How I made Jon Doe Friend me on Armbook:

First, I created my account:

First Name: Sean

Last Name: Kells

Your Email: chipmunkd3@gmail.com

Re-enter Email: chipmunkd3@gmail.com

New Password: Spaghettios!4

I am: Male

Birthday: Jan 1 1960

After surfing the website I noticed that other users homepages have the full URL of http://csec380-core.csec.rit.edu:84/home.php?id='#'# . I noted the id query parameter that may be useful. I examined the armbook source code and located the add_friend.php, which also seems to take in an id. The php file friends users based on their id parameter value and has no apparent protections if the session is still open. (NO CSRF Tokens). For this I needed the id of my account, for this I created another secondary account.

Secondary Account (Used to find my initial account ID)

First Name: Fake

Last Name: Accountz

Your Email: superhacker@gmail.com

Re-enter Email: superhacker@gmail.com

New Password: Spaghettios!4

I am: Male

Birthday: Jan 2 1960

I found that my ID was 30 and went to http://csec380-core.csec.rit.edu:5004/ and placed the URL http://csec380-core.csec.rit.edu:84/add_friend.php?id=30 inside the 'Leave a Comment' forum. Now all I had to do was add Jon Doe as a friend and my work is complete.