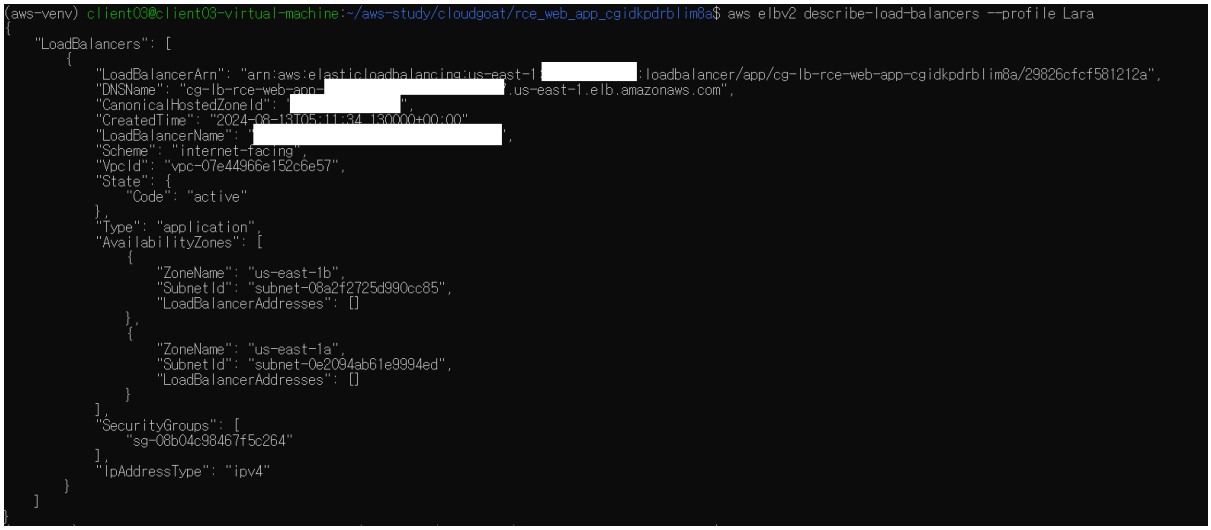
Cloudgoat – RCE_WEB_APP Analysis

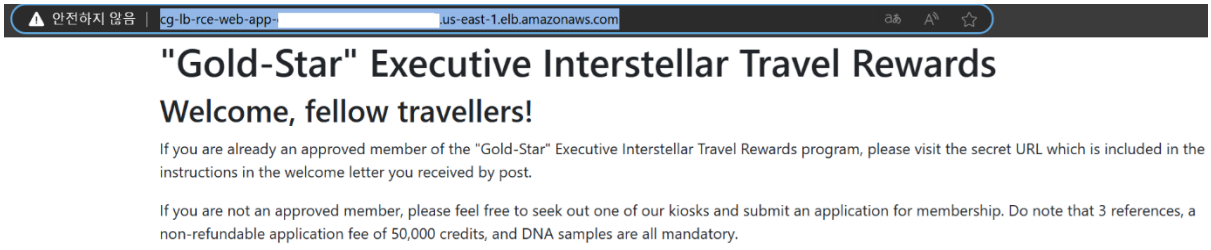
Name: LEE WON HUI

DATE: 2024/08/13

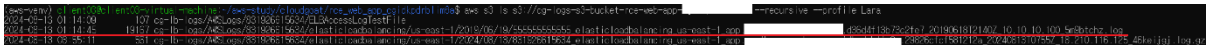
This document assumes that you have executed ./cloudgoat.py create rce_web_app.



After executing the command shown in the image above, you can find a DNSName written, which is the target webpage for the upcoming practice.

