

wpForo <= 2.4.1 - Subscriber+ Reputation Manipulation and Privilege Escalation via hidden parameter

Summary:

As we have installed the wpForo plugin, we can register an account to access the forum. This plugins have four default usergroups, that is **Admin, Customer, Guest, Moderator, and Registered**. The default role is subscriber and it has been registered to "**Registered**" main usergroups. But the users can have 2 usergroups, for example "**Registered**" as main usergroups and "**Customer**" is **secondary** usergroups. The vulnerability is, user can add secondary usergroups to their itself account.

So, for the testing scenario, I have add new usergroup and name it to "Staff" and mark set this usergroup to "can be also as Secondary usergroup".

Usergroups [Add New](#)

Usergroup Name

User Role

Default Forum Access

This is only used when a new Usergroup is created, it automatically gets the selected Forum Access in all forums.

Display on Members List

Can be also used as Secondary Usergroup

Dashboard - Manage Boards & Forums <input checked="" type="checkbox"/>	Dashboard - Moderate Topics & Posts <input checked="" type="checkbox"/>	Dashboard - Can edit member <input checked="" type="checkbox"/>
Dashboard - Manage Settings <input checked="" type="checkbox"/>	Dashboard - Manage Usergroups <input checked="" type="checkbox"/>	Dashboard - Can ban member <input checked="" type="checkbox"/>
Dashboard - Manage Tools <input checked="" type="checkbox"/>	Dashboard - Manage Phrases <input checked="" type="checkbox"/>	Dashboard - Can delete member <input checked="" type="checkbox"/>
Dashboard - Manage Members <input checked="" type="checkbox"/>	Dashboard - Manage Themes <input checked="" type="checkbox"/>	Front - Can pass moderation <input checked="" type="checkbox"/>
Front - Can view statistic <input checked="" type="checkbox"/>	Front - Can view member subscriptions <input checked="" type="checkbox"/>	Front - Can view avatars <input checked="" type="checkbox"/>
Front - Can view members <input checked="" type="checkbox"/>	Front - Can upload cover <input checked="" type="checkbox"/>	Front - Can view member username <input checked="" type="checkbox"/>
Front - Can view profiles <input checked="" type="checkbox"/>	Front - Can upload avatar <input checked="" type="checkbox"/>	Front - Can view member email <input checked="" type="checkbox"/>
Front - Can view member activity <input checked="" type="checkbox"/>	Front - Can have signature <input checked="" type="checkbox"/>	Front - Can view member title <input checked="" type="checkbox"/>
Front - Can view member custom title <input checked="" type="checkbox"/>	Front - Can view member reg. date <input checked="" type="checkbox"/>	Front - Can view member about me <input checked="" type="checkbox"/>
Front - Can view member reputation <input checked="" type="checkbox"/>	Front - Can view member location <input checked="" type="checkbox"/>	Front - Can write PM <input checked="" type="checkbox"/>
Front - Can view member website <input checked="" type="checkbox"/>	Front - Can view member occupation <input checked="" type="checkbox"/>	Front - Can access to attachments <input checked="" type="checkbox"/>
Front - Can view member social networks <input checked="" type="checkbox"/>	Front - Can view member signature <input checked="" type="checkbox"/>	Front - Can access to add topic page <input checked="" type="checkbox"/>

[save](#)

Step to Reproduce:

1. Login to subscriber account as attacker, don't forget to create 3 topic to the main forum for enable the "account" settings feature.

Forum

Forums Members Recent Posts My Profile Logout 🔔 🔍

🏠 > Main Category > Main Forum >

Main Forum

This is a simple parent forum

[Add topic](#)

[Subscribe for new topics](#) [RSS](#)

Status	Author	Topics	Forum	Replies	Views	Last Post
		hello By attacker, 19 minutes ago		0	0	 By attacker 19 minutes ago
		asdasd By attacker, 20 minutes ago		0	0	 By attacker 20 minutes ago
		test test By attacker, 21 minutes ago		0	0	 By attacker 21 minutes ago

2. Navigate to My Profile > Account page. The attacker's reputation is "active member", so let's grab the highest reputation.

