CS 6035

FLAG 4: Command and Concat (25 pts)

Make sure you have gone through the Setup and Intro sections.

If you haven't already, run the start script in the home directory of log4j user, start the container with the start script:

```
./StartContainer.sh
```

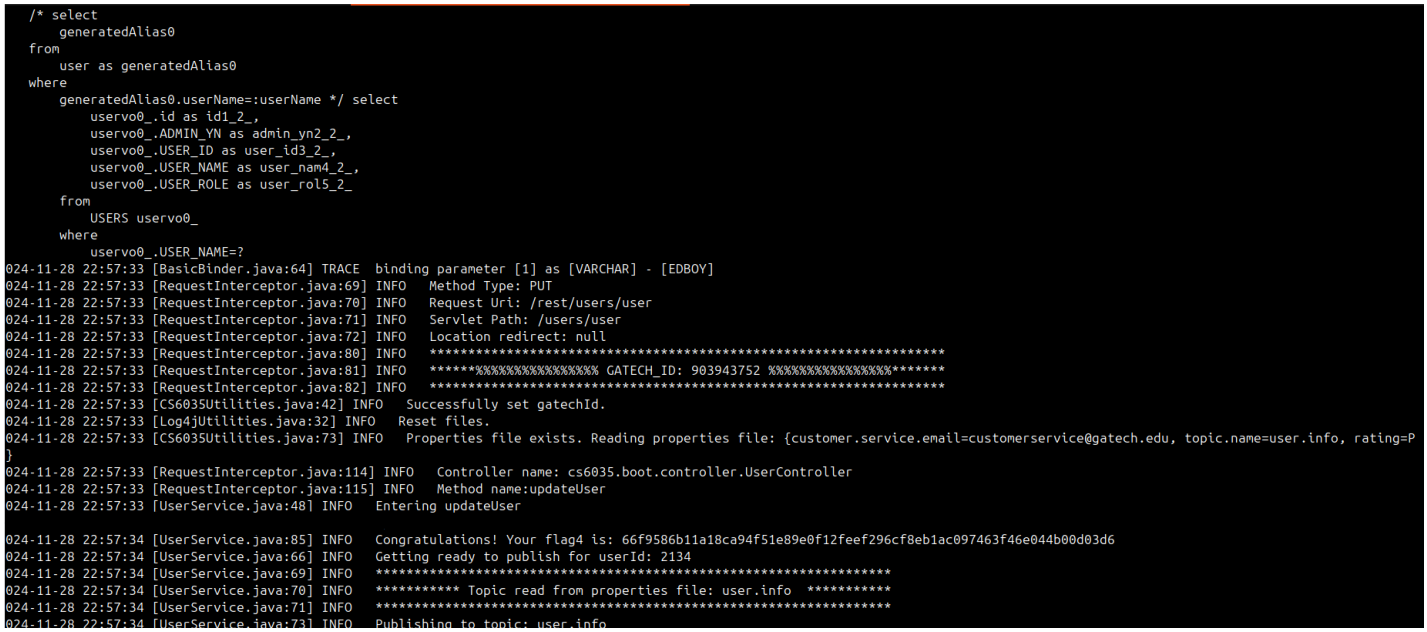
For this flag, we will exploit an endpoint that adds a new user:

```
curl -X PUT 'http://localhost:8080/rest/users/user' -H 'GATECH_ID:123456789' -H 'Content-Type:app
```

Take some time to inspect this output and see what you need to exploit. Yes the exception is expected, and maybe there is even a clue above it ;)

For this flag, you will construct a malicious file (Exploit.java) and compile it, so that when deserialized it will create a simple ".txt" file on the server to get the flag. Using the log4shell exploit, create a file named "Ronnie.txt" on the server and add ONE line that says "AintNothinButAPeanut!" (You do not need the quote). If you do not follow this exactly, you will not get this flag.

Upon success, you will see the output below. (You might have to scroll for this)



Hint: The name of this flag is a huge hint as to what you need to do. Pay close attention to the logged messages and their format.

*** **IF THIS FLAG COMES OUT BLANK, Restart container by running the stopContainer and startContainer scripts in the home directory of the log4j user. *****