CS 6035

Projects / Log4Shell / Flag 1: Environment Echo

Flag 1: Environment Echo (5 pts)

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

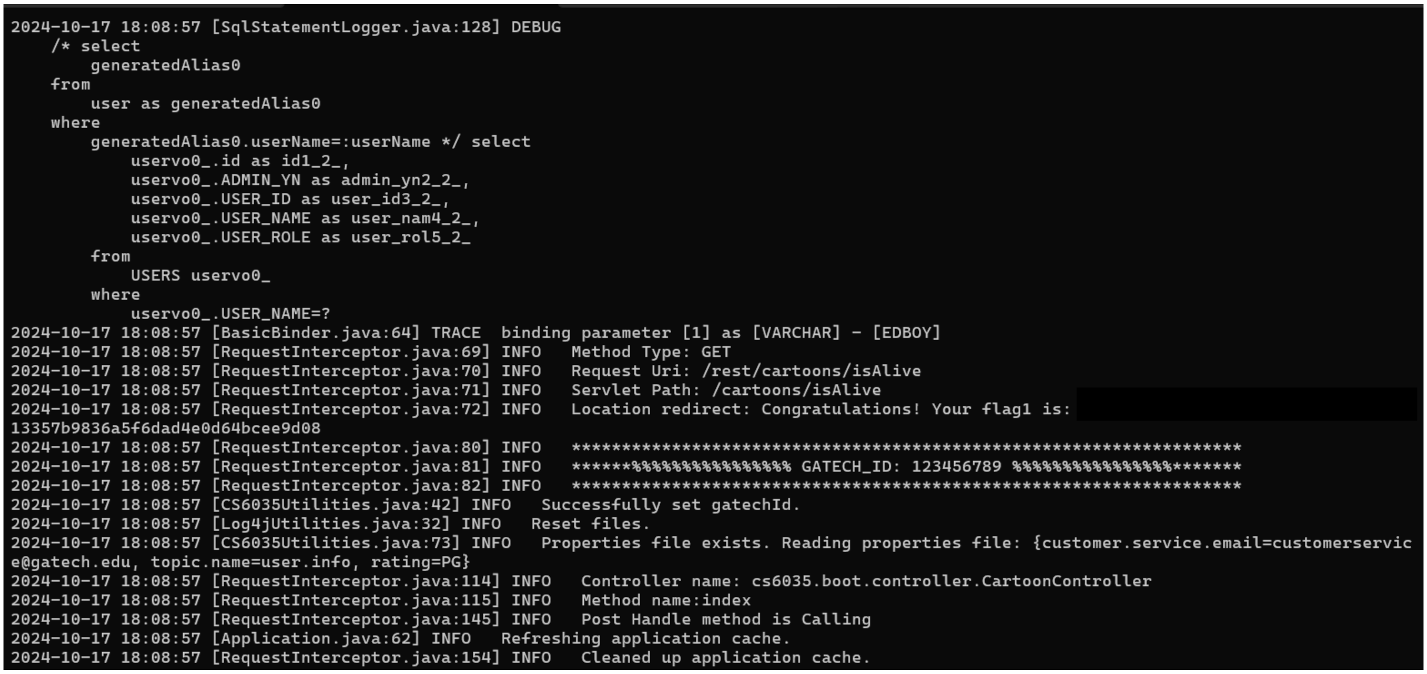
If you haven't already, run the start script in the home directory of log4j user, start the container with the start script:

```
./StartContainer.sh
```

The endpoint for this exploit can be called and inspected via:

```
curl 'http://localhost:8080/rest/cartoons/isAlive' -H 'GATECH_ID:123456789' -H 'Accept:applicatio
```

Now that you have seen how to check environment variables, run a lookup for `ADMIN_PASSWORD` which stores your flag for this exercise. If successful, you should see the below output:



```
2024-10-17 18:08:57 [SqlStatementLogger.java:128] DEBUG
    /* select
        generatedAlias0
    from
        user as generatedAlias0
    where
        generatedAlias0.userName=:userName */ select
            uservo0_.id as id1_2_,
            uservo0_.ADMIN_YN as admin_yn2_2_,
            uservo0_.USER_ID as user_id3_2_,
            uservo0_.USER_NAME as user_nam4_2_,
            uservo0_.USER_ROLE as user_rol5_2_
        from
            USERS uservo0_
        where
            uservo0_.USER_NAME=?
2024-10-17 18:08:57 [BasicBinder.java:64] TRACE  binding parameter [1] as [VARCHAR] - [EDBOY]
2024-10-17 18:08:57 [RequestInterceptor.java:69] INFO   Method Type: GET
2024-10-17 18:08:57 [RequestInterceptor.java:70] INFO   Request Uri: /rest/cartoons/isAlive
2024-10-17 18:08:57 [RequestInterceptor.java:71] INFO   Servlet Path: /cartoons/isAlive
2024-10-17 18:08:57 [RequestInterceptor.java:72] INFO   Location redirect: Congratulations! Your flag1 is: [redacted]
13357b9836a5f6dad4e0d64bcee9d08
2024-10-17 18:08:57 [RequestInterceptor.java:80] INFO   ******************************************************************
2024-10-17 18:08:57 [RequestInterceptor.java:81] INFO   ******%%%%%%%%%%%%%%%% GATECH_ID: 123456789 %%%%%%%%%%%%%%%*******
2024-10-17 18:08:57 [RequestInterceptor.java:82] INFO   ******************************************************************
2024-10-17 18:08:57 [CS6035Utilities.java:42] INFO   Successfully set gatechId.
2024-10-17 18:08:57 [Log4jUtilities.java:32] INFO   Reset files.
2024-10-17 18:08:57 [CS6035Utilities.java:73] INFO   Properties file exists. Reading properties file: {customer.service.email=customerservic
e@gatech.edu, topic.name=user.info, rating=PG}
2024-10-17 18:08:57 [RequestInterceptor.java:114] INFO   Controller name: cs6035.boot.controller.CartoonController
2024-10-17 18:08:57 [RequestInterceptor.java:115] INFO   Method name:index
2024-10-17 18:08:57 [RequestInterceptor.java:145] INFO   Post Handle method is Calling
2024-10-17 18:08:57 [Application.java:62] INFO   Refreshing application cache.
2024-10-17 18:08:57 [RequestInterceptor.java:154] INFO   Cleaned up application cache.
```

Add this flag (Congratulations! Your flag1 is: ____) to your project_log4shell.json file.

NOTE: You do not need to use Java code, ldap, python server, etc to get this flag.

Hint: `Accept` is not the only valid HTTP Header. Location, location, location

Disclaimer: You are responsible for the information on this website. The content is subject to change at any time.