Forum

Forum Home | Recent Posts

attacker @attacker

Active Member ★

Joined: Feb 5, 2025
Last seen: Feb 5, 2025

0 Followers / 0 Following

Profile Activity Favored Subscriptions

Username: **attacker**

Display Name: attacker

Nickname: @attacker

Email: attacker@localhost.com

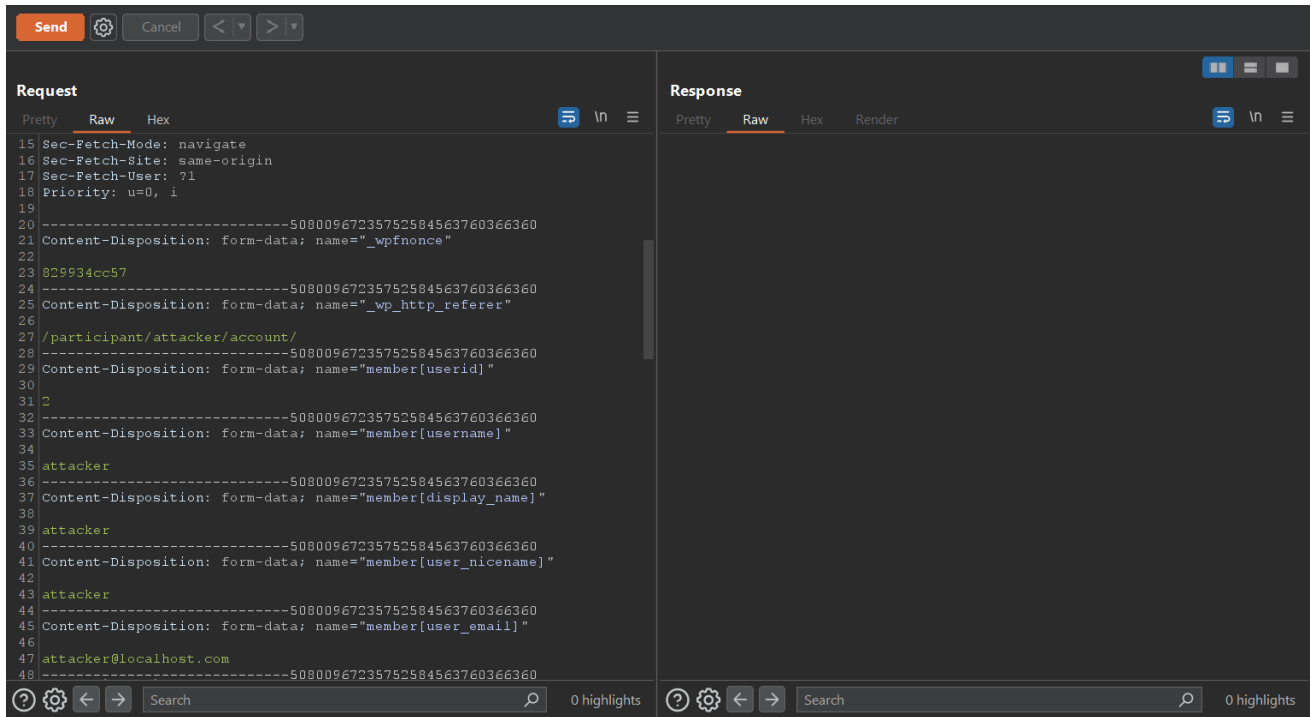
Title: Member

Avatar: Default avatar Specify avatar by URL: Upload an avatar [Browse...](#) No fil...cted.

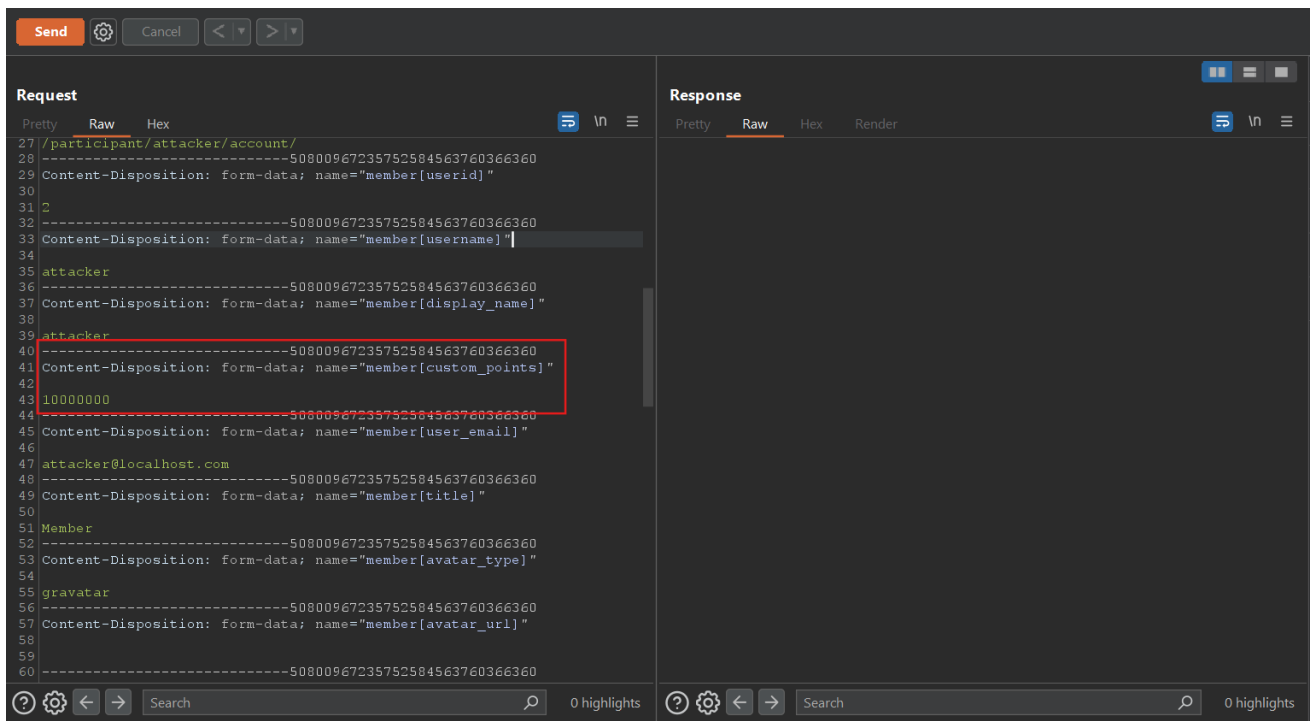
About Me

11pt B I U ABC A [list icons]

