Nicholas Graca

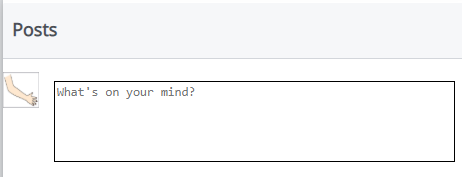
Web App Homework #6 Writeup

Act 1:

When you put a script in the search bar, it was reflected XSS because it only showed me the alert once to me.



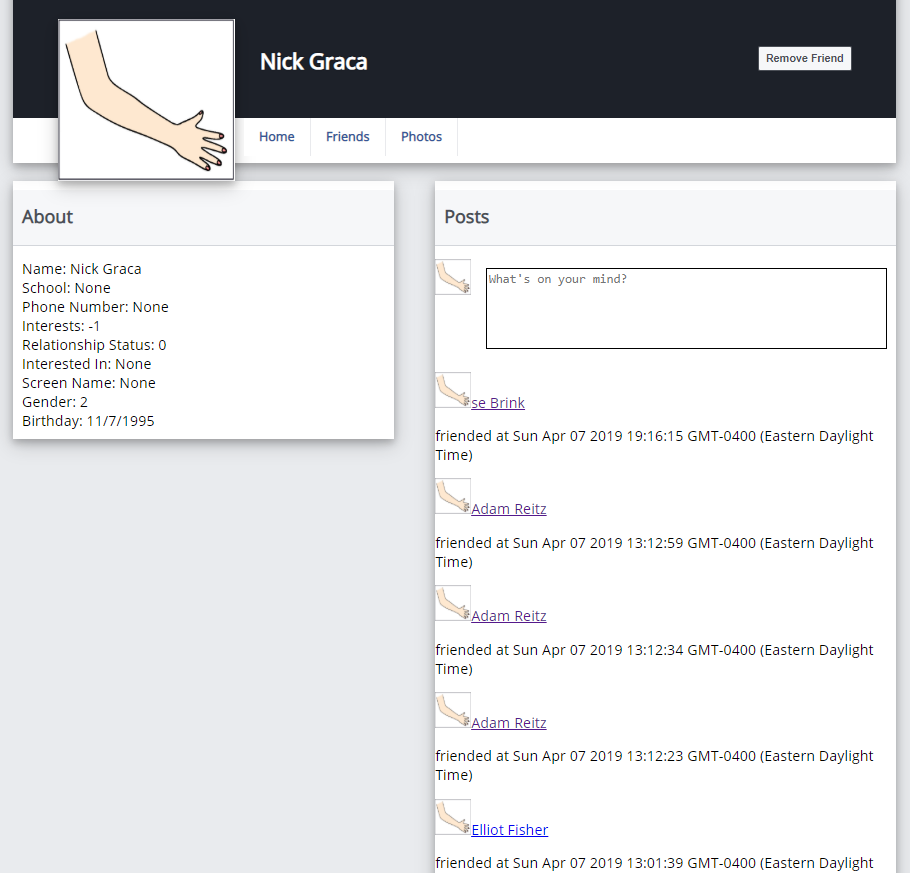
However, when you put a script into the comment section, this would be persistent XSS since the web server saved the comments so every time you loaded the page, it would run the script and for anyone that looked at my page.



Act2:

See attached file for my code.

Here is a screenshot showing some of the people that friended me.



Act 3:

I found that there for a /admin/admin.php file and f you go there you can see every ones password including the admins. You then use those credentials to sign in at /admin and once authenticated you can change Andy’s password. It changed it from ‘ADifferentPassword’ to ‘ChangeIt’.

