

Instantly share code, notes, and snippets.

thepiyushkumarshukla / CouchCMS-privilege-Escalation.md



Created 3 weeks ago

<> **Code** ↻ Revisions 1

CouchCMS-privilege-Escalation.md

# Vulnerability :- Privilege Escalation via Parameter Tampering in CouchCMS

A normal Admin user can able to make as many SuperAdmin users in CouchCMS, which is not in the application functionality. By doing so, that user is able to become a SuperAdmin on the application without any restriction.

## Theory :

This application has mainly 4 Types of Users

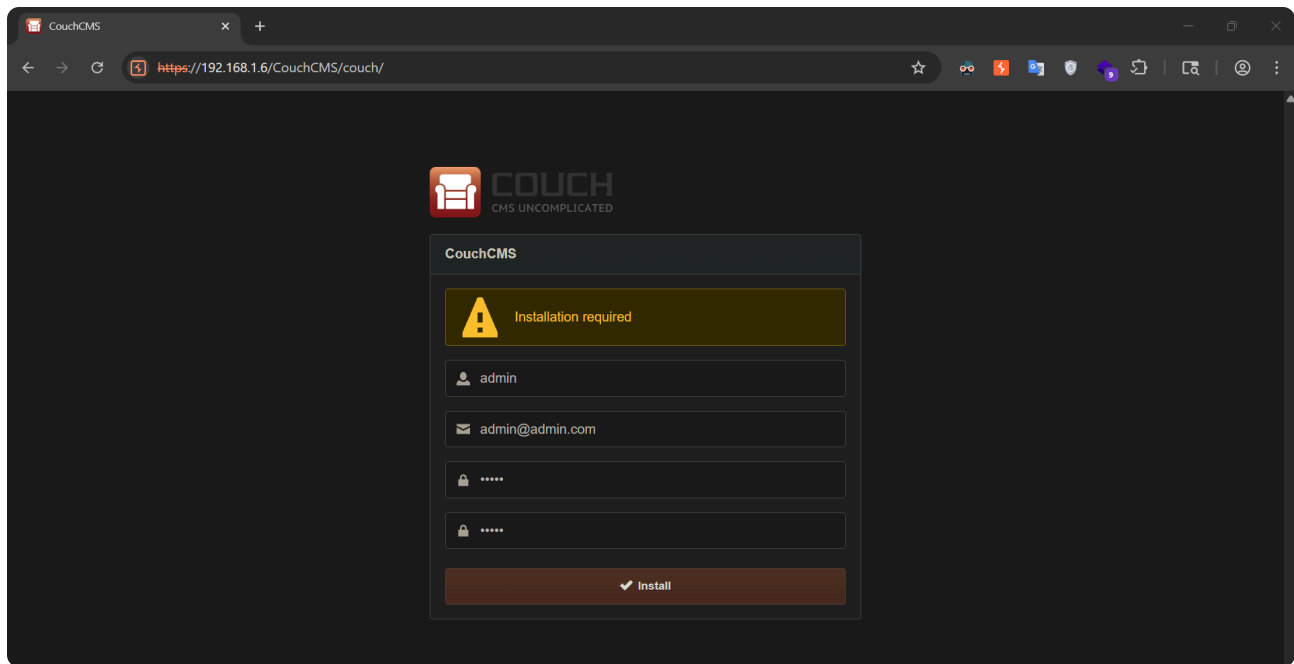
1. Super Admin
2. Admin
3. Authenticated (special)
4. Only Authenticated

## STEPS TO REPRODUCE

### 1. Open and Setup CouchCMS

Open and setup CouchCMS in any XAMPP or LAMP server:

