Frequently Asked Question(s) (FAQ)

Start With:

- General Project Introduction *This is a general overview. Some details may change each semester (i.e., login credentials)*
- Important Reference Materials

Note: *To ensure that the autograder accurately grades your submission, you should create/update your .json file in a text editor on the VM and submit from the VM. Do not use a word document program like LibreOffice or Word. The submission must be proper json format for the autograder to give credit.*

VM Questions

Q) Do I need to use the provided VM for this project

- A) Yes. You won't be able to complete the project without using it, as the environment is set up specifically to handle this project.

Q) I am re-taking this course. Can I use the VM that I downloaded from an earlier semester?

- A) NO! Using a VM from earlier semesters is not permitted and may result in a 100% penalty. Please download the VM from the link present in the writeup for the current semester.

Q) I have an M1-based Mac, can I run the VM?

- A) Unfortunately, we do not have a version of this project for M1-based Mac's

Q) The VM Password is:

- A) Credentials for the vm are on the assignment page for Log4Shell in Canvas

Q) Should I update the VM?

- A) No DON'T update the virtual machine! You can allocate more resources via the Virtual Box (or other platform) configurations depending on your local host but you shouldn't need to.

Q) My Virtual Machine is slow or not turning on, what should I do?

- A) Feel free to increase the amount of RAM in the Virtual Machine by a little. You may also have to disable 3D acceleration within the Virtual Machine

Q) General Ambiguous errors with importing: "Error When Importing Project E_INVALIDARG (0x80070057)"

- A) This is normally due to insufficient space on the hard drive or File System mismatch (file system on Windows needs to be NTFS with VirtualBox).
- Make sure you also have permission to be allocating storage. If you are on a work laptop that has secured partitions, you may not be able to import the VM.
- You can also try following these steps: VirtualBox : Failed to import appliance

Q) VirtualBox is giving me weird "Kernel Driver not installed" errors (Intel Mac).

- A) This is likely due to permissions settings. See Driver not installed

Q) I have restarted the VM correctly and am still getting a blank flag. What else can I try?

- A) When rebooting, we have found you can't "switch user" and then log into the proper username. You need to "log out" of the wrong account, then log in as the project user.

Common troubleshooting steps for VirtualBox:.

- Enabling/disabling 3d acceleration, giving more video memory
- Increasing cpus and/or ram (or if you don't have enough, maybe lowering those)
- Enabling/disabling PAX/VT-X in the vm system settings

Submission and Gradescope

Q) What is the format and name of the file I need to submit?

- A) The submission file (only file to be submitted to Gradescope) is json format. There is a template that can be copied in the Submission Page page. You only need to fill in the values for each flag.

Q) Do I need to submit to both Gradescope and Canvas?

- A) For this project, you only need to submit to Gradescope.

Q) How many times can I submit to Gradescope?

- A) You can submit as many times as you want until the project closes in Gradescope.

Q) Once I submit to Gradescope, when will I get my grade?

- A) Grades will be released after the due date + any extensions have expired. Gradescope submissions will, however, give immediate feedback on passing our autograder tests. There are no hidden tests so you can be confident in your score (barring any issues with academic honesty).

Q) Do I get partial credit for passing some tasks?

- A) Yes, See rubric in writeup for grading scale

Q) I am getting a flag in the VM but Gradescope still shows the answer as incorrect.

- A) Make sure you are using your GTID (9 digit numeric student ID number) for each flag.

Q) Do I need to do all flags in sequence?

- A) No, but encouraged. You can do these in any order you wish. However, each flag builds on the previous one so concepts you learn in a previous flag will be used in a later one. IF YOU GET STUCK ON SOMETHING TRY ANOTHER FLAG AND COME BACK TO IT!

Q) Do I need to run all the setup steps again if I restart the VM?

- A) Yes, you need to rerun all setup steps and start the container when restarting the VM.

Q) Can we submit late?

- A) No. Please refer to the syllabus.

Q) When is the project due?

- A) Please refer to the Schedule.

Flag Task Hints and Questions

Q) I don’t know where to start! I’m having trouble understanding what to do.

- A) Start at the beginning of the instructions, watch the linked tutorial video, read the resources linked. While there is no particular order required for completing these tasks, the first task is helpful as an introduction to the tools and process. Follow the steps and experiment a lot. Find online resources of other examples of this exploit and follow them step for step.

Q) What does the web server on port 8080 represent?

- A) It's a REST API that retrieves information for a frontend client. It's owned by the victim and runs on Apache Tomcat in a Docker container.

Q) What are the different servers involved in this project?

