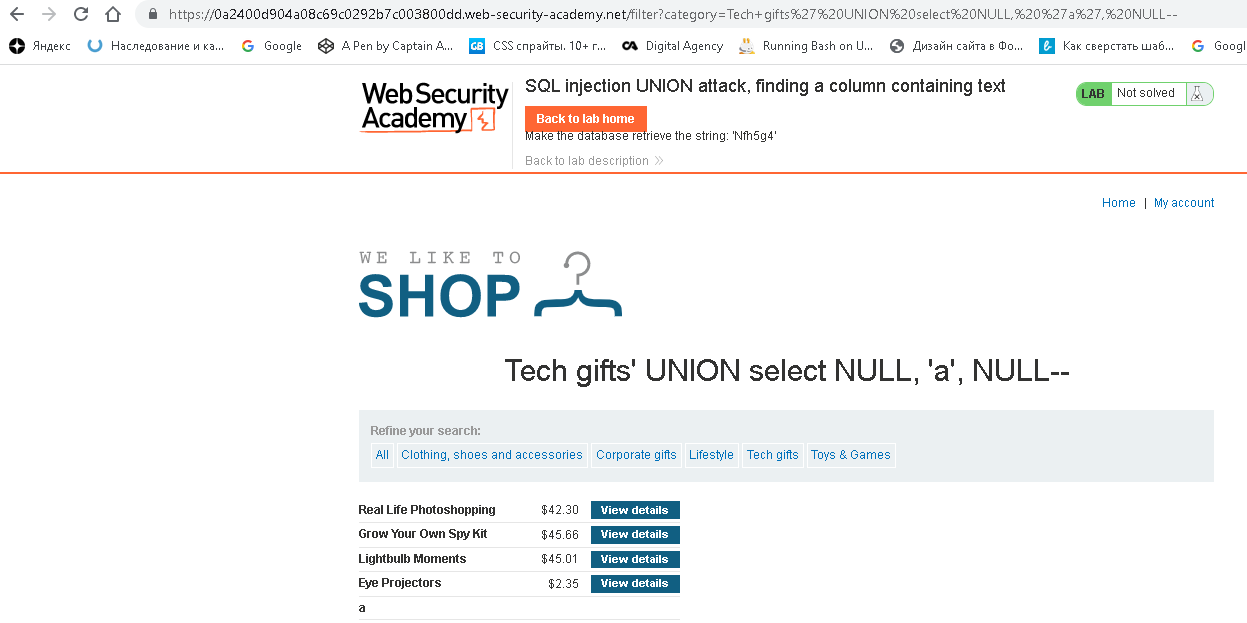


Добавим в урл ' UNION select 'a', NULL, NULL–

и видим ту же ошибку.

Посмотрим вторую колонку, добавив в урл ' UNION select NULL, 'a', NULL–

Появилась новая строка:



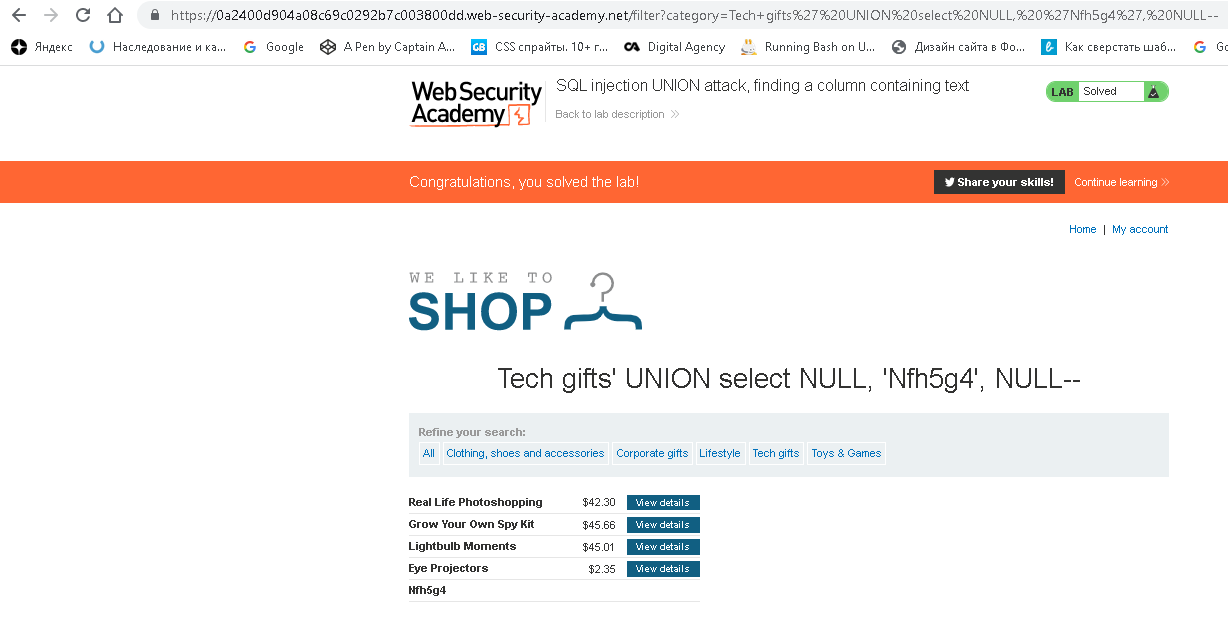
И проверим третий параметр, добавив в запрос ' UNION select NULL, 'a', 'a'--

