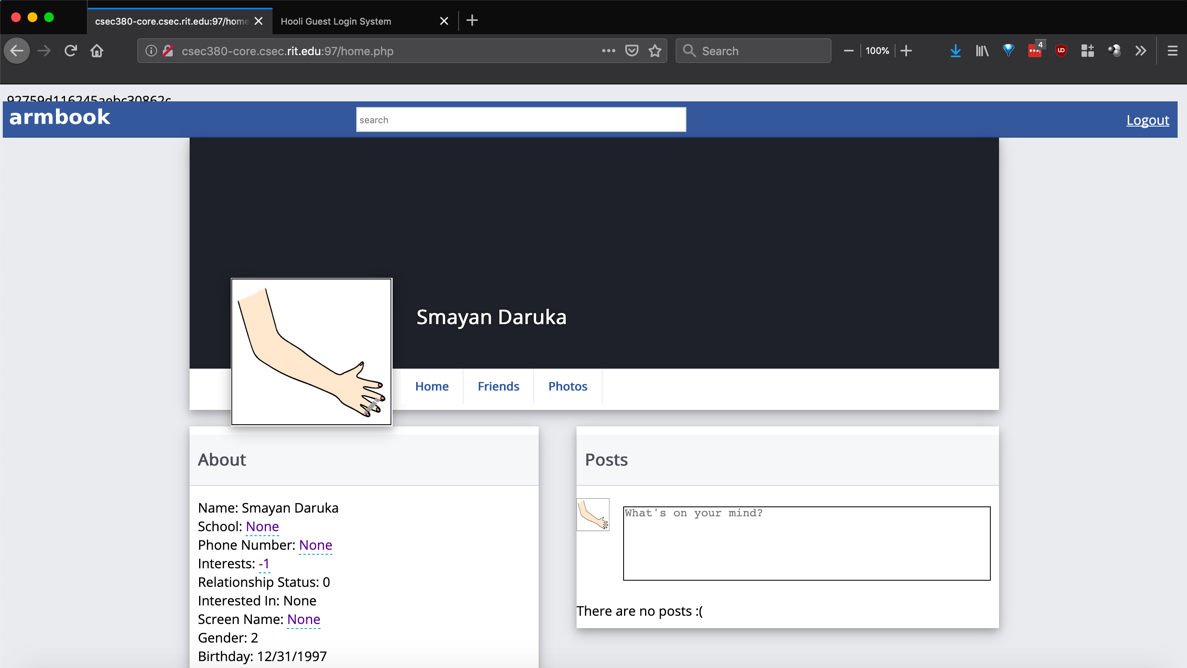
**Homework 7 –Writeup**

**ACTIVITY 1 – STEP 2 (Find out about the Client):**

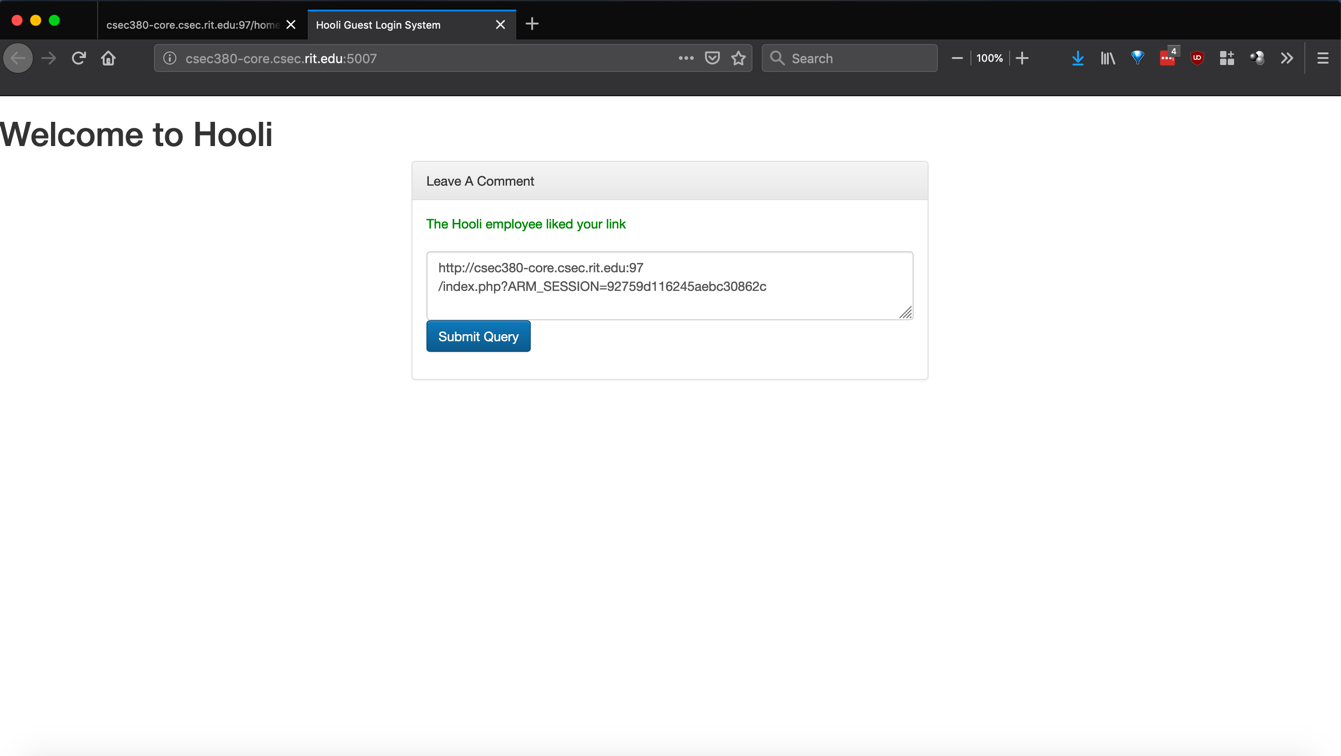
The image below shows my profile page upon logging in:



