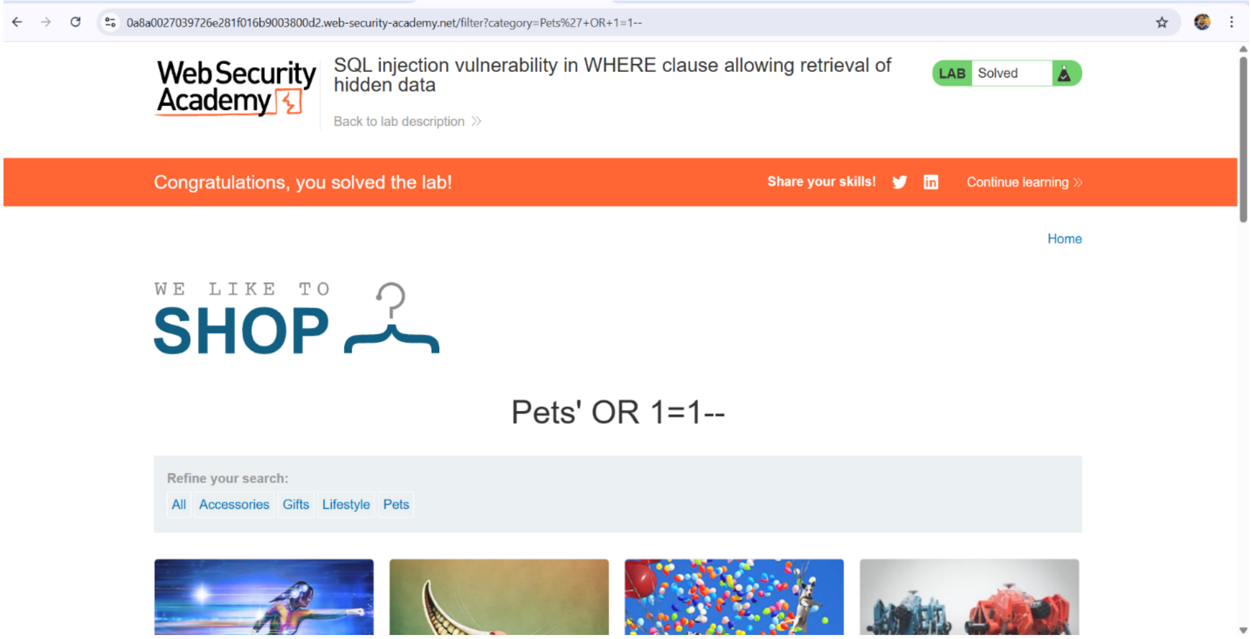
SQL Injection Labs

Retrieving hidden data:

From this topic I learnt how to retrieve hidden data in basic way. Here if the website is vulnerable, there I can notice a change by keeping (‘) this apostrophe after parameter. Suppose there a parameter like (=gifts). There I should use (--) so that rest of the hidden query will be interpreted by comments. Also there is a query like (released=1). This will be also interpreted. So this will reveal datas. After typing an apostrophe then I should write OR 1=1. That means true. So the results will be published.

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



0a8a0027039726e281f016b9003800d2.web-security-academy.net/filter?category=Pets%27+OR+1=1--

SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills!

Continue learning »

Home

WE LIKE TO SHOP

Pets' OR 1=1--

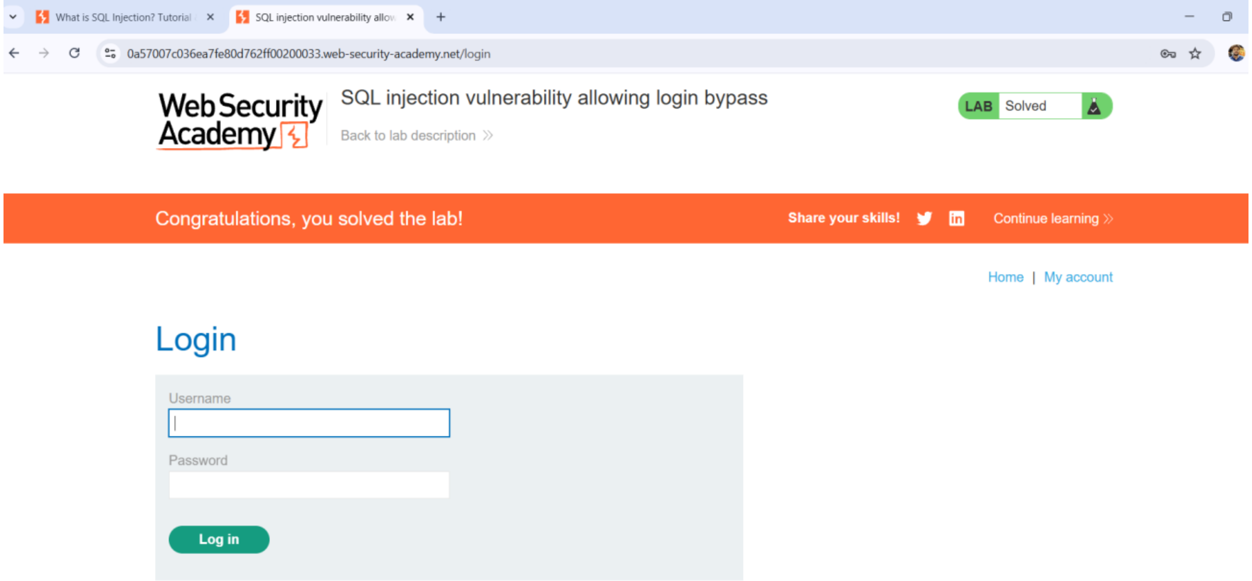
Refine your search:

All Accessories Gifts Lifestyle Pets

Here in this lab I used (‘+OR+1=1--). Thus the lab was solved by retrieving datas.

Subverting application logic:

From this topic I learnt about applying logics of query. Suppose there’s a login panel. If the website is vulnerable I can apply the username as (administrator--) and in the password box I will fillup with anything like any string or integer. This will work because after (--) the password queries will convert in comments. So if I know the username that will be enough for me.


What is SQL Injection? Tutorial
SQL injection vulnerability allow
0a57007c036ea7fe80d762ff00200033.web-security-academy.net/login
Web Security Academy
Back to lab description »
LAB Solved
Share your skills!
Continue learning »
Home | My account
Username
Password
Log in

SQL injection vulnerability allowing login bypass

Congratulations, you solved the lab!

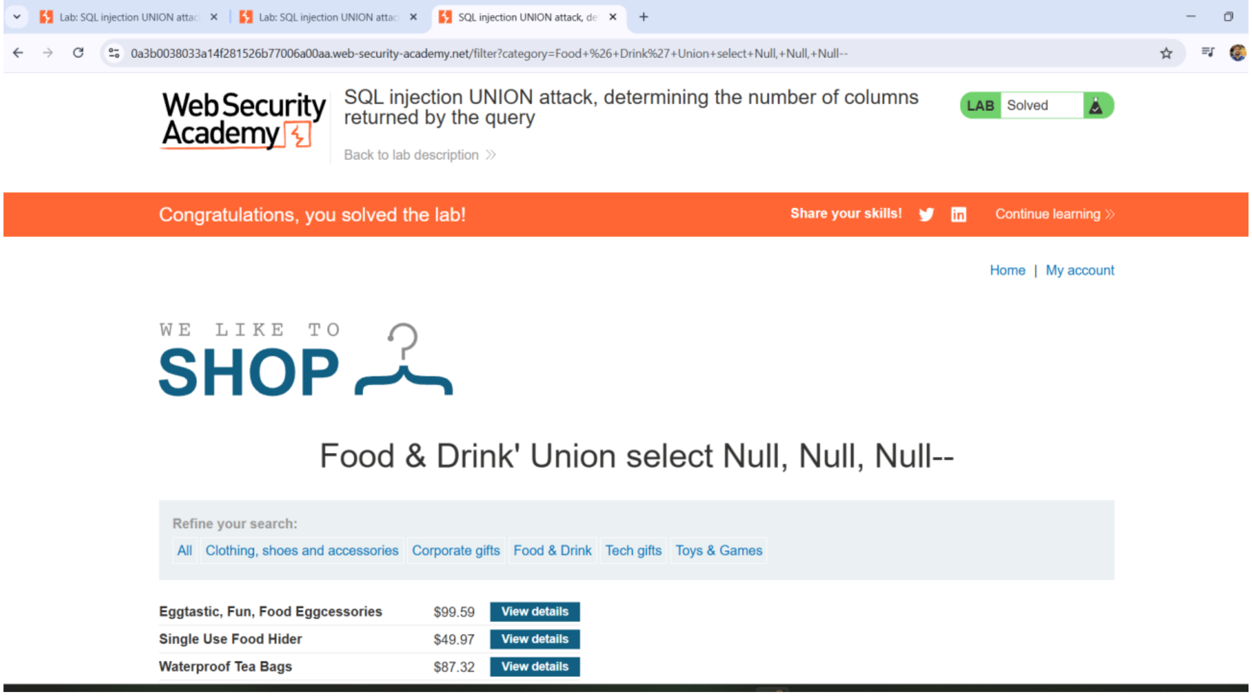
Login

Here I wrote (administrator--) in username and in password I wrote (abc). It solved.

