**Project 2 Sprint 1**

This past lecture Momo went over a range of different vulnerabilities that can be used to exploit web applications. This week’s goal is to with your team assess the security of an application without the source code provided. Most of the vulnerabilities that were discussed in class are possible in this application.  
  
This week the required submission is very simple we need each of you to spend some time and consider all the different angles you could use to exploit this application. After having done that we want each of you to provide a simple walk through of what you tried.   
  
**You do not need to be successful in exploiting the application this week. If you are able to exploit it good for you that will be less work for the next week.   
  
Requirements:**There must be N short explanations ( 3 sentence minimum ) of what you observed in the application that you believe may be vulnerable and how you went about attempting to exploit it for the number N of students on your team.  
  
  
**Application Information:**  
The application is accessible at: http://chalbroker.cs1122.engineering.nyu.edu:5555/  
  
You will be asked to enter your netid and then you will be redirected to the application so you can assess it.  
  
**Important:** The web application is private to each student you can register any amount of accounts you need to, to accomplish the exploit you are attempting. Try not to destroy the container but we can reset it if you break it beyond repair.

**Reference Information:**  
The exploits that are possible here were each talked about in about enough depth during the lecture to attempt this week and for implementation next week. If you are still confused for reference you can refer back to those slides or search : <https://www.owasp.org/index.php/Main_Page> for more reference material regarding the implementation of each exploit.