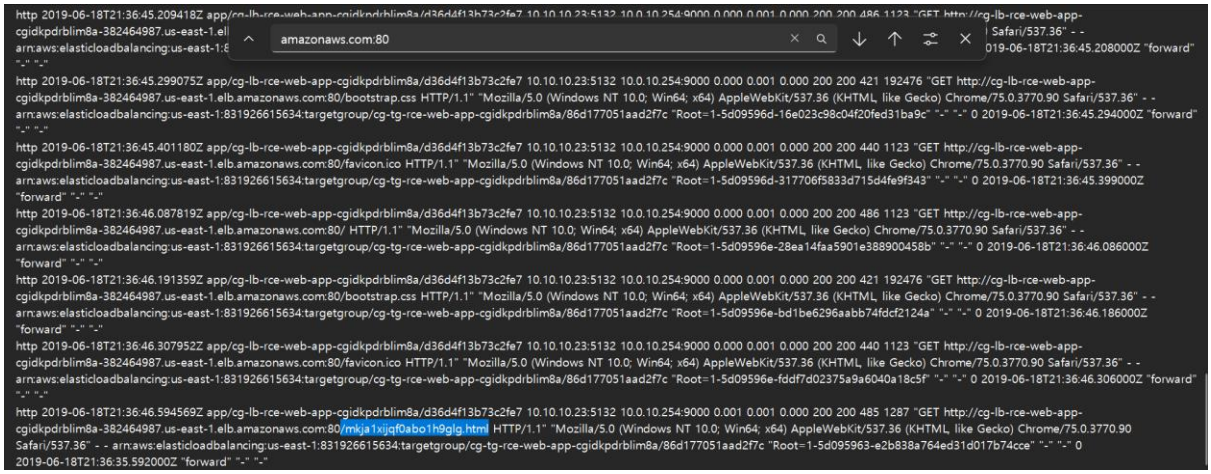


When you access the webpage, you can see a webpage called Gold-Star appears.

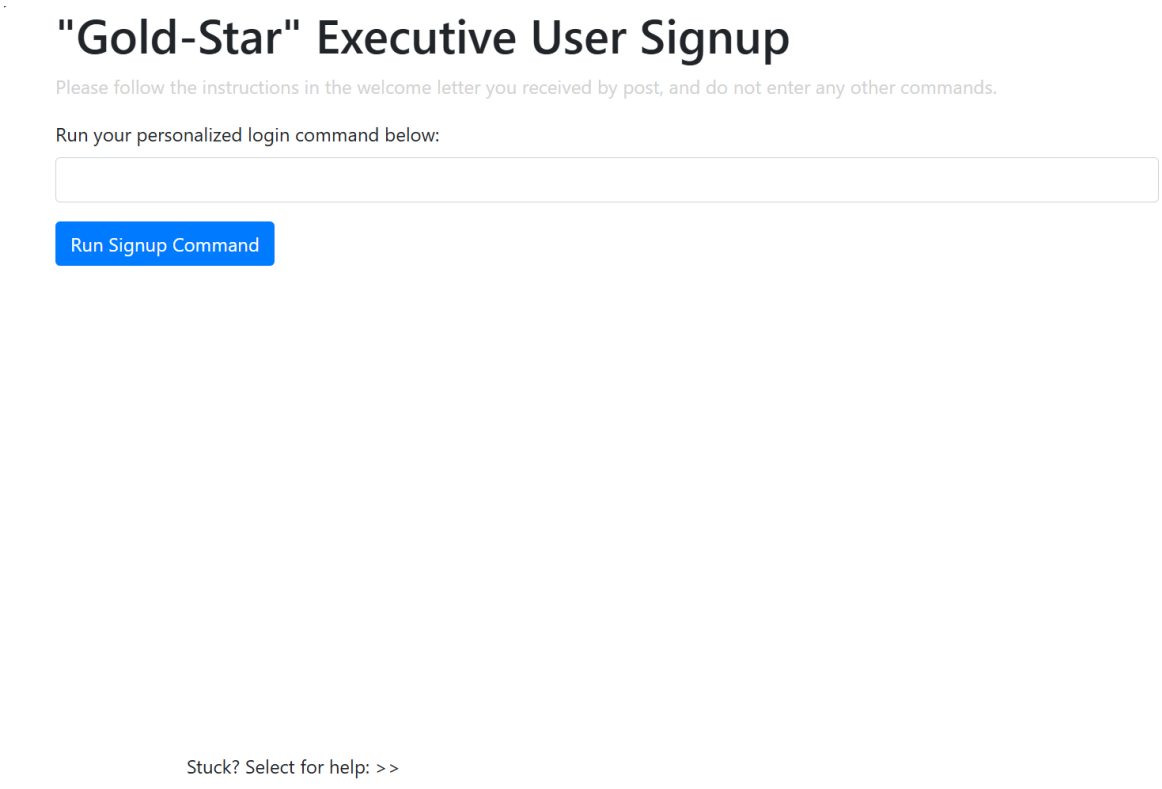


Next, I found a directory related to log file collection and identified the log file within it.