<https://github.com/CouchCMS/CouchCMS>



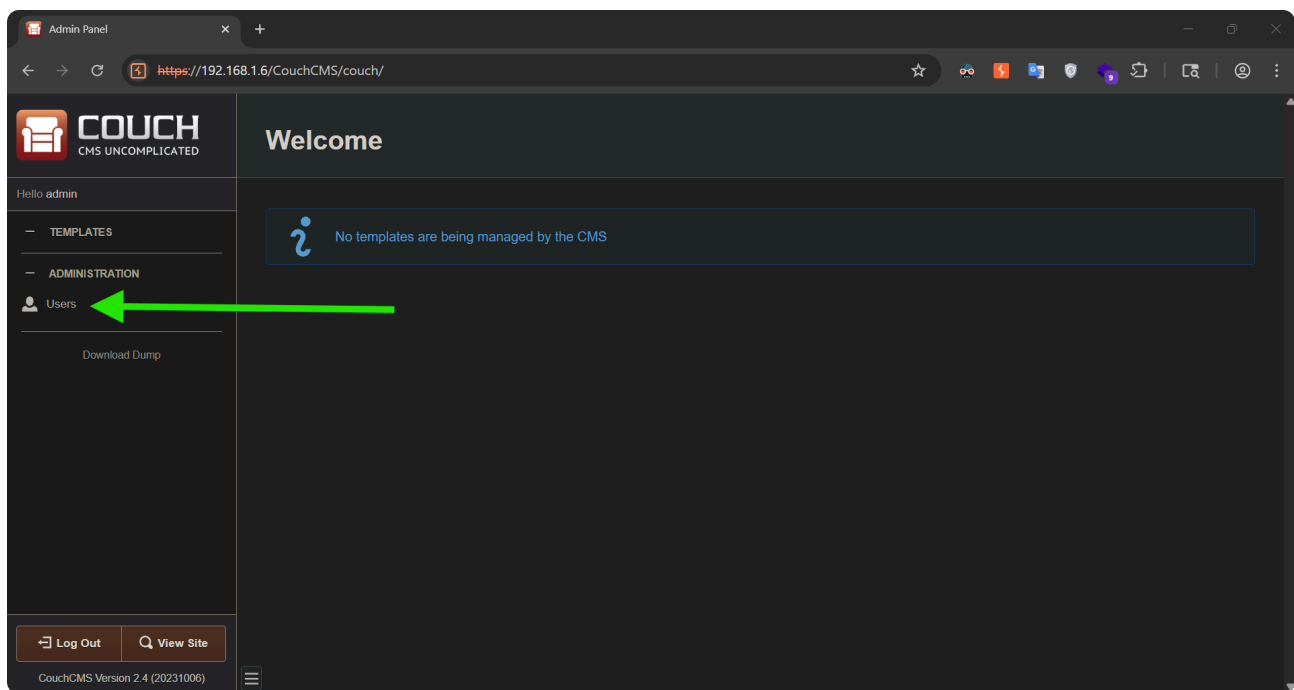
---

## 2. Login with Initial Credentials

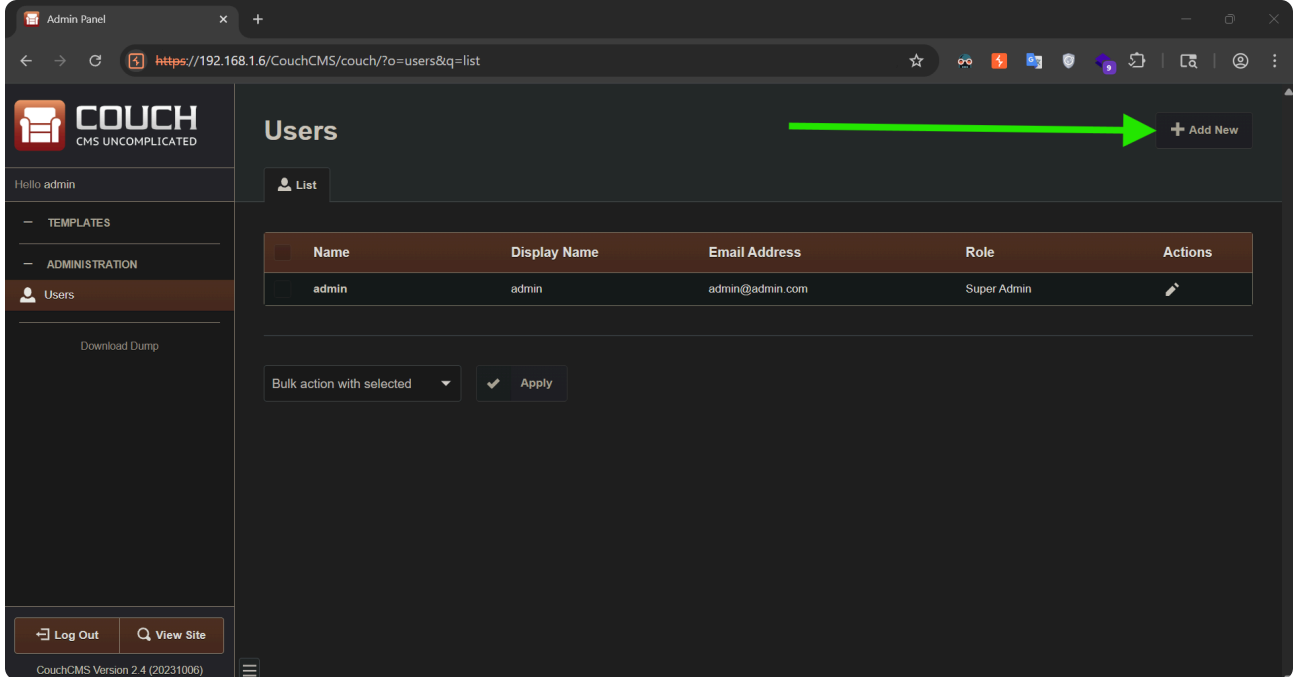
