**Project 2 Sprint 2**

Given the past week you and your group should now have had time to think about what was vulnerable in the application. Remember even if it turns out that what you thought was vulnerable was not actually vulnerable, that is fine. We just wanted you to think about what you could possibly do.  
  
This week you will be responsible for actually exploiting the application. The source code will be accessible to you under the resources section of Project 2 and the resources repo on the GitHub. You and your team must work together to successfully complete 3 different exploits against the application.   
  
  
Remember it is important to know that more basic vulnerabilities can be combined into more complex attacks and these will count as a distinct vulnerability.  
  
You also may need to use multiple accounts on the application itself. To “logout” on the application you may delete the cookie called “token” that is associated with the challenge’s domain.

Partial Credit will be awarded if the attack is not successful, but you still provide us with a write up of what you have attempted and any example code you were trying.  
  
As you will see in the source code, the entire application is JavaScript and Python, some of you had asked about PHP and there is none in here. This is using code very similar to what you learned in Project 1 made poorly on purpose to facilitate easier exploitation.

Additionally the OWASP top 10 contains the exploits we expect you to create here. Not all 10 are possible but at least 5 are possible.  
  
**Note:** Changing the chalbroker auth token to access other students containers is not a vulnerability it is intended behavior of chalbroker for identifying docker containers. Modifying another student’s container will not be tolerated.  
  
 **Requirements:**Given the source code for the application and the week you have spent looking at the application for ways it might be vulnerable, this week you will need to successfully exploit at least 3 vulnerabilities in the application.  
  
Each vulnerability will be worth 33% of your grade for Sprint 2.  
  
To earn your full 33% of the grade a step by step instruction of what you did to successfully exploit the application must be provided. From reading your instructions any of the TA’s should be able to successfully reproduce the vulnerability and see it work on your application. We additionally like screenshots of the successful exploit and any code you wrote for the exploit.  
  
This requires special attention to detail and thinking about the fact the TA’s are not you as a person. What makes sense in your head may not to someone else so when in doubt be more explicit in your instruction, even if you find it trivial it is in your best interest to be as explicit as possible.   
  
**Please submit each exploit as a PDF through your project github.**  
  
  
**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.