Ultimate Member callback functions

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.

remote command execution vulnerability

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:

$data['custom_dropdown_options_source'] and *$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

This function is called when processing select/multiselect field

Fileds can be added here

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*

Then I reload this page

And the result can be found in every users' profile

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.

specific PHP functions execution vulnerability

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

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

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

;