SQL injection UNION attacks

Determining the number of columns required:

In this method if the site is vulnerable I should apply apostrophe first. Then if I notice vulnerable response then I should findout the vulnerable column number by typing (‘ UNION SELECT NULL--). If it doesn’t work then again I have to type (‘ UNION SELECT NULL,NULL--). Now the thing is how I will ensure that second column is vulnerable. I have to notice that there’s no error output in the time of (‘ UNION SELECT NULL,NULL--). If third column would vulnerable then I have to type extra NULL.



Lab: SQL injection UNION attac
Lab: SQL injection UNION attac
SQL injection UNION attack, de
0a3b0038033a14f281526b77006a00aa.web-security-academy.net/filter?category=Food+%26+Drink%27+Union+select+Null,+Null,+Null--
Web Security Academy
LAB Solved
Back to lab description
Share your skills!
Continue learning
Home | My account
WE LIKE TO SHOP
Refine your search:
All
Clothing, shoes and accessories
Corporate gifts
Food & Drink
Tech gifts
Toys & Games
View details

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

Congratulations, you solved the lab!

Food & Drink' Union select Null, Null, Null--

Eggtastic, Fun, Food Eggcessories	$99.59	View details
Single Use Food Hider	$49.97	View details
Waterproof Tea Bags	$87.32	View details

Here third column was vulnerable because I typed (‘ UNION SELECT NULL, NULL, NULL--). Then it came without error message. Thus 3rd column is vulnerable and the lab solved.

Database specific syntax

Here it said about database type like Oracle. In oracle I have to add DUAL at last to retrieve comments. Also they mentioned SQL injection cheat sheet.

SQL injection cheat sheet

String concatenation

I can concatenate together multiple stings to create a single string. Suppose for Oracle and PostgreSQL I can write 'Hello'||'world'. For Microsoft 'Hello'+'world'. For MySQL 'Hello' 'world' CONCAT('Hello','world').

Substring

Here I learnt about extract part. Suppose for Oracle SUBSTR('foobar',4,2). That means here written 'ba'. That means 4 number character and 2 is for after 4 number character it will take one more character and total 2 characters. Suppose if the password is 'batman', here I can write for MYSQL: SUBSTRING(password,4,2). The result will be 'ma'. That's how it works.

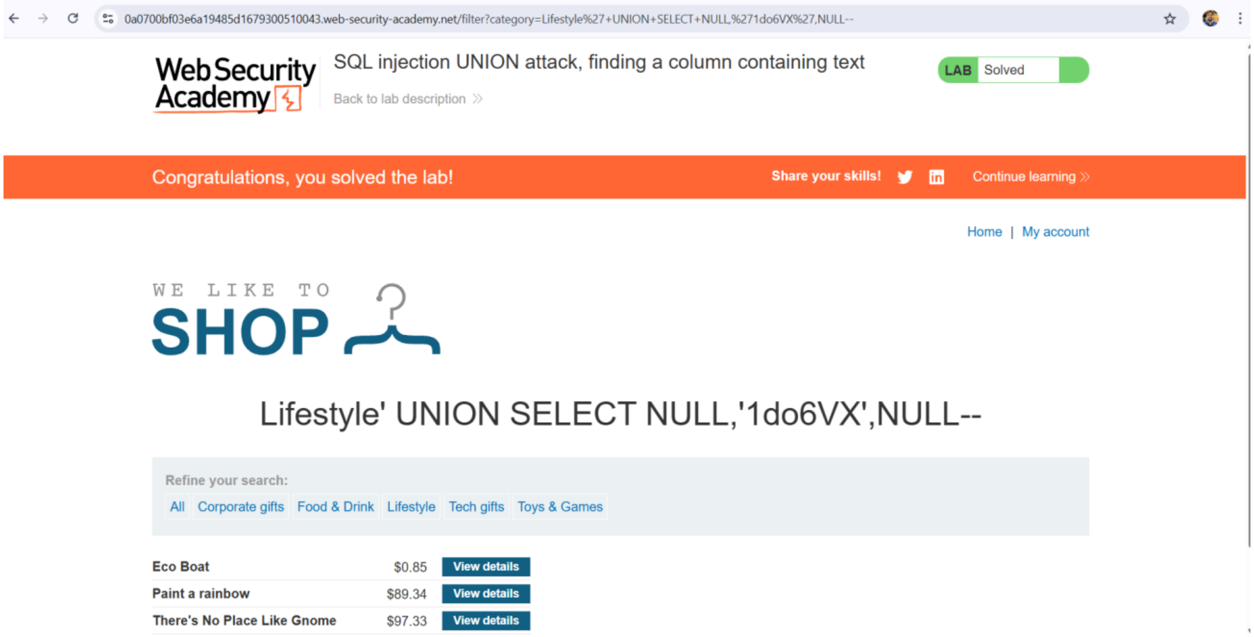
Comments

For comment in Oracle: --comment. For Microsoft: /*comment*/ and --comment. For PostgreSQL: /*comment*/ and #comment. For MYSQL: -- comment.

