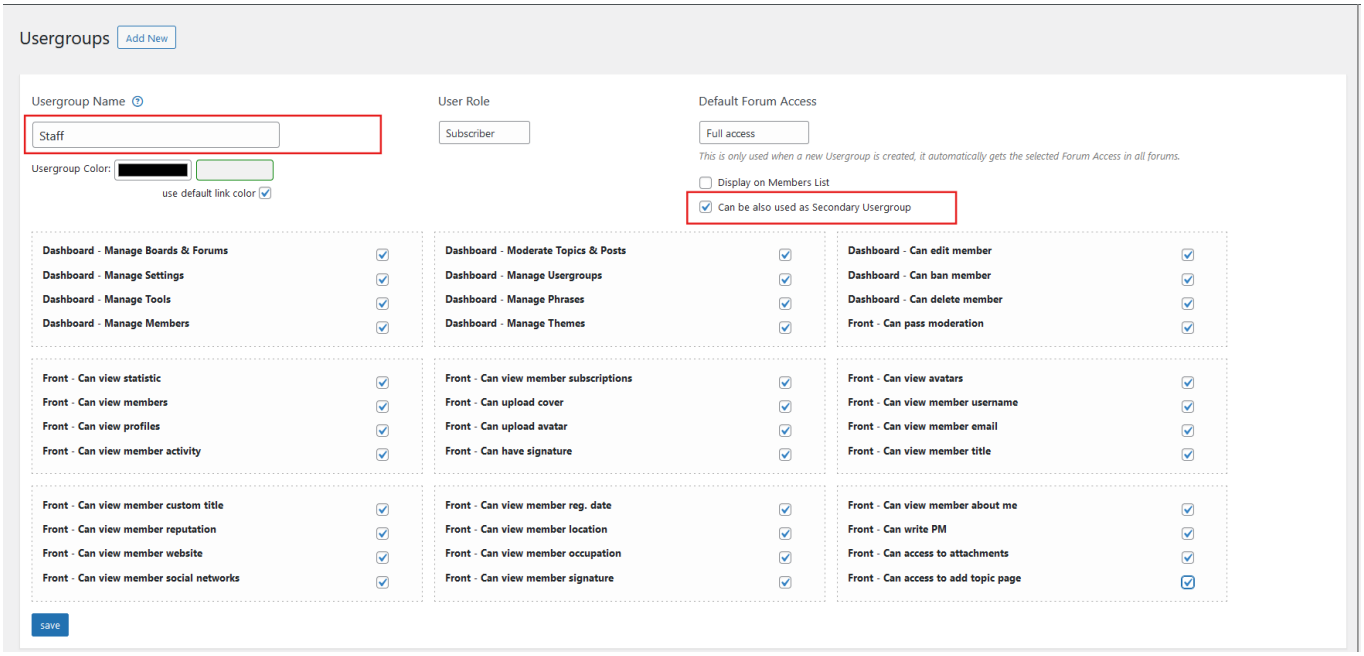
wpForo <= 2.4.1 - Subscriber+ Reputation Manipulation and Privilege Escalation via hidden parameter

Summary:

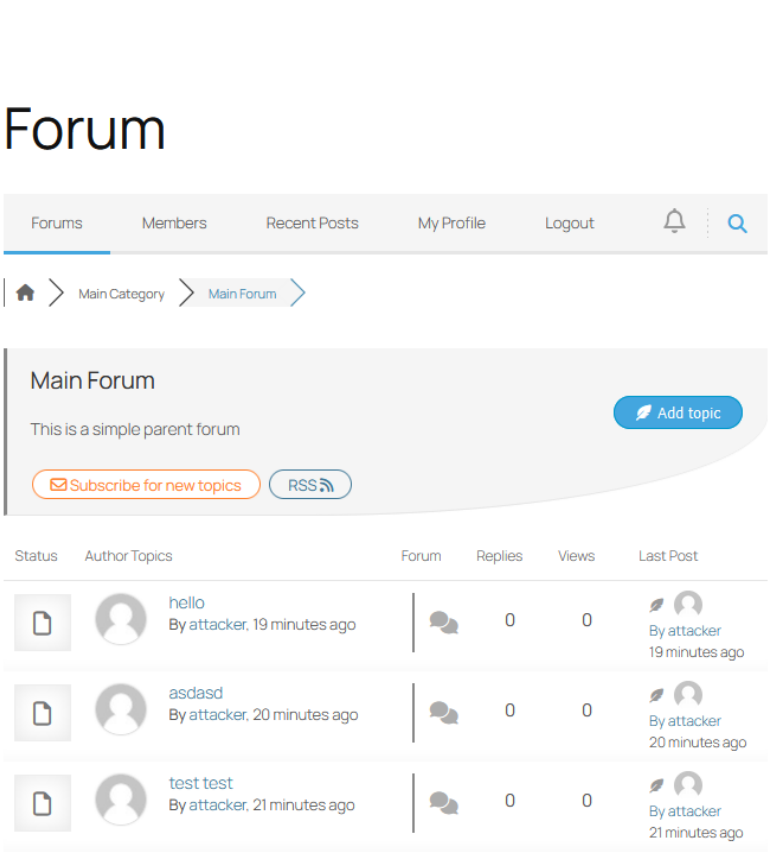
As we have installed the wpForo plugin, we can register an account to access the forum. This plugins have four defult usergroups, that is **Admin, Customer, Guest, Moderator, and Registered**. The default role is subscriber and it has been registered to "**Registered**" main usergroups. But the users 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".

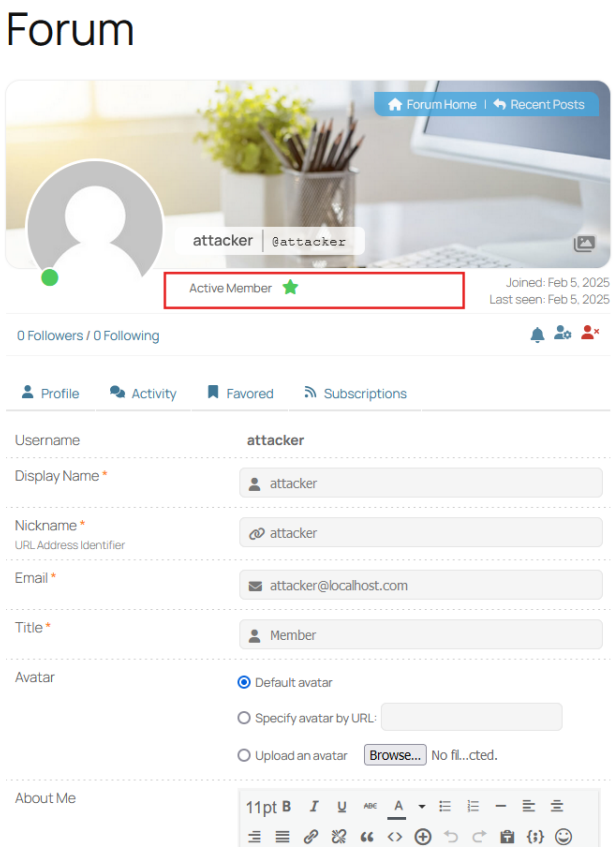


Step to Reproduce:

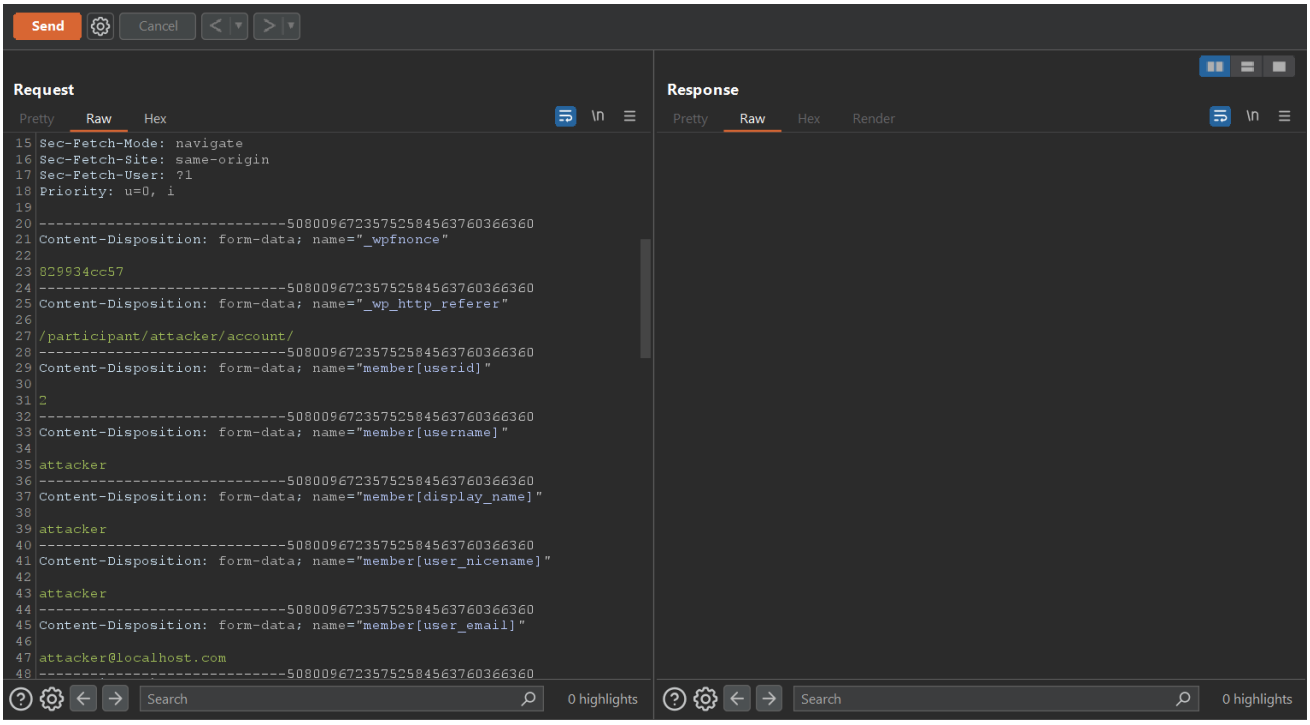
1. Login to subscriber account as attacker, don't forget to create 3 topic to the main forum for enable the "account" settings feature.



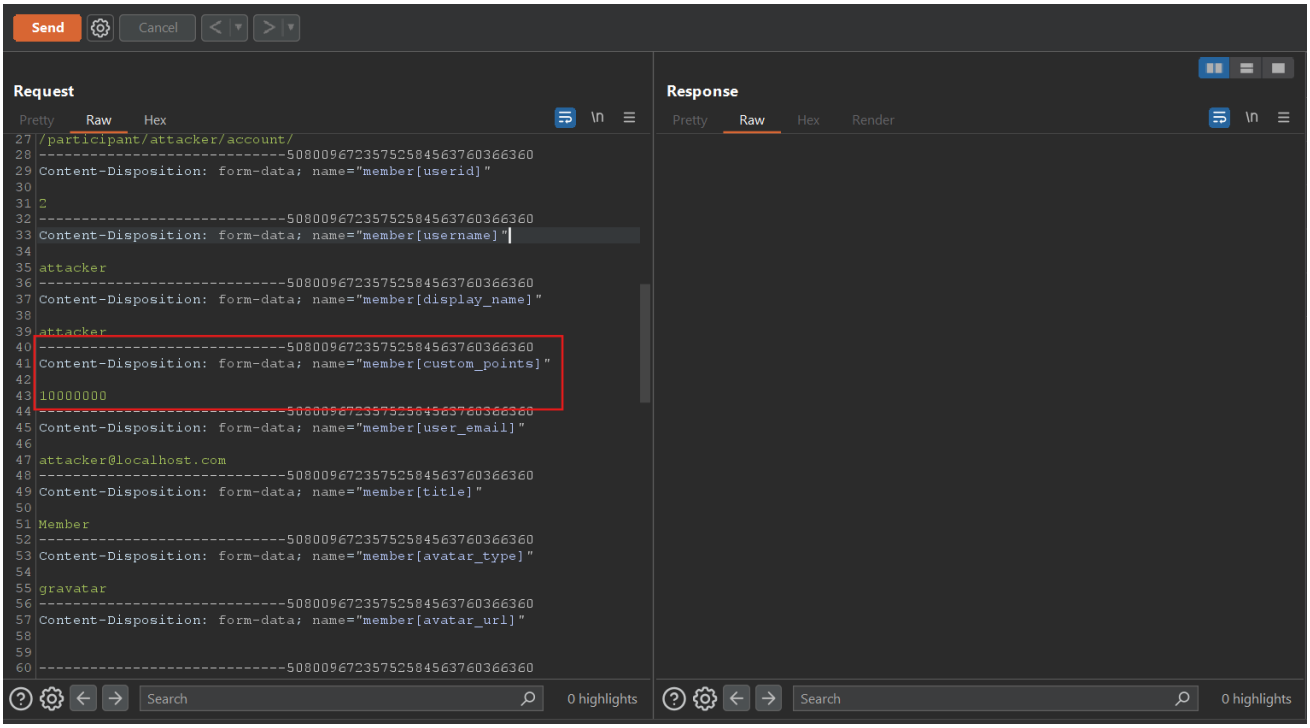
2. Navigate to My Profile > Account page. The attacker's reputation is "active member", so let's grab the highest reputation.



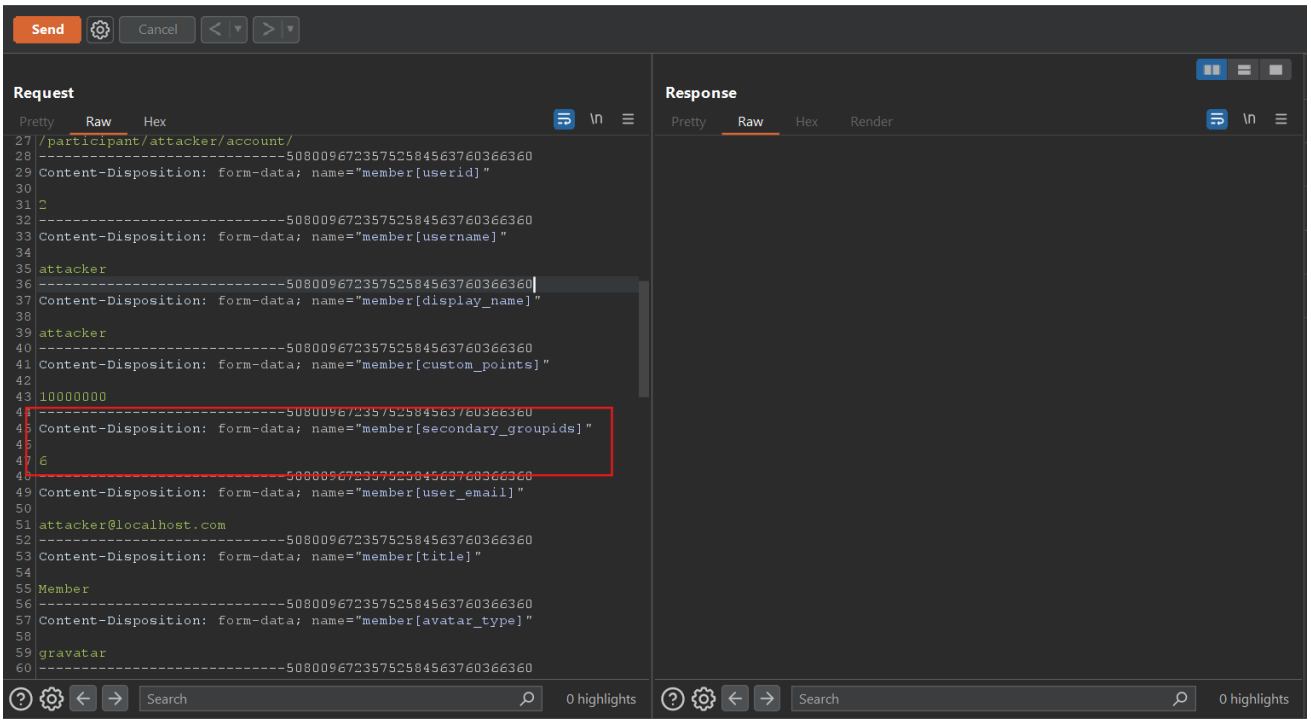
3. Update and submit the profile. Send the captured request to repeater.

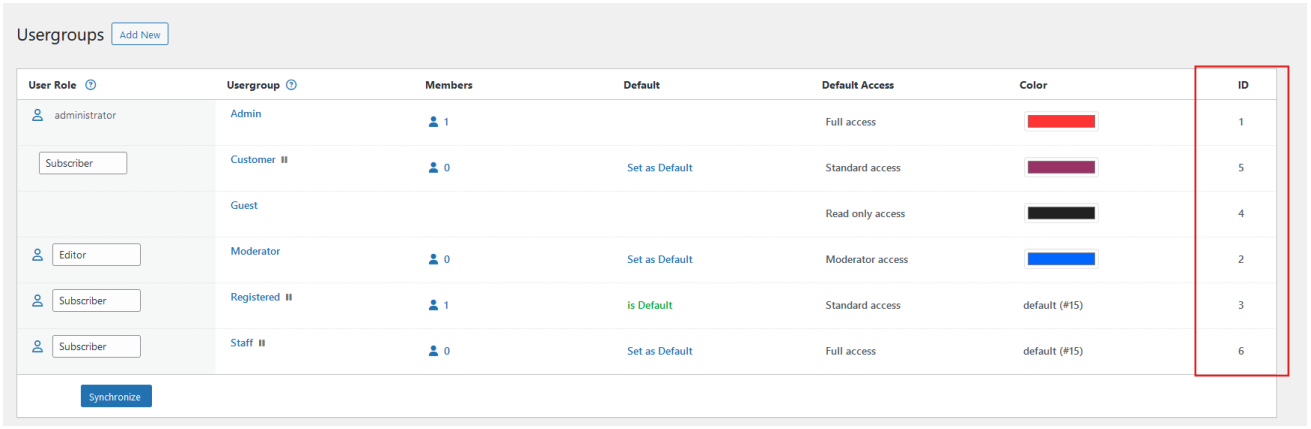


4. To manipulate the reputation, add new parameter "member[custom_points]" with value 1000000.

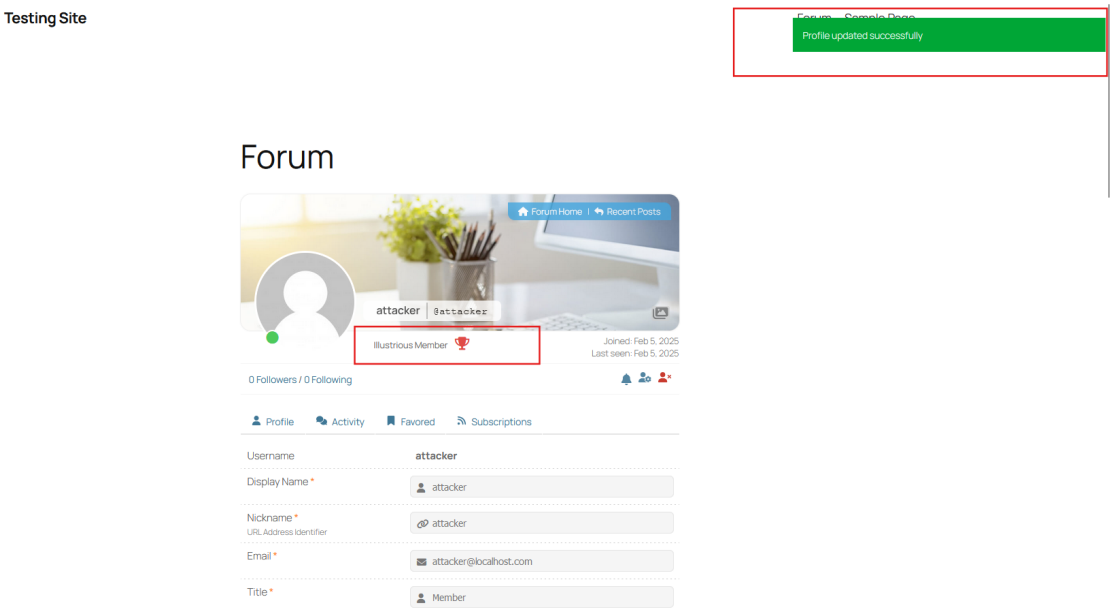


5. To grab "Staff" as secondary usergroup, add new parameter member[secondary_groupids] with ID value, in this case is 6.





6. Submit the request



Impact:

Attacker have access to the wpForo forum like an admin. They can delete the topic, ban any members, update member's usergroup, and access/update the wpForo settings. Look at the picture below.