- A) There are three main servers:
  - Vulnerable application server (REST API on port 8080)
  - LDAP server
  - Local Python server

Q) I'm stuck on the intro flag. Any hints?

- A) For the intro flag:
  - Look at the screenshots provided in the intro flag instructions
  - Use the Apache Log4j Lookups page to understand the syntax for accessing environment variables
  - Focus on echoing the Java version as mentioned in the instructions

Q) How do I transition from solving the intro flag to solving Flag 1?

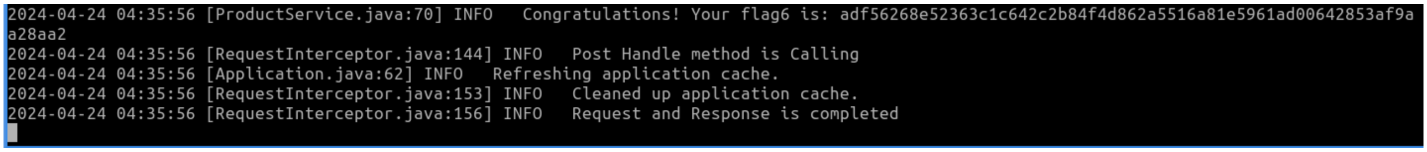
- A) Once you've solved the intro flag:
  - Use the same basic approach but focus on the ADMIN_PASSWORD environment variable
  - Modify your payload to target this specific variable
  - Remember that Flag 1 is called "Environment Echo" - this is a hint about which lookup to use

Q) I do not see the log4shell folder in my VM Desktop?

- A) Make sure you are logged in to the user log4j. If you are on the incorrect user, logout by clicking the blue Lubuntu logo in the bottom left -> Leave -> Logout.

Q) How do I know if I got the flag?

- A) You will see an output message with your flag displayed when the exploit is successful. Copy this flag into the appropriate key-value pair in the json file.



```
2024-04-24 04:35:56 [ProductService.java:70] INFO   Congratulations! Your flag6 is: adf56268e52363c1c642c2b84f4d862a5516a81e5961ad00642853af9a
a28aa2
2024-04-24 04:35:56 [RequestInterceptor.java:144] INFO   Post Handle method is Calling
2024-04-24 04:35:56 [Application.java:62] INFO   Refreshing application cache.
2024-04-24 04:35:56 [RequestInterceptor.java:153] INFO   Cleaned up application cache.
2024-04-24 04:35:56 [RequestInterceptor.java:156] INFO   Request and Response is completed
```

Q) Why does the message say that I got the flag but the flag is blank?

- A) Run the scripts to stop the container and start it again. Refer to the Setup steps in the instructions for this.

Q) I am not seeing my System.out.println messages. Why are they not printing?

- A) You need to tail the `console.log` file not the `cs6035.log` file.

Q) Do I need to import anything into the Java class?

- A) Yes, you will likely need to import some packages from the Java standard library. Only Java standard library imports are needed for this project. If you find yourself wanting to use a 3rd party .jar, you are over complicating your solution and we will not help you compile your code.

Q) I am having trouble with the java class. Do I use a main method? How do I call it?

- A) No, you will not be using a main method. Only write your code in the areas specified with the "// TODO: your exploit code should go here" comment. Look into what a "static block" is, and why it is important/needed for this exploit to work.

Q) Do I need to implement an interface such as serializable?

- A) No. Don't overthink it. The code for each of the flag exploits will be different but none should need more than a few lines of code. You are not expected to be creating classes or interfaces or any new files.

Q) I echoed the ADMIN_PASSWORD and got a huge output, is this correct?

- A) No, it should match the screenshots output. You need to echo the ADMIN_PASSWORD env variable stored on the application server NOT the vm. This should be done through curl command.

Q) I uncommented and am using the provided logger in the Exploit class. But when I run the exploit I get an endless loop of logging?

- A) This is expected. There are several recalls happening when you use the logger that create this infinite loop. To stop this, just kill the process for the LDAP server (python command). It may still be useful to print test statements as you code your exploit but be aware that this is normal. Comment out the log statements to exploit without the loop. The logger is just for debugging. You should comment log statements out when you run to get your flag.

Q) I am not able to find where ADMIN_PASSWORD is stored. Do you have any suggestions?

- A) The ADMIN_PASSWORD is an environment variable. You should look up how to echo environment variables. This will be very similar to the java version lookup you performed in the intro.

Q) I am really struggling with Flag 2. Can you provide any help?

- A) Although Flag 2 is not the hardest flag, it is the hardest to get started on and get over the learning curve. Once you complete Flag 2, a lot of the hard parts to understand of the following 4 flags will be covered. We strongly suggest putting the project down, and go to the linked resources and follow those guides and really take the time to understand the exploit, how it is possible, how it is accomplished, and how all the parts used work together to achieve the task. Once you understand all this, you should be equipped to do Flag 2 and the later flags.

Q) What should I modify in the Exploit.java file for Flag 2?

- A) You need to add code to the Exploit.java file that will allow you to gain a reverse shell on the target server. The exact code is part of the challenge.

Q) Which ports should I use for the different components in Flag 2?

- A) You can use the default ports specified in the setup instructions. For the netcat listener, port 9999 is commonly used.

Q) Why am I not seeing any output in my netcat listener for Flag 2?

- A) If you're not seeing a "Connection received" message, it's likely that either your curl command is incorrect or your Java code in Exploit.java is not properly creating a reverse shell.

Q) What if I can see my exploit executing but can't run commands like 'whoami'?

- A) This likely means your reverse shell command in the Java code is not correctly implemented. Review your code!

Q) What should I see in the different terminal windows when the exploit is successful?

- A) You should see:
  - LDAP server showing a redirect to your Exploit.class
  - Python server showing a 200 status code for GET /Exploit.class
  - "Entering Exploit" message in console.log (which is the result of System.out.println in your Exploit.class)
  - "Connection received" message in the netcat listener (only for Flag 2)

Q) Do I need an in-depth understanding of Java to complete this project?

- A) No, you should be able to complete this project with no Java background and have plenty of time to learn/research the requirements of java. You will need a basic/moderate understanding of networking though.

Q) I think my code is right but I am not getting any output. How do I tell if my code executes or not?

- A) You can use the logging framework in the class file to output useful commands like "Starting the exploit", "Exploit code ran", or anything else to help you track control execution. BEWARE USING THE LOGGER COULD RESULT IN ENDLESS LOOPING FROM THE SERVER LOOKUPS. Use CTRL + C in the LDAP terminal to stop it.

Q) My LDAP is being called but returning "Foo". Why is that?

- A) This usually means the server is not getting a response from the python server or you sent a bad request to it from the curl. Ensure your python server is receiving the request. If not, the issue lies there. If it is returning 404, make sure the requested file from the LDAP's name matches your .class file. For simplicity, please use Exploit.class or Exploit2.class etc if multiple are needed.

Q) Is it normal for my Python HTTP server to receive multiple requests for one curl request?

- A) Yes, it's not unusual due to nested logging. The number of requests doesn't interfere with getting the flags.

Q) Why are my flag hashes the same when I use my GATECH ID or the generic "123456789"?

- A) The flag will be the same for Flag 1. For the rest of the flags, it should be different.

Q) What should I do if 'tail -f console.log' stops updating?

- A) This might be due to the VM or curl causing an endless loop. Try restarting the VM or the container.

Q) Do I need to change the URL for each flag?

- A) Each flag has its specific URL(s) provided in the writeup. You only need to modify the attack vector for each flag.

Q) I'm getting a 400 Bad Request error. What does this mean?

- A) This usually indicates that your curl command syntax is incorrect. Double-check your command, especially the formatting of the JNDI lookup string.

Q) Should I be calling the LDAP server directly from my curl command?

- A) No, your curl command should be sent to the vulnerable application (localhost:8080). The application should then make the LDAP call as part of the exploit.

Q) Can I run 2 LDAP servers?

- A) Yes, there could be some flags where this is required.

Q) How do I run another LDAP? I get an error about port 1389 in use.

- A) You can specify a port using an optional parameter after the LDAP command. Refer to the write up on how to do this.

Q) Do I need to run a python server for each Exploit.class file?

- A) No, the server can "serve" any file you have stored in the directory you are running it in. You just need to update the curl and the LDAP command to request the specific file you wish to send to the vulnerable application.

Q) I am getting "/rest/error and Controller name: org.springframework.boot.autoconfigure.web.servlet.error.BasicErrorController. How do I fix this error?

- A) You don't, this is expected and is a built in feature of Springboot. Scroll further up in the logs to see the actual REST api call you made.

Q) How can I debug my exploit if it's not working?

- A) Add print statements to your Java code, check all terminal outputs (LDAP, Python server, netcat (for flag 2)), and review the console.log file. Ensure your curl command is correct and you're using the right ports.

Q) Any idea how to fix this:

```
Resolved [org.springframework.web.HttpMediaTypeNotAcceptableException: Could not parse 'Accept' h
```

- A) You don't/can't. This is expected as you are not sending a valid mime type when you do the environment echo.

Q) What is a mime type?

- A) You do not need to know this to complete this project. However, here is some info if you're curious

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