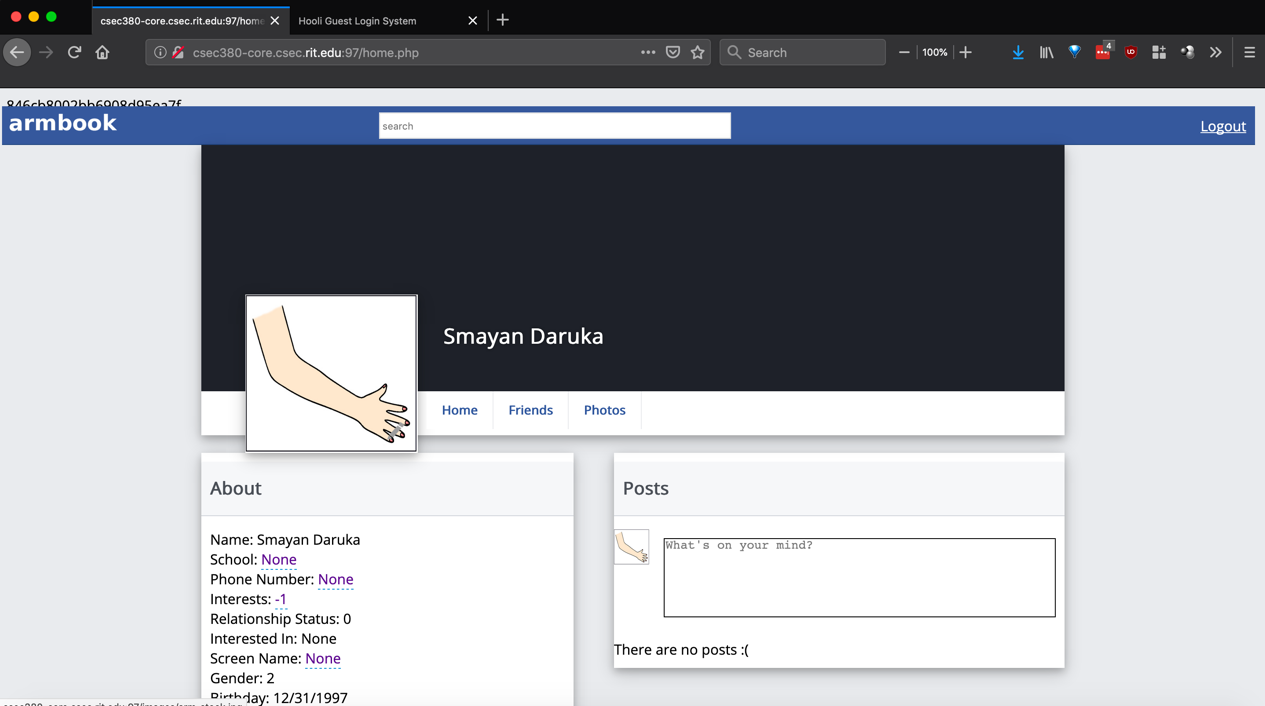
As we can see above, there is a session ID that is visible on the top left. The session ID currently is “92759d116245aebc30862c”.

