

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:

Last Name:

Email Address:

Phone Number:

Notes:

```
<script>alert('Hello World')</script>
```

[Home](#)

ggbaker.ca 显示

Hello World

确定

[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.

Simple PIM

You are logged in as user4. [Logout](#)

Contacts

These are contacts that you have added.

- [1 8798798](#)

[New Person](#)

Friends

These people have shared their contacts with you.

- [user3](#)

You have shared your contacts with these people:

- *You have not shared contacts with anyone.*

[Share my contacts with a friend](#)

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.

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

Contacts from user1

- [Greg Baker](#)
- [Some Person](#)
- [Frank Grimes](#)
- [ratatata ratatata](#)
- [ratata32r 12314](#)
- [hhh hhh](#)
- [0;DROP TABLE Contacts; 0;DROP TABLE Contacts;](#)

[Home](#)

You are logged in as user4. [Logout](#)

[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
- user3
- 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.*

Friend: ▼

[Continued]

4.CSRF

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

Edit Person

First Name:

Last Name:

Email Address:

Phone Number:

Notes:

[Home](#)

```
<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>
```

Details for 1 1

First Name

1

Last Name

1

Notes

[Edit](#) | [Home](#)

[Continued]

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

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;](#)
- [1 1](#)

[New Person](#)

[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.

Name	× HeadersPreviewResponseInitiatorTimingCookies
login/	cache-control: max-age=0
security/	content-length: 134
style.css	content-type: application/x-www-form-urlencoded
extn-utils.html	cookie: csrftoken=rPRkCZnoCHVTmCCNAJgC69utlq9FrjWUEoUyJ8HynVlz4Senyb1HcpBDA549j1cu
extn-utils.js	origin: https://ggbaker.ca
	referer: https://ggbaker.ca/security/accounts/login/?next=/security/
	sec-ch-ua: "Chromium";v="94", "Google Chrome";v="94", ";Not A Brand";v="99"
	sec-ch-ua-mobile: ?0
	sec-ch-ua-platform: "Windows"
	sec-fetch-dest: document
	sec-fetch-mode: navigate
	sec-fetch-site: same-origin
	sec-fetch-user: ?1
	upgrade-insecure-requests: 1
	user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like 37.36
	▼ Form Data view source view URL-encoded
	csrfmiddlewaretoken: CgSaPRovMI9M0xNuK5H7B8vsixT8uT10PPVow0IFxWzsINp4IxsCHoCCxcOCmBhA
	username: user1
	password: user1
	next: /security/
5 requests	4.0 kB transferred

[Continued]

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:

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](#)
- [1 1](#)
- [1 1](#)
- [1 1](#)
- [0;DROP TABLE contact; 10;DROP TABLE contact;](#)
- [1 1](#)

[Home](#)

[End]