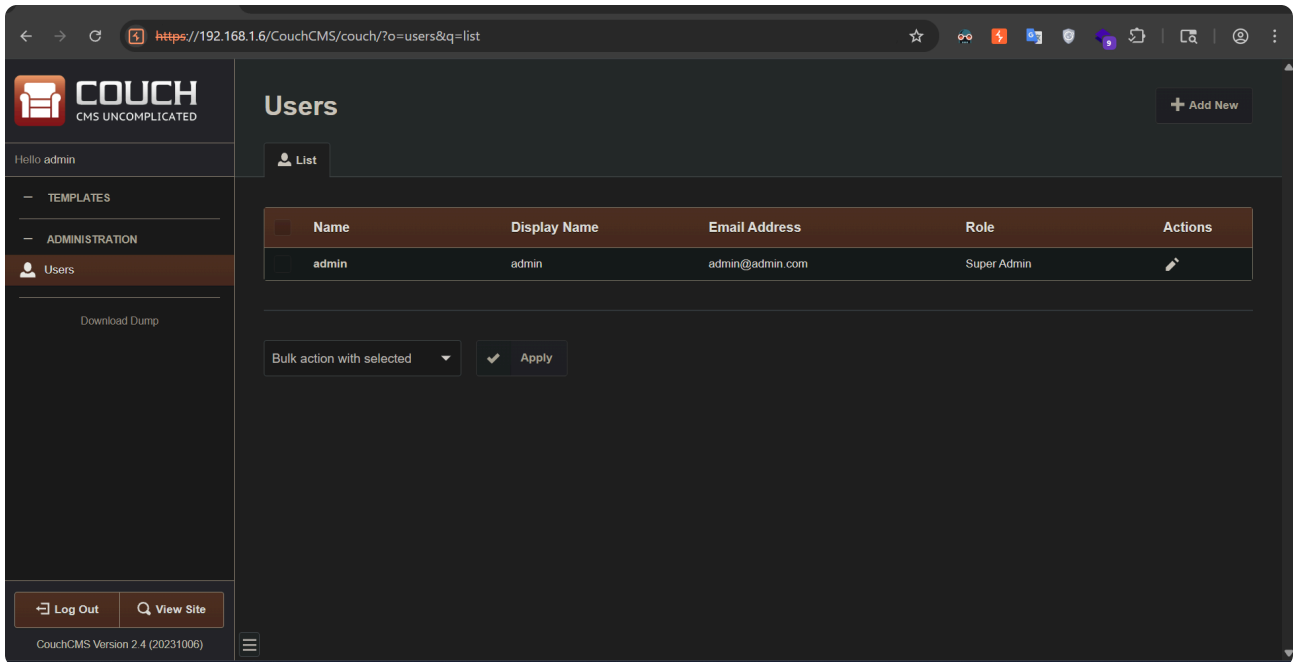
Sign in and log in with the first created credentials, which you made during the setup process.