The next step is to use the session ID above and send the following crafted link to the guestbook:

“http://csec380-core.csec.rit.edu:97/index.php?ARM\_SESSION=92759d116245aebc30862c”



In order to prove that the session ID changes when someone logs in, I logout and log back in which can be seen in the screenshot below:



The new session ID that can be seen above is “846cb8002bb6908d95ea7f”.

At this point, I logout again and go to the following link from the first screenshot:

“http://csec380-core.csec.rit.edu:97/home.php?ARM\_SESSION=92759d116245aebc30862c”

A screenshot of a social media post

Description automatically generated

As can be seen above, I was able to use the session ID and login as someone else.

**ACTIVITY 1 – STEP 3 (Fix the client):**

I updated index.php and login.php to mitigate the session fixation issue. The dockerfile and all its components are in the folder called “ACT1STEP3”.

**ACTIVITY 2 – STEP 1 (Testing for fitness):**

I used Burp to analyze the security of the session ID that is generated by the new armbook.

A screenshot of a social media post

Description automatically generated

This screenshot shows that effective entropy is 0 bits. This means that it is fairly easy to guess the session IDs being generated.

A screenshot of a cell phone

Description automatically generated

In this screenshot, we see that the maximum bits of entropy are 1.

A screenshot of a social media post

Description automatically generated

In this screenshot, all the bits failed the FIPS run test. This test concludes that the session IDs aren’t completely random and it is possible to brute force them and figure out valid session IDs.

**ACTIVITY 2 – STEP 2 (Recommended changes):**

The PowerPoint presentation is in the folder “ACT2STEP2”.

**ACTIVITY 3 – STEP 1 (Punish Him!):**

As can be seen below, I was able to login and made a comment using Jon Doe’s account.

A screenshot of a social media post

Description automatically generated

The screenshot below shows the credentials for the account above.

A screenshot of a computer

Description automatically generated

Username is “ces1509@rit.edu” and password is “AReallyComplexPassword”.

**ACTIVITY 4 – STEP 1 (Finish Him!):**

Using Burp, I was able to find usernames and passwords to other people’s accounts. There are screenshots below that also prove me logging in and making a post on their profile.

