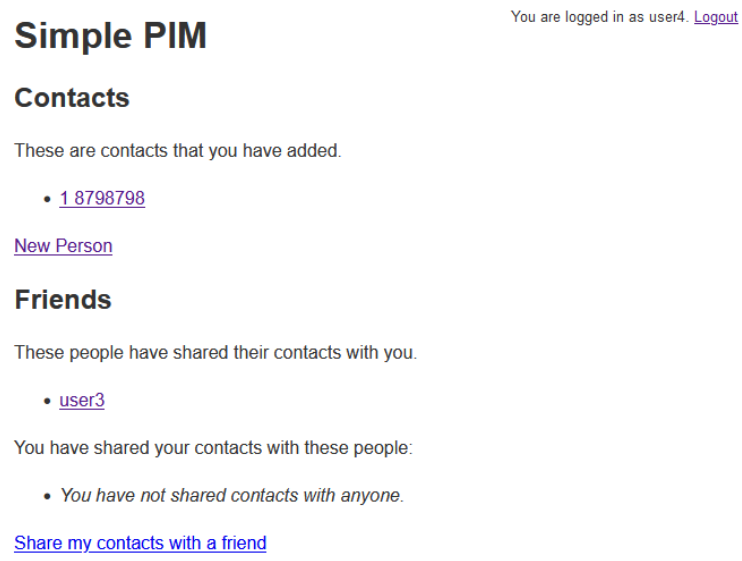
1.XSS(Cross Site Scripting)

When we Edit or Add some person's information, we can write some script, and it does really work! As the picture showed below.

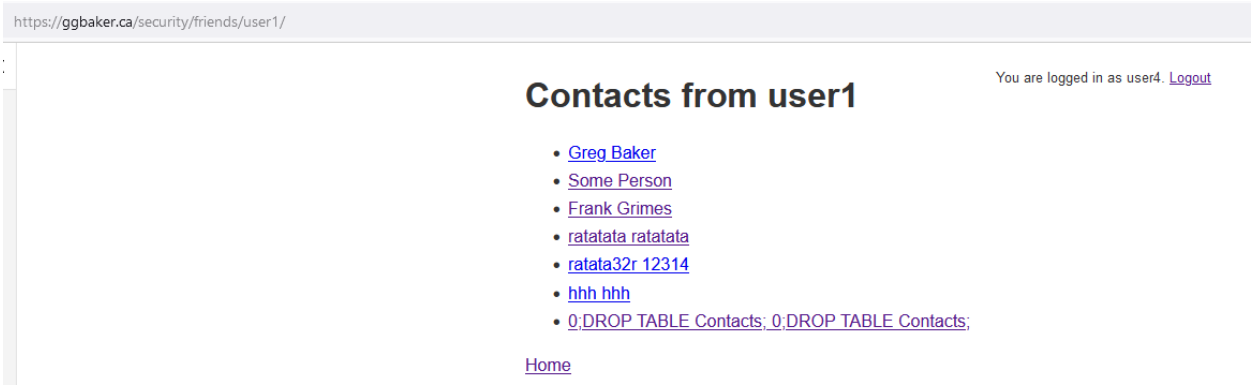
[Continued]

2.Insufficient authentication/permissions not checked(1)

I am User 4 and currently only user3 share his contact with me. The logic of this website should be: if some other people who does not share his contact with me, then I should not be allowed to view his contact. But I found I can still view other people's contact even if he did not share his contact with me.



I only need to visit the link: https://ggbaker.ca/security/friends/user3/, and change the /user3/ to /user1/, then I can view user1's contact without any authentication.

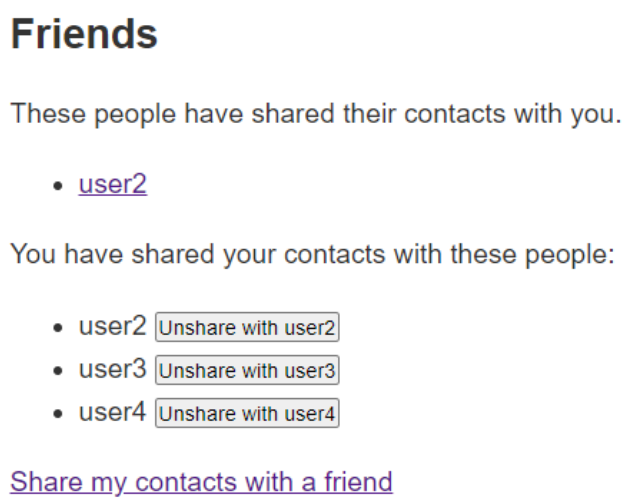


[Continued]

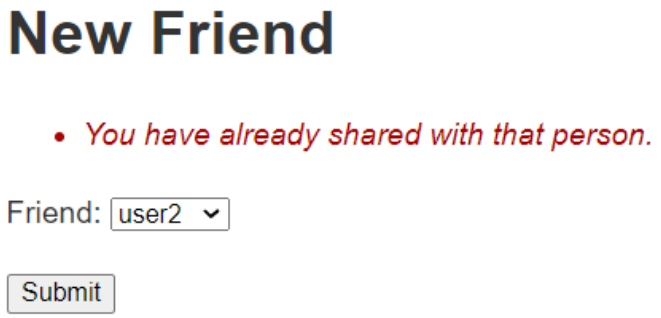
3.Insufficient authentication/permissions not checked(2)

I am user1, and now already shared my contact with all of user2, user3 and user4. But In this page,

When I click the ‘share my contacts with a friend’ -- When I attempt to launch a request, but I should not do so, after check from the server, this request should have been blocked, otherwise, while I step into that page, I will be deadly stuck inside.(see the picture below)



Whoever I choose, it will tell me that I already choose him, or I can not choose my self. There is no ‘home’ button, or ‘return back’ button, so user will not be able return back to any other page.



[Continued]

4.CSRF

While I am in this page, then enter the following script in the textbox,

<form action="/security/friends/user3/from-user1/delete" method="post"><input type="hidden" name="csrfmiddlewaretoken" value="aIJHkEk5PhmrDXJnXWnm6Dp5TDYHBE9bDIomA5YzG5U9h3MnUPLF3aORBD6mDgzT">

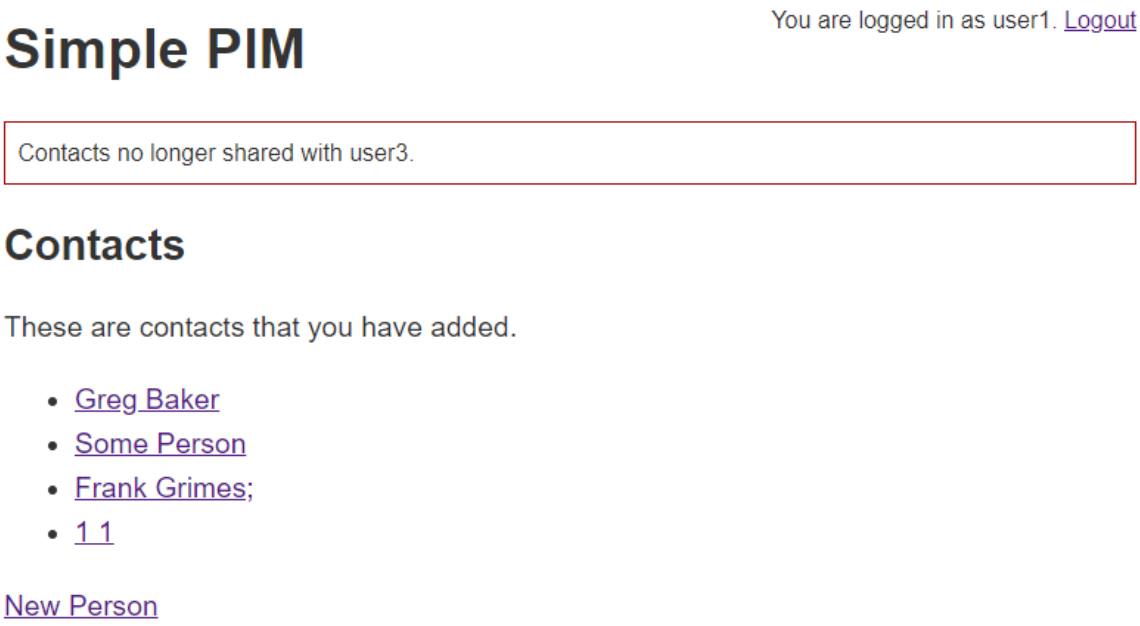
<input type="text" />

<input type="submit" value="Search" />

</form>

[Continued]

