

CS 6035

[Projects](#) / [Log4Shell](#) / Flag 5: PubSub Override

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:

```

at java.lang.Thread.run(Thread.java:745) [?:1.8.0_20]
2024-04-24 04:22:53 [UserService.java:66] INFO Getting ready to publish for userId:
2024-04-24 04:22:53 [UserService.java:69] INFO *****
2024-04-24 04:22:53 [UserService.java:70] INFO ***** Topic read from properties file: *****
2024-04-24 04:22:53 [UserService.java:71] INFO *****
2024-04-24 04:22:53 [UserService.java:73] INFO Publishing to topic:
2024-04-24 04:22:53 [Operation.java:41] INFO
*****Entering exploit.*****
*****
*****
***** Entering exploit.*****
*****
2024-04-24 04:22:53 [Subscriber.java:25] INFO Congratulations! Your flag5 is: 3c1902aaa63b6d185586f22b9f3d5e032590ca819344a34f66ff4b11fd6235
cc
2024-04-24 04:22:53 [Subscriber.java:36] INFO Processed message.
2024-04-24 04:22:53 [SqlStatementLogger.java:128] DEBUG
/* load cs6035.boot.valueobjects.UserVO */ select
    userinfo_.id as id1_1_0_,
    userinfo_.ADMIN_YN as admin_yn2_1_0_,
    userinfo_.USER_ID as user_id3_1_0_,
    userinfo_.USER_NAME as user_nam4_1_0_,
    userinfo_.USER_ROLE as user_rol5_1_0_
from
    USERS userinfo_
where
    userinfo_.id=?
Hibernate:
/* load cs6035.boot.valueobjects.UserVO */ select
    userinfo_.id as id1_1_0_,
    userinfo_.ADMIN_YN as admin_yn2_1_0_,
    userinfo_.USER_ID as user_id3_1_0_,
    userinfo_.USER_NAME as user_nam4_1_0_,
    userinfo_.USER_ROLE as user_rol5_1_0_
from
    USERS userinfo_
where
    userinfo_.id=?
2024-04-24 04:22:53 [BasicBinder.java:64] TRACE binding parameter [1] as [INTEGER] - [1]
2024-04-24 04:22:53 [RequestInterceptor.java:144] INFO Post Handle method is Calling
2024-04-24 04:22:53 [Application.java:62] INFO Refreshing application cache.
2024-04-24 04:22:53 [RequestInterceptor.java:153] INFO Cleaned up application cache.
2024-04-24 04:22:53 [RequestInterceptor.java:156] INFO Request and Response is completed

```

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. *******

Disclaimer: You are responsible for the information on this website. The content is subject to change at any time. © 2024 Georgia Institute of Technology. All rights reserved.