CS 6035

FLAG 5: PubSub Override (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 a previous endpoint that publishes updates to a topic on the server:

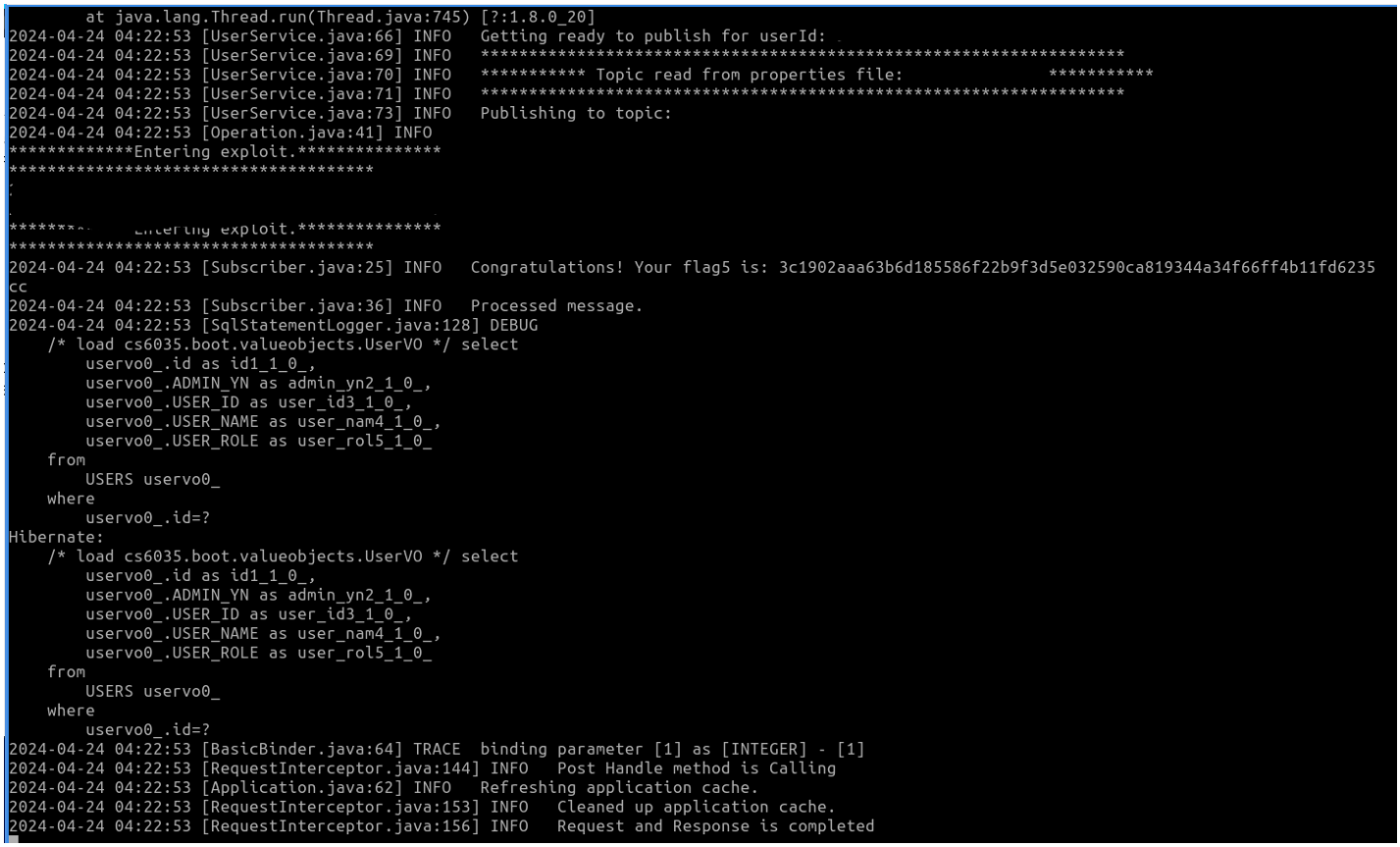
```
curl -X PUT 'http://localhost:8080/rest/users/user' -H 'GATECH_ID:123456789' -H 'Content-Type:app
```

You remember that properties file? Good! We are going to play with it yet again.

For this exploit, you will use the log4j exploit to overwrite the "config.properties" file saved in the root directory of the application. This properties file contains a topic that the application will publish a message to when updateUser call is made (the application is also subscribed to this topic as you can see in the logs).

You will need to trick the application into publishing a message to a different topic with your GATECH_ID as the account number in order to generate a valid flag.

Upon success, you should see your output similar to that below:



Hint: Look through the cs6035.log to find clues about what this other topic could be. *Your flag could be invalid if you have not sent your GATECH_ID appropriately in the published message.*

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