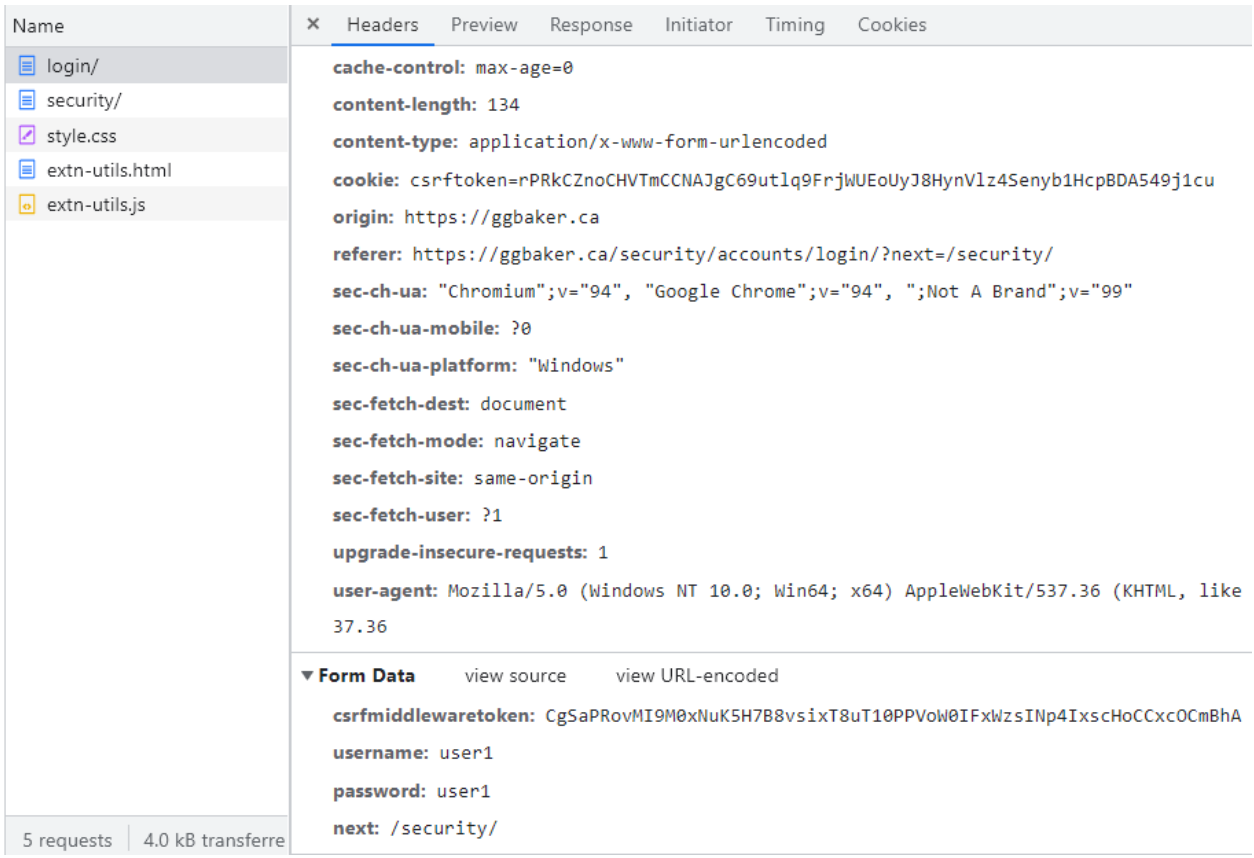
When we click the button, it will send the post and we will successfully be unshared with user3



[Continued]

5.Other Inappropriately logic 1

The exact password will be seen clearly in the post data(right-bottom). Maybe better if there are some technique(e.g., hash with salt and etc.) to keep it more secretly.



[Continued]

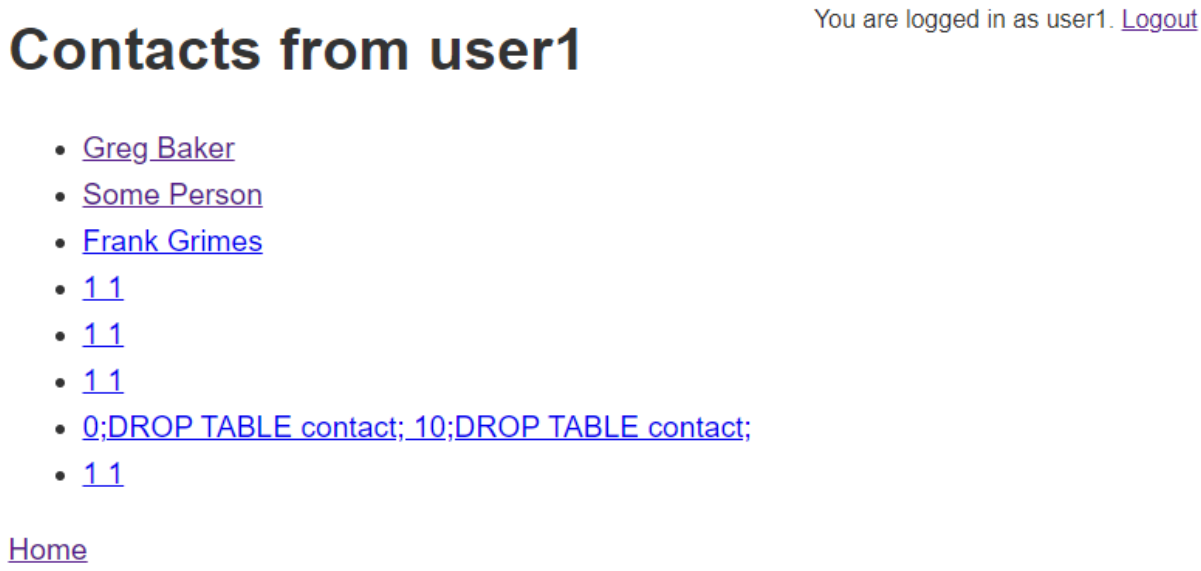
6.Other Inappropriately logic 2

I am now user 1, I can not add myself as a friend,

But I can still view my own contacts via this link, which seems weird, because we can see this link path is under ../friends/…

https://ggbaker.ca/security/friends/user1/

This implementation logic is a contradiction.



[End]