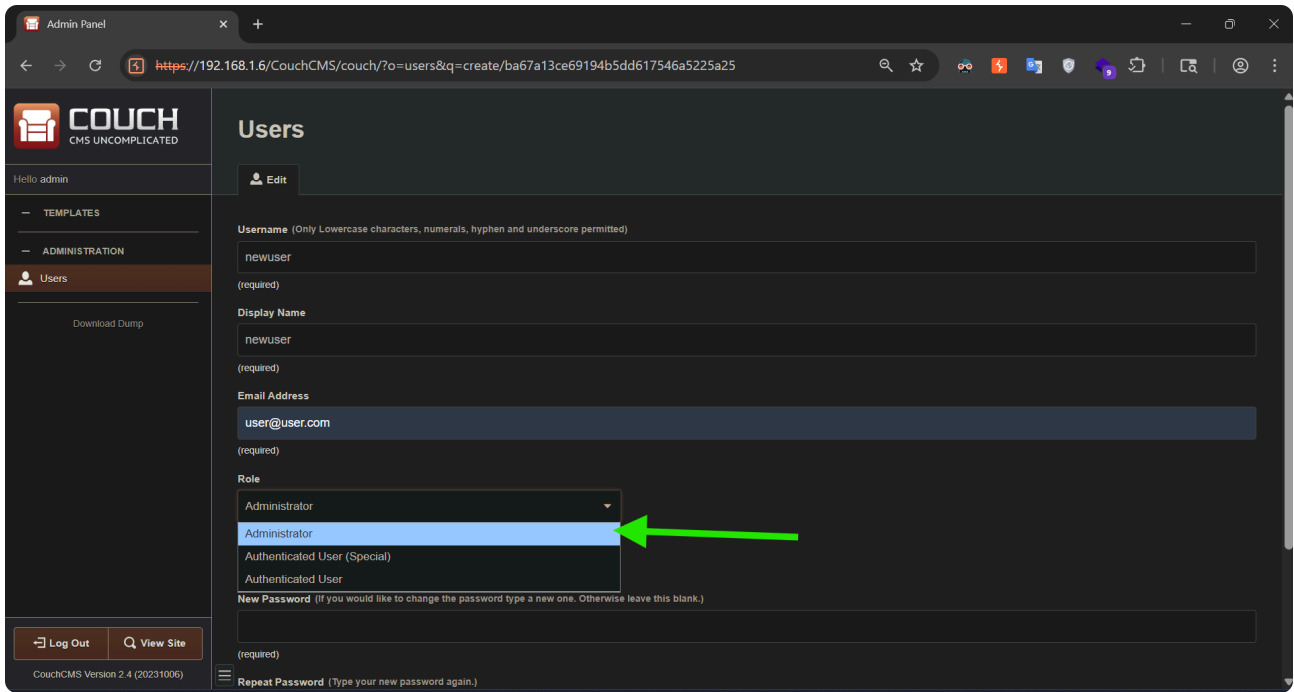
---

## 3. Navigate to the Users Section

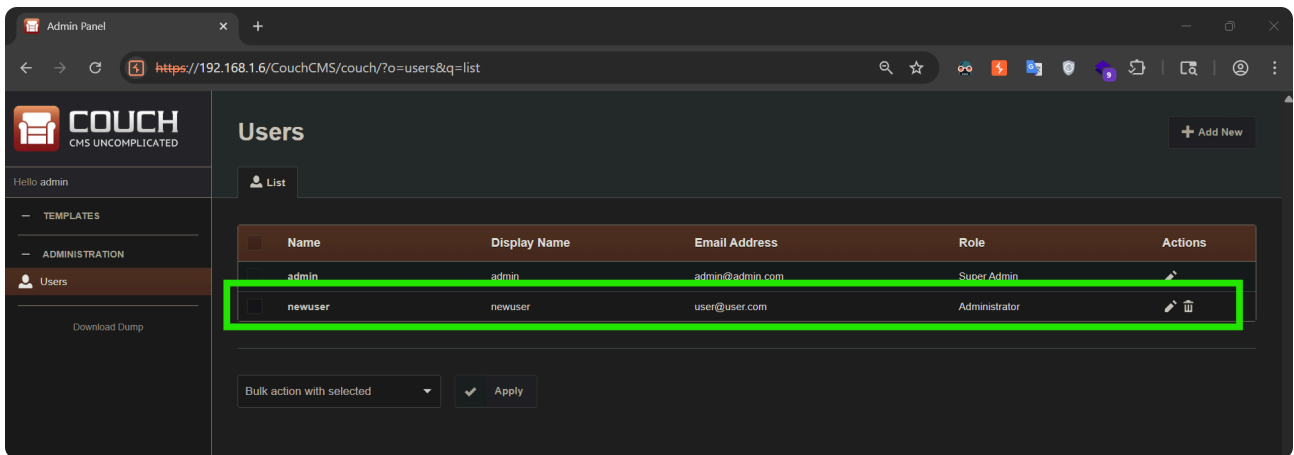


# 4. Add a Normal Admin User from Here

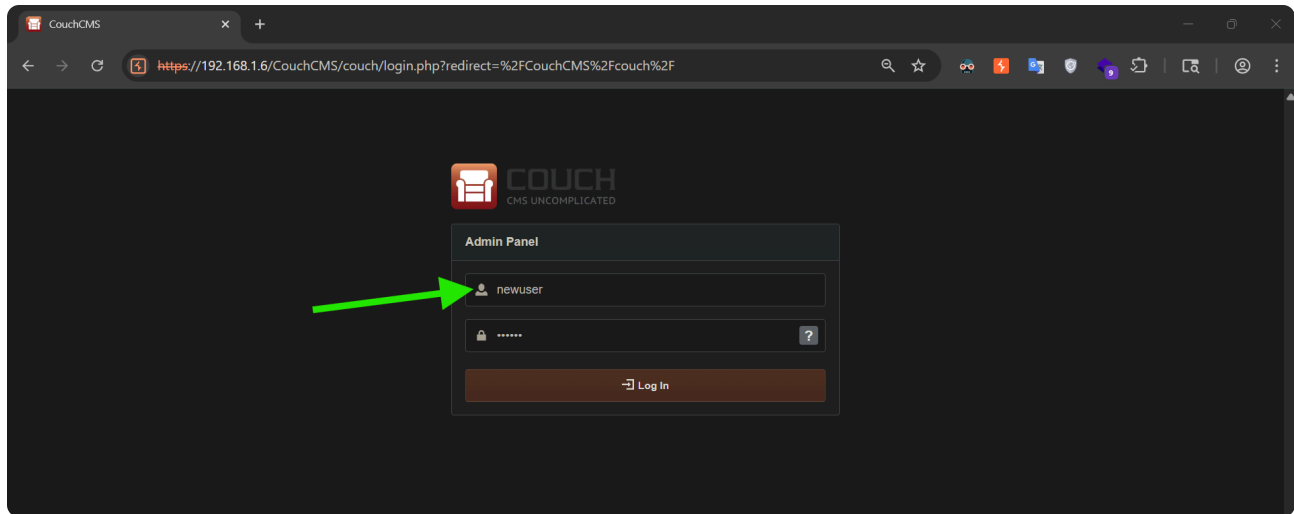




## 5. A Normal Admin User Added



## 6. Now Login as this `newuser` into the Application

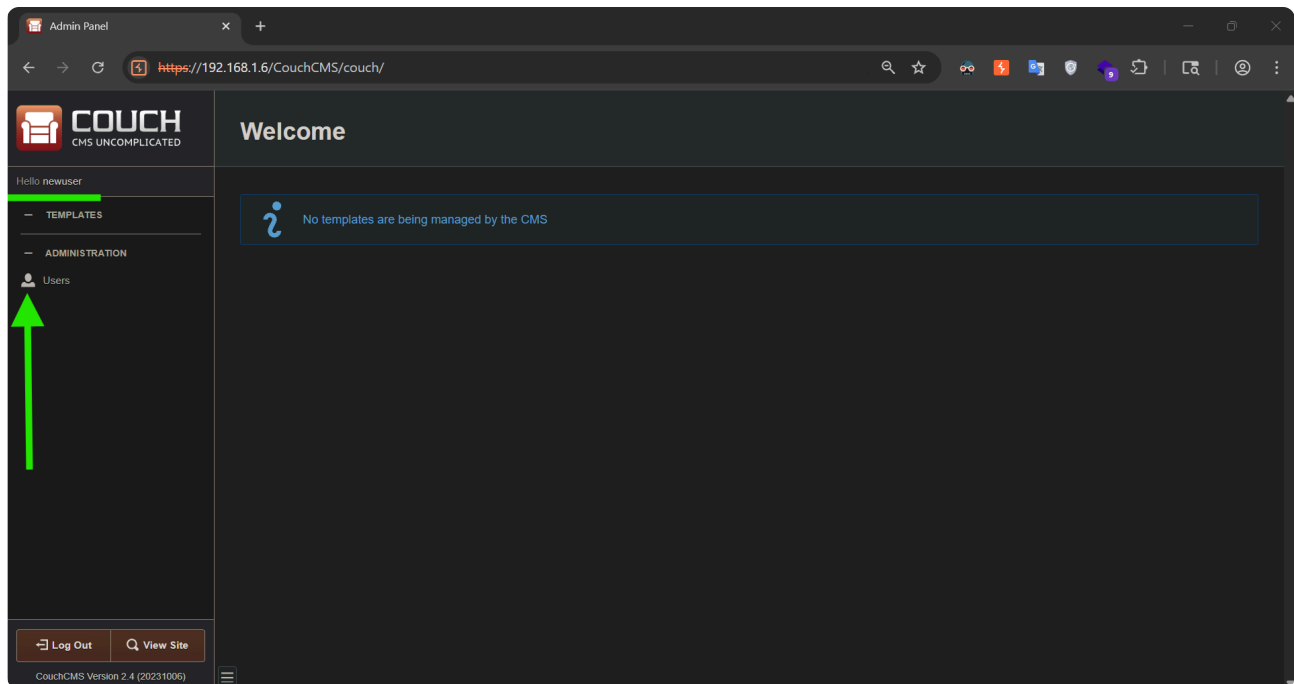


## 7. Expected Behavior

Now from here, no Admin user can able to add another Admin user or either Super Admin user, because the application is made in a way that only one Super Admin will be possible in the application.

## 8. Try to Add Any Normal User

Now navigate to the `Users` section, and try to add any normal user of your choice.



The top screenshot shows the CouchCMS Admin Panel 'Users' list page. A green arrow points to the '+ Add New' button in the top right corner. The table below shows the current users:

Name	Display Name	Email Address	Role	Actions
admin	admin	admin@admin.com	Super Admin	
newuser	newuser	user@user.com	Administrator	

