# 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.

# **Edit Person**

First Name: hello
Last Name: world
Email Address: 123123@123.com
Phone Number: 111-1111
<pre><script>alert('Hello World')</script></pre>
Notes:
Submit
<u></u>
ggbaker.ca 显示
Hello World
确定

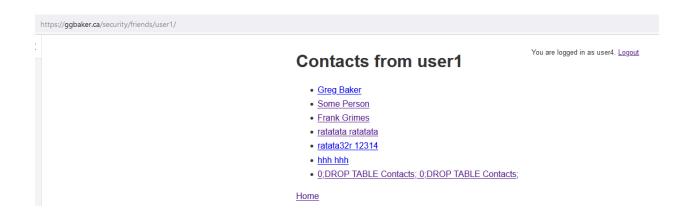
#### 2.Insufficient authentication/permissions not checked(1)

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.

# You are logged in as user4. Logout Contacts These are contacts that you have added. • 18798798 New Person Friends These people have shared their contacts with you. • user3 You have not shared contacts with anyone.

Share my contacts with a friend

I only need to visit the link: <a href="https://ggbaker.ca/security/friends/user3/">https://ggbaker.ca/security/friends/user3/</a>, 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)

#### **Friends**

These people have shared their contacts with you.

• user2

You have shared your contacts with these people:

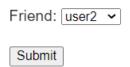
- user2 Unshare with user2
- user3 Unshare with user3
- user4 Unshare with user4

Share my contacts with a friend

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.

# **New Friend**

You have already shared with that person.



# 4.CSRF

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

Edit | Home

Edit Person
First Name: 1
Last Name: 1
Email Address:
Phone Number:
Notes:
Submit
Home
<pre><form action="/security/friends/user3/from-user1/delete" method="post"><input name="csrfmiddlewaretoken" type="hidden" value="aIJHkEk5PhmrDXJnXWnm6Dp5TDYHBE9bDIomA5YzG5U9h3MnUPLF3aORBD6mDgzT"/></form></pre>
<input type="text"/>
<input type="submit" value="Search"/>
Details for 1 1
First Name
1
Last Name
1 Notes
not share with user3

[Continued]

# Simple PIM

You are logged in as user1. Logout

Contacts no longer shared with user3.

#### **Contacts**

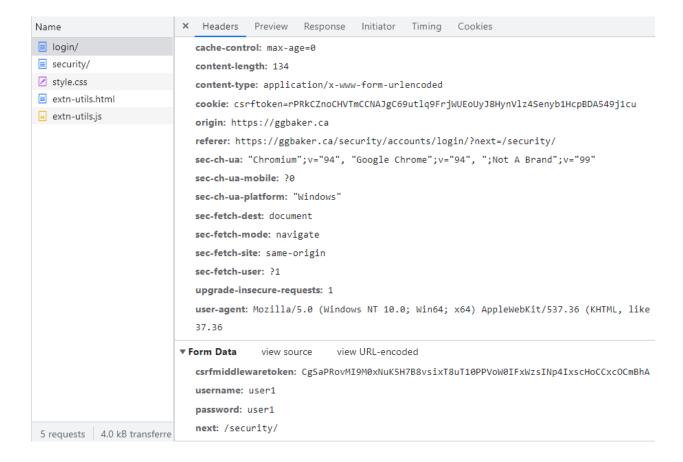
These are contacts that you have added.

- Greg Baker
- Some Person
- · Frank Grimes;
- <u>11</u>

New Person

#### 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.



#### 6.Other Inappropriately logic 2

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

# **New Friend**

You are logged in as user1. Logout

· Cannot friend yourself.

Friend: user1 V

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.

# Contacts from user1

You are logged in as user1. Logout

- Greg Baker
- Some Person
- Frank Grimes
- 11
- <u>11</u>
- 11
- 0;DROP TABLE contact; 10;DROP TABLE contact;
- 11

**Home**