A screenshot of a social media post

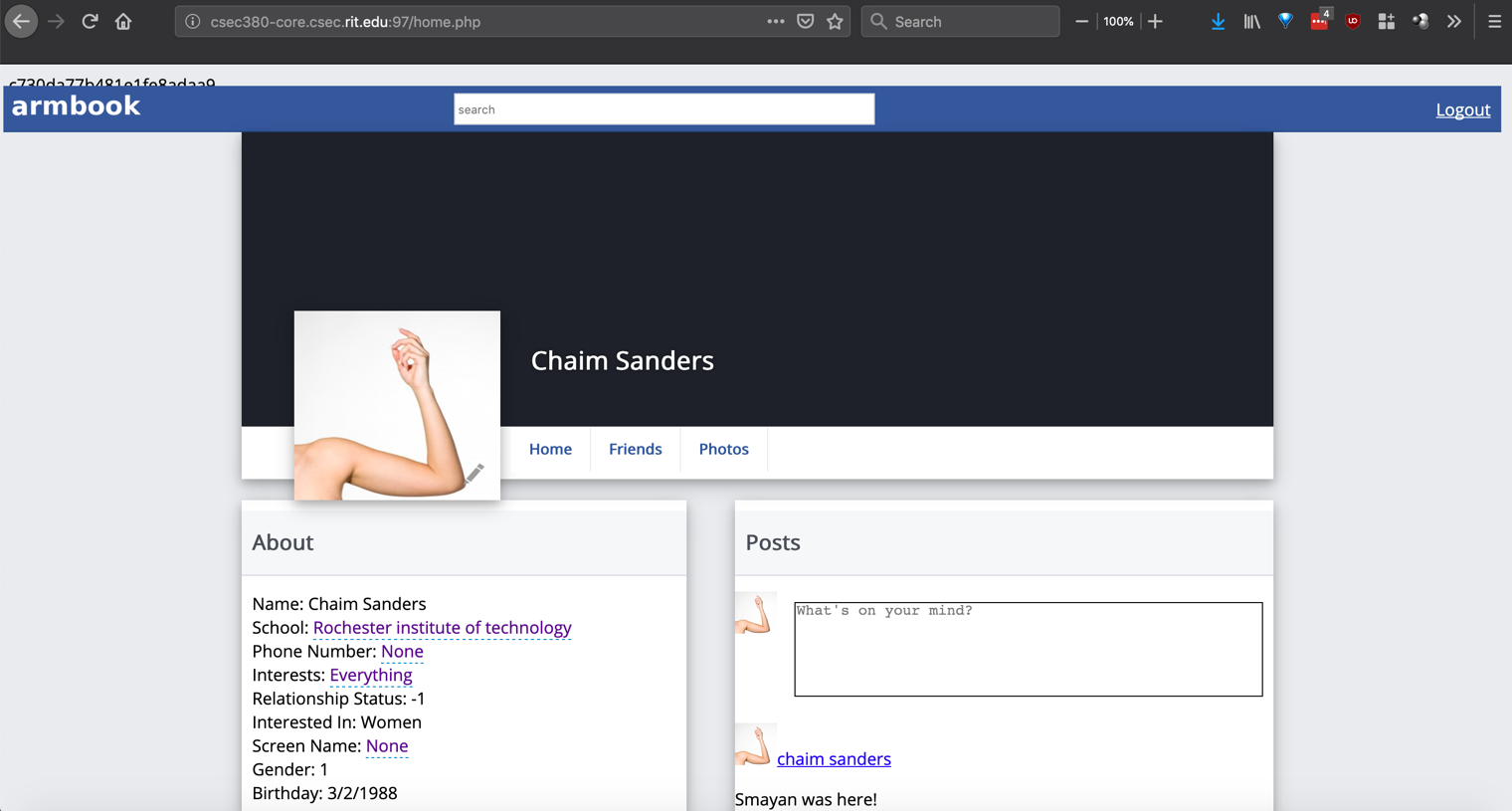
Description automatically generated

Username is “neil@neil.com” and password is “apple”.

A screenshot of a social media post

Description automatically generated

Username is “jruppal@gmaill.com” and password is “password”. I was unable to make a comment for some reason.



Username is “chaim@chaim.com” and password is “test”.