How I Got *Jon Doe* to be Friends With Me

First, after studying the `add_friend.php` script, I noticed that the script took an `id` parameter. This `id` parameter is used as the id of the account you want to friend. After seeing this, I made this link:

> http://csec380-core.csec.rit.edu:84/add_friend.php?id=36

And posted it to the message board. My username:

> oneNutW0nder reee :: id=36

How I Fixed This Issue

This issue can be fixed by implementing CSRF tokens. These tokens will be generated when a user logs in, and they will be sent with each request. When the request reaches its destination (application endpoints) the token sent with the request will be checked against the token generated for the session.

Files Edited
> login.php – Generate a token when successful login occurs
> home.php – Added tokens to requests to add/del_friend.php
> search.php – Added tokens to requests to add/del_friend.php
> add_friend.php – Check session token against request token
> del_friend.php – Check session token against request token

Now, if I send the same link to *Jon Doe* he will not be able to friend me because a token is not included in his request.

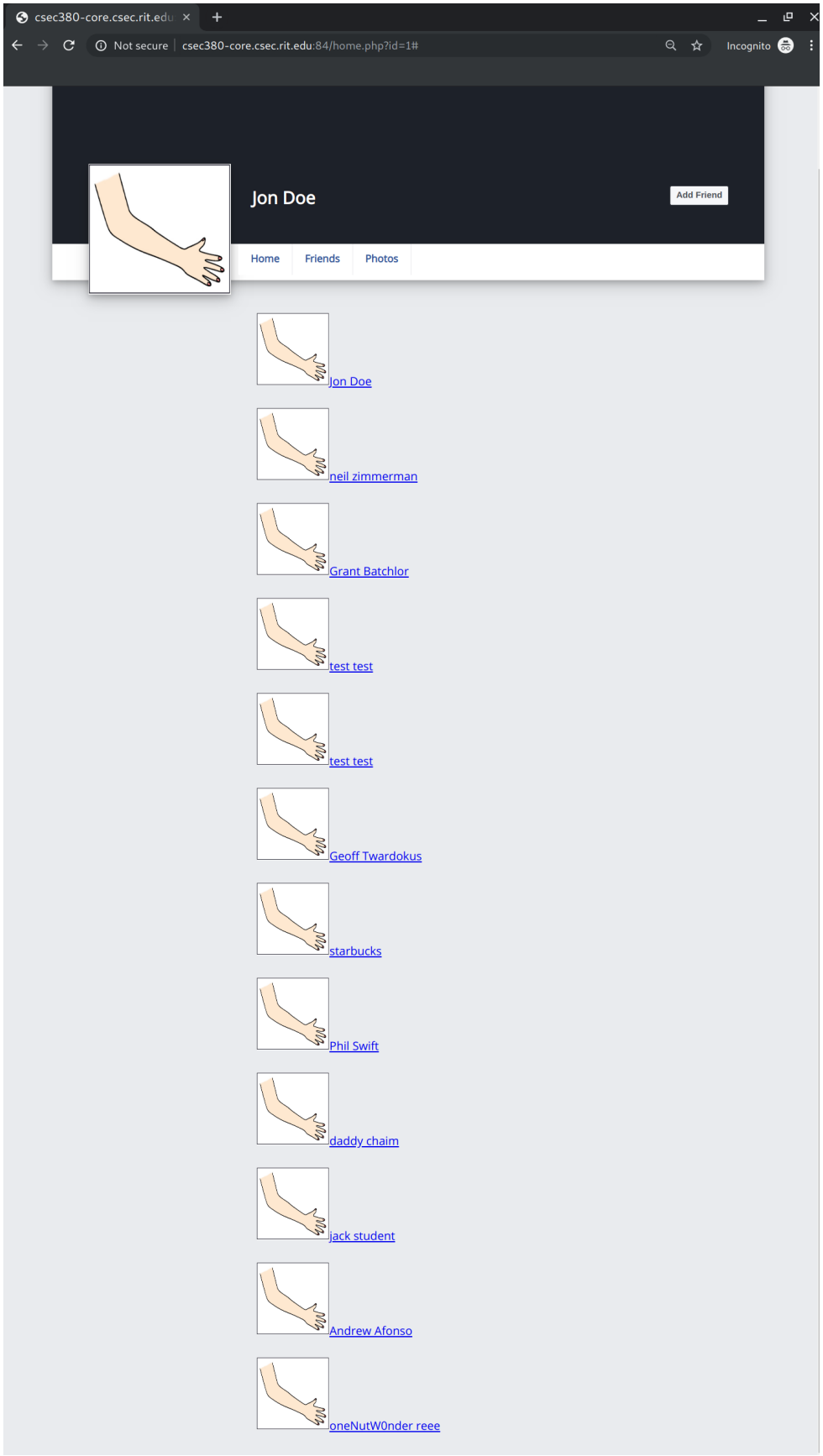

Figure 1: Friends