Similar I have learnt Database version, Database contents, Conditional errors, Extracting data via visible error messages, Batched (or stacked) queries, Time delays, Conditional time delays, DNS lookup, DNS lookup with data exfiltration. Those were much interesting topics from SQL.

Finding columns with a useful data type

Here I learnt how to retrieve column text from vulnerable column. Suppose a website has 4 columns and 3 number column is vulnerable. So I can write like this to retrieve data: UNION SELECT NULL,NULL,'a',NULL—



```
0a0700bf03e6a19485d1679300510043.web-security-academy.net/filter?category=Lifestyle%27+UNION+SELECT+NULL,%271do6VX%27,NULL--
```

SQL injection UNION attack, finding a column containing text

Congratulations, you solved the lab!

Lifestyle' UNION SELECT NULL,'1do6VX',NULL--

Refine your search:

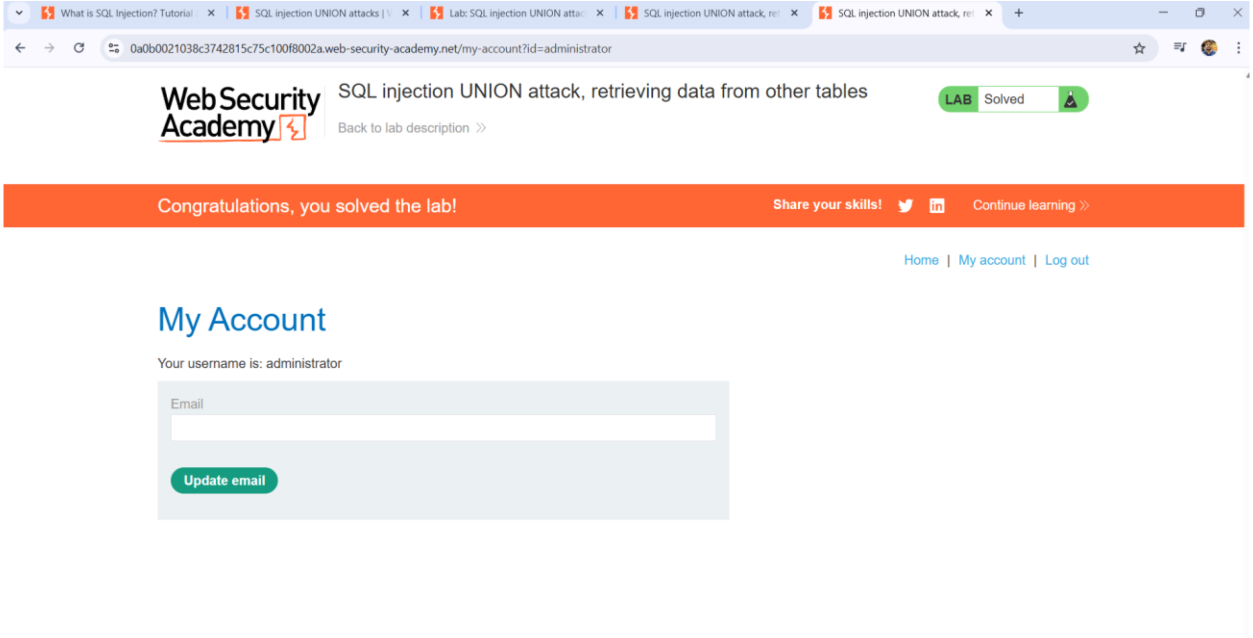
All | Corporate gifts | Food & Drink | Lifestyle | Tech gifts | Toys & Games

Eco Boat	$0.85	View details
Paint a rainbow	$89.34	View details
There's No Place Like Gnome	$97.33	View details

So here 2 number column was vulnerable.

Using a SQL injection UNION attack to retrieve interesting data

Here if a website is vulnerable, I can ensure with a method and that is I can type the username in the username box and then I can add comment(--). That means I don't need to give password as they can't read after comment.



What is SQL Injection? Tutorial
SQL injection UNION attacks |
Lab: SQL injection UNION attac
SQL injection UNION attack, re
SQL injection UNION attack, re

0a0b0021038c3742815c75c100f8002a.web-security-academy.net/my-account?id=administrator

SQL injection UNION attack, retrieving data from other tables

Back to lab description
LAB Solved

Congratulations, you solved the lab!

Share your skills!
Continue learning
Home | My account | Log out

My Account

Your username is: administrator

Email

Here I have written ‘administrator—’ and system didn’t read the next lines means password. So it logged in.