Возникла ошибка Internal Server Error.

Получается во второй колонке есть текстовое значение. Заменим параметр а на код

и подставим в урл ' UNION select NULL, 'Nfh5g4', NULL–

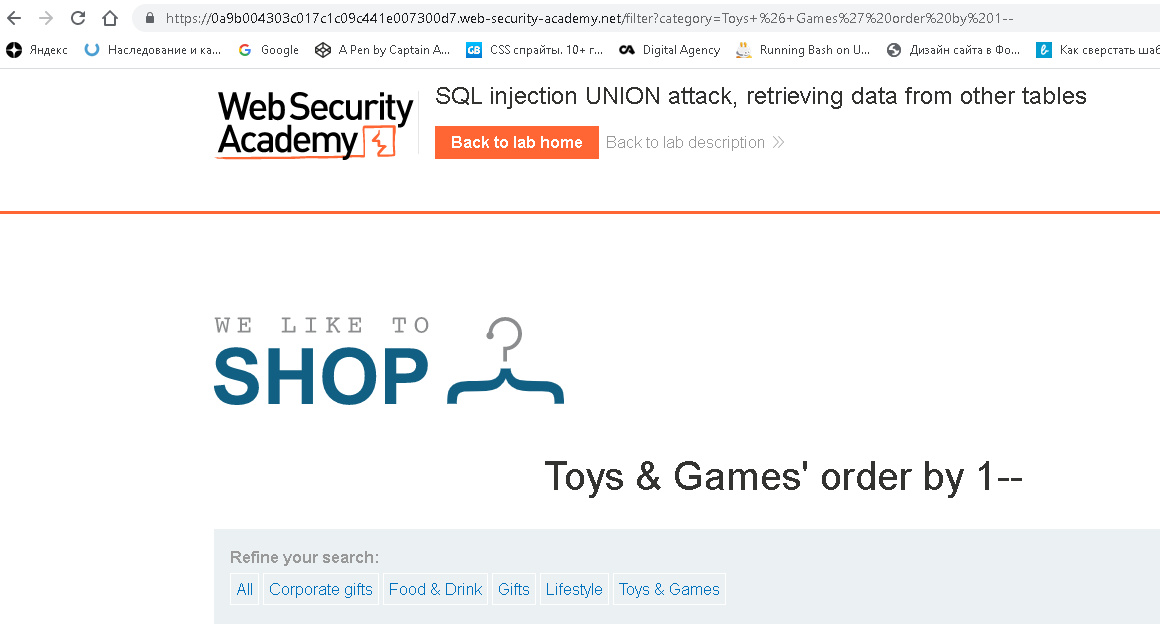
Получаем верный ответ:

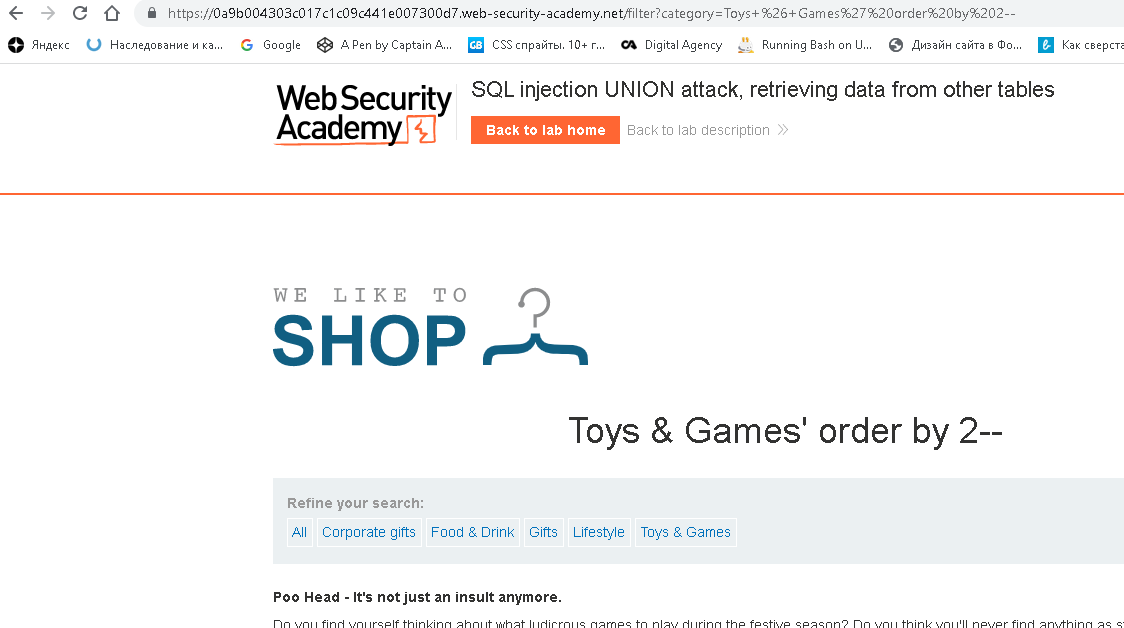


* [Лабораторная 3](https://portswigger.net/web-security/sql-injection/union-attacks/lab-retrieve-data-from-other-tables) SQL injection UNION attack, retrieving data from other tables

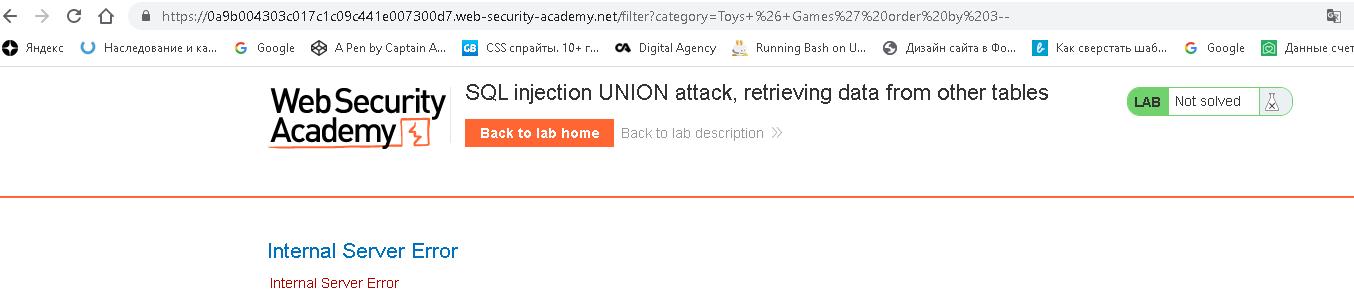
Добавим в урл по очереди ORDER BY N–

где N=1,2,3- до появления ошибки Internal Server Error



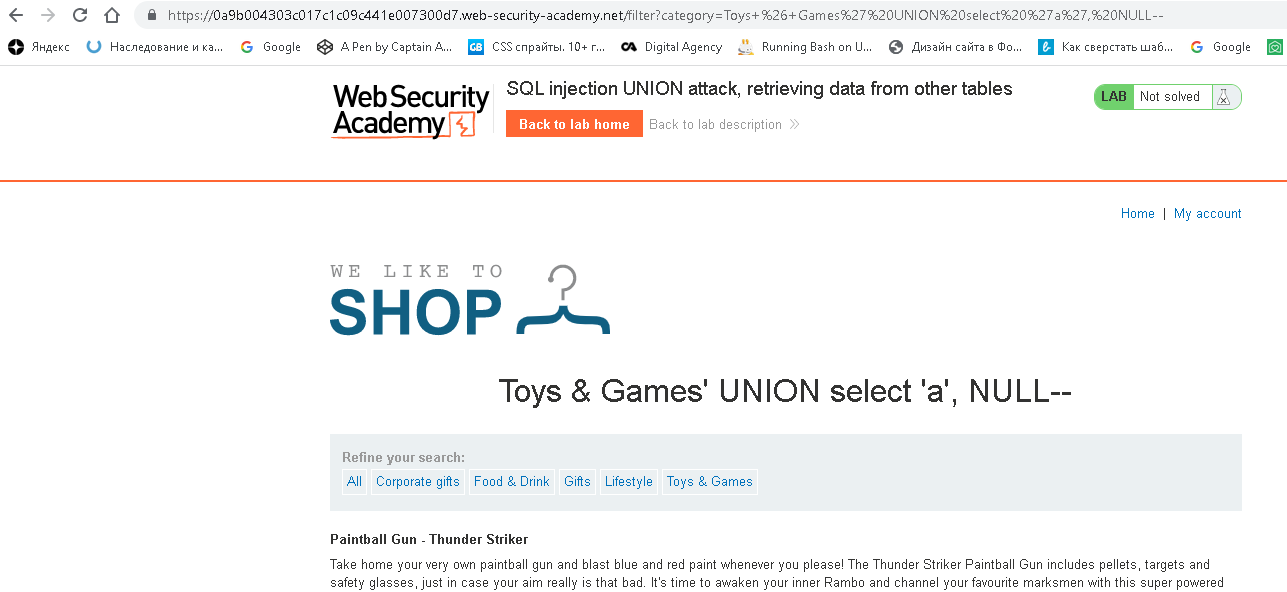


На третьем шаге возникла ошибка



Количество колонок 3-1= 2.

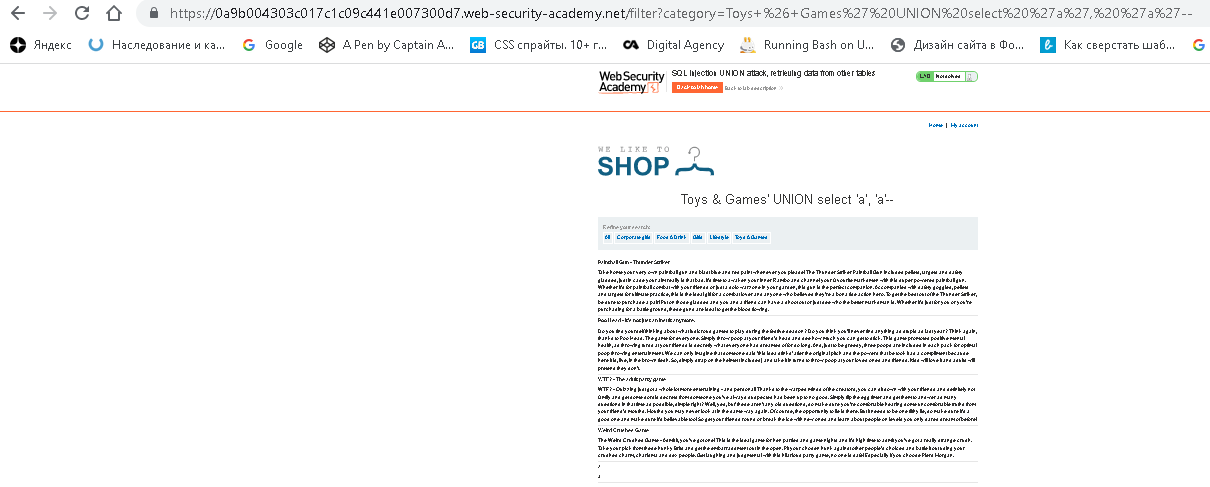
Добавим в урл ' UNION select 'a', NULL–



Внизу появляется строка с а.

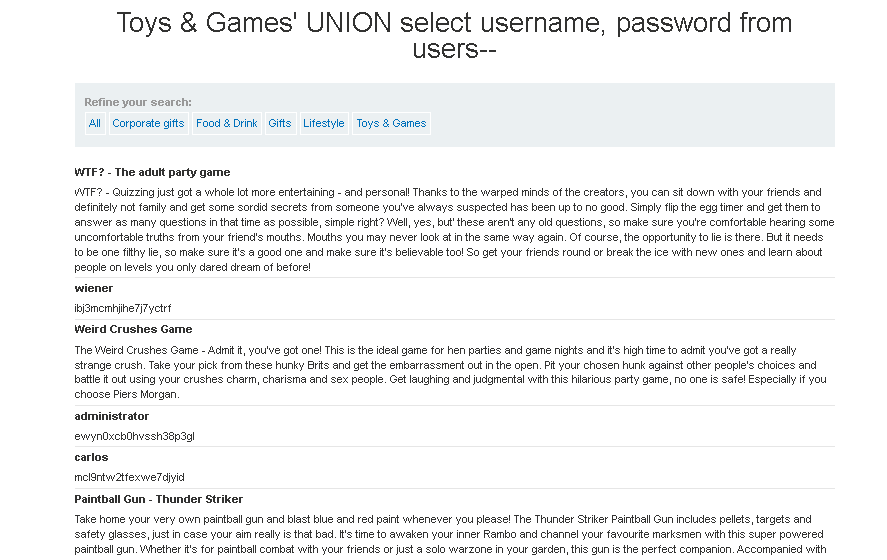
Запишем запрос ‘ UNION select ‘a’,’a’--

Появится вторая строка с а. Следовательно есть две колонки с типом string.



Добавляем в урл ' UNION select username, password from users–

для вывода логина и пароля



Берем админский логин и пароль и пробуем зайти. Все получилось.