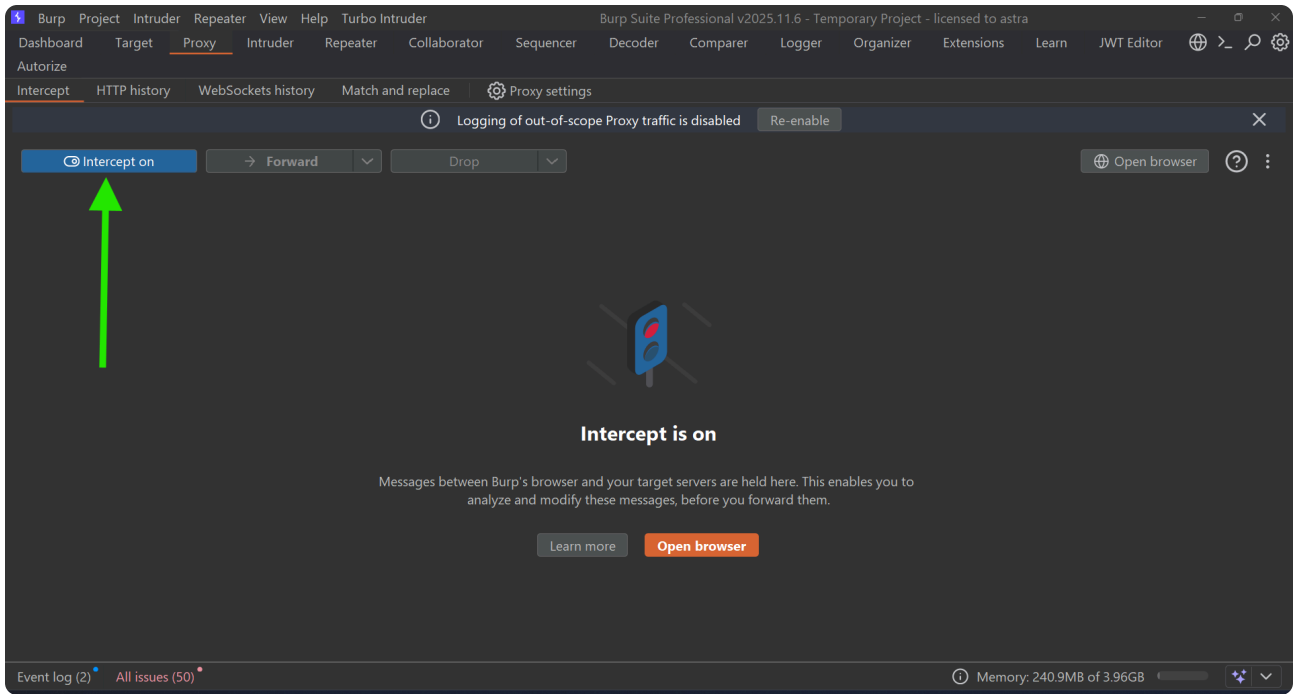
The bottom screenshot shows the 'Users' edit page. A green box highlights the 'Role' dropdown menu, which only shows 'Authenticated User' options:

- Authenticated User (Special)
- Authenticated User (Special)
- Authenticated User

There is no option to add any **SUPER ADMIN** or even **ADMIN** user.

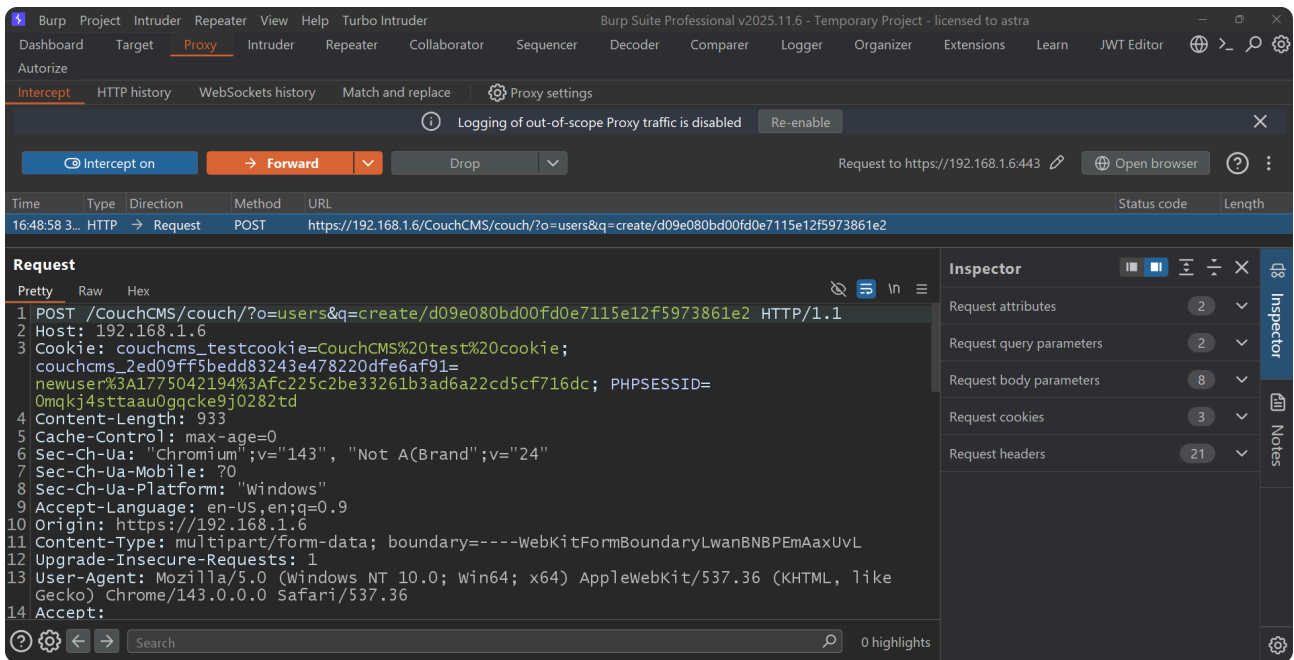
## 9. Intercept the Request Using Burp Suite

Before submitting the request, open Burp Suite and turn on interception.