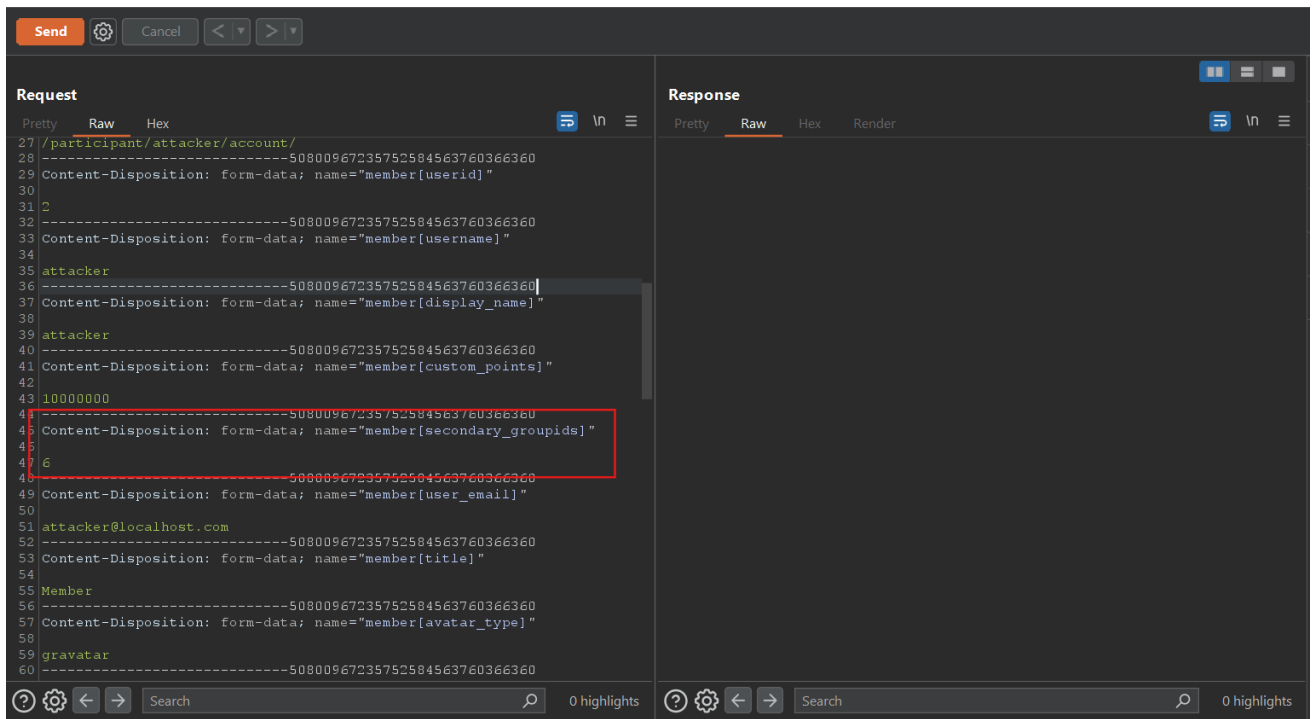
3. Update and submit the profile. Send the captured request to repeater.



4. To manipulate the reputation, add new parameter "member[custom_points]" with value 1000000.



5. To grab "Staff" as secondary usergroup, add new parameter member[secondary_groupids] with ID value, in this case is 6.



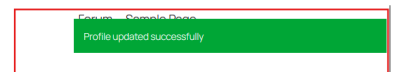
Usergroups [Add New](#)

User Role	Usergroup	Members	Default	Default Access	Color	ID
administrator	Admin	1		Full access		1
Subscriber	Customer	0	Set as Default	Standard access		5
	Guest			Read only access		4
Editor	Moderator	0	Set as Default	Moderator access		2
Subscriber	Registered	1	is Default	Standard access	default (#15)	3
Subscriber	Staff	0	Set as Default	Full access	default (#15)	6

[Synchronize](#)

6. Submit the request

Testing Site



Forum

attacker | @attacker

Joined: Feb 5, 2025
Last seen: Feb 5, 2025

0 Followers / 0 Following

Profile Activity Favored Subscriptions

Username: attacker

Display Name: attacker

Nickname: attacker

Email: attacker@localhost.com

Title: Member

Impact:

