

CS 6035

[Projects](#) / [Log4Shell](#) / Flag 4: Command and Concat

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)

```

/* select
generatedAlias0
from
  user as generatedAlias0
where
  generatedAlias0.userName=userName */ select
  userinfo0.id as id1_2_,
  userinfo0.ADMIN_YN as admin_yn2_2_,
  userinfo0.USER_ID as user_id3_2_,
  userinfo0.USER_NAME as user_name4_2_,
  userinfo0.USER_ROLE as user_role5_2_
from
  USERS userinfo0_
where
  userinfo0.USER_NAME=?
024-11-28 22:57:33 [BasicBinder.java:64] TRACE binding parameter [1] as [VARCHAR] - [EDBOY]
024-11-28 22:57:33 [RequestInterceptor.java:69] INFO Method Type: PUT
024-11-28 22:57:33 [RequestInterceptor.java:70] INFO Request Uri: /rest/users/user
024-11-28 22:57:33 [RequestInterceptor.java:71] INFO Servlet Path: /users/user
024-11-28 22:57:33 [RequestInterceptor.java:72] INFO Location redirect: null
024-11-28 22:57:33 [RequestInterceptor.java:80] INFO *****
024-11-28 22:57:33 [RequestInterceptor.java:81] INFO *****GATECH_ID: 903943752 *****
024-11-28 22:57:33 [RequestInterceptor.java:82] INFO *****
024-11-28 22:57:33 [CS6035Utilities.java:42] INFO Successfully set gatechId.
024-11-28 22:57:33 [Log4jUtilities.java:32] INFO Reset files.
024-11-28 22:57:33 [CS6035Utilities.java:73] INFO Properties file exists. Reading properties file: {customer.service.email=customerservice@gatech.edu, topic.name=user.info, rating=P
}
024-11-28 22:57:33 [RequestInterceptor.java:114] INFO Controller name: cs6035.boot.controller.UserController
024-11-28 22:57:33 [RequestInterceptor.java:115] INFO Method name:updateUser
024-11-28 22:57:33 [UserService.java:48] INFO Entering updateUser
024-11-28 22:57:34 [UserService.java:85] INFO Congratulations! Your flag4 is: 66f9586b11a18ca94f51e89e0f12feef296cf8eb1ac097463f46e044b00d03d6
024-11-28 22:57:34 [UserService.java:66] INFO Getting ready to publish for userId: 2134
024-11-28 22:57:34 [UserService.java:69] INFO *****
024-11-28 22:57:34 [UserService.java:70] INFO ***** Topic read from properties file: user.info *****
024-11-28 22:57:34 [UserService.java:71] INFO *****
024-11-28 22:57:34 [UserService.java:73] INFO Publishing to topic: user.info

```

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. *******

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.