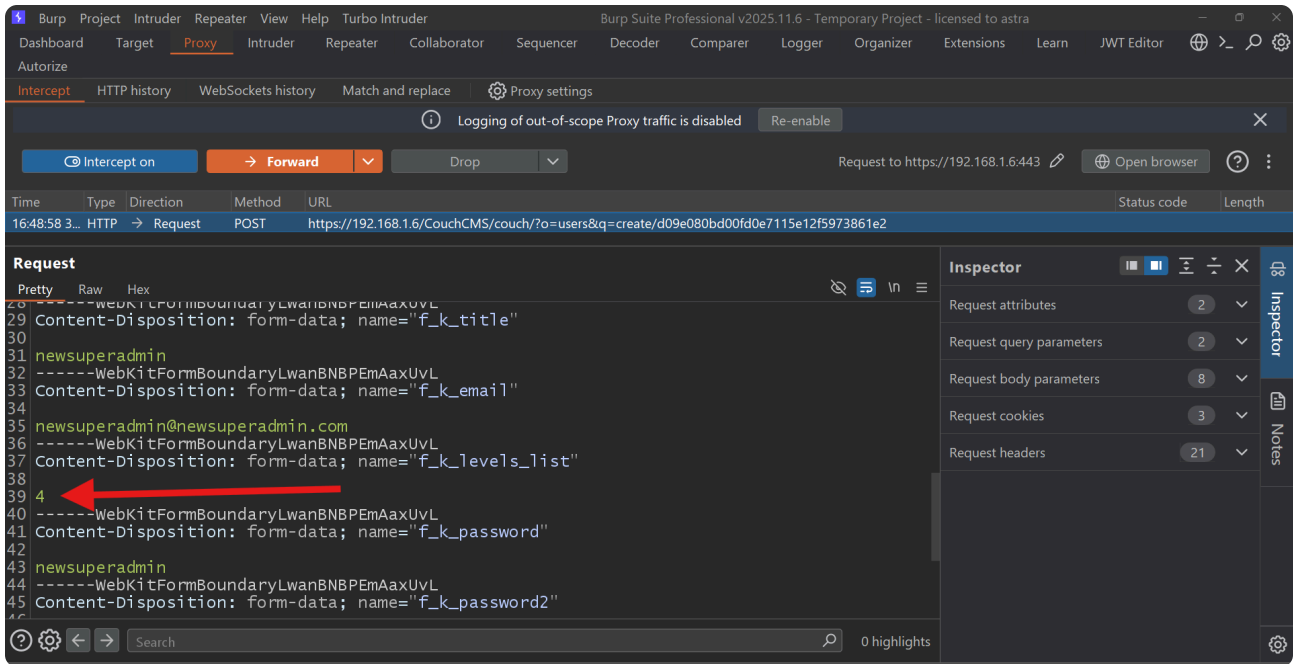
## 10. Capture the Raw HTTP Request

After clicking on `Save`, you are able to see the raw HTTP request here.



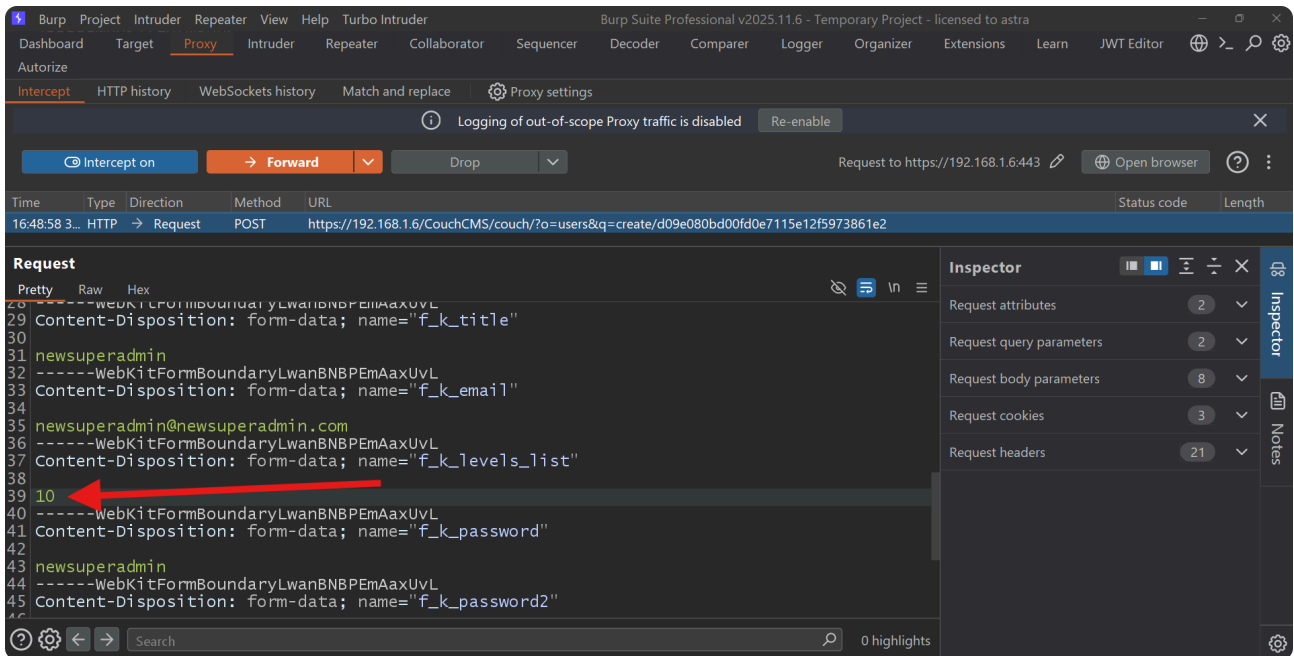
## 11. Locate the Parameter

Scroll down to the bottom, and you will find a new parameter: `f_k_levels_list`



## 12. Modify the Parameter Value

This value is 4, which represents only an authenticated user creation request. Now simply change this value to 10.

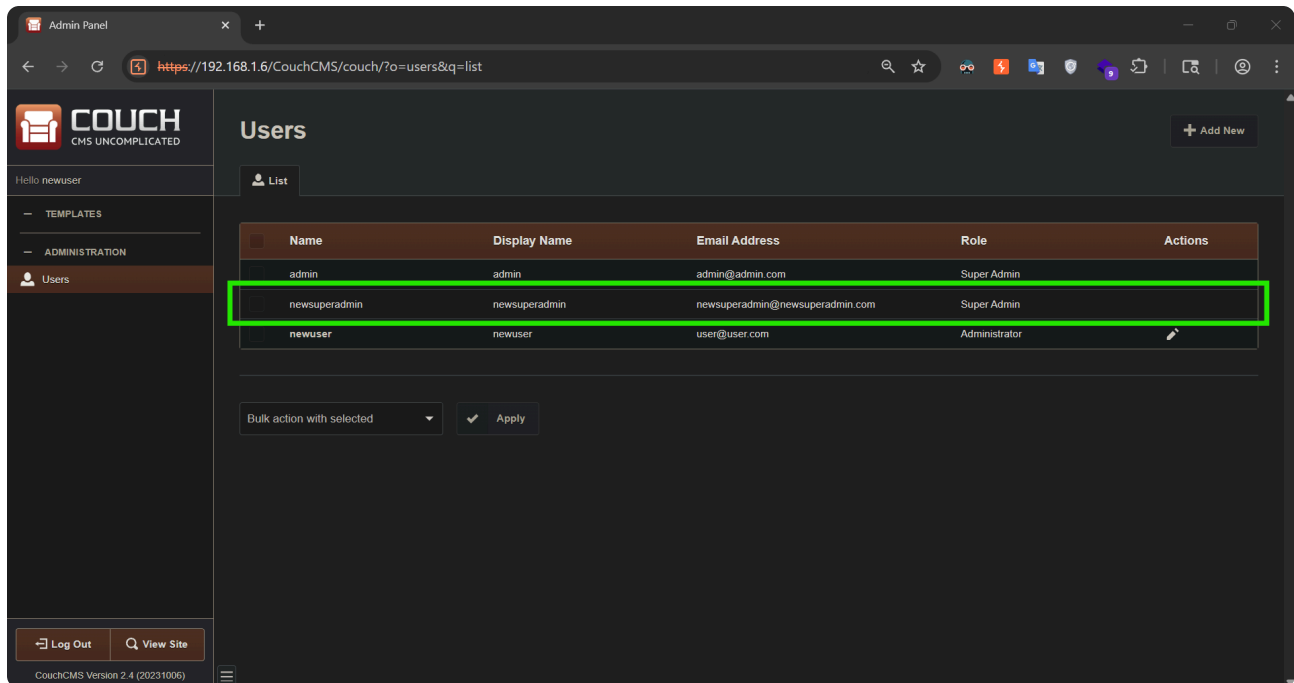


## 13. Forward the Request

And simply forward this request.

## 14. Verify the Result

Now navigate to the `Users` section again with the same `newuser`, and you will find that a new `Super Admin` user is created, which is never allowed to be created by this application.



## 15. Impact

This way, a normal Admin user is able to fully take over the application by adding a `Super Admin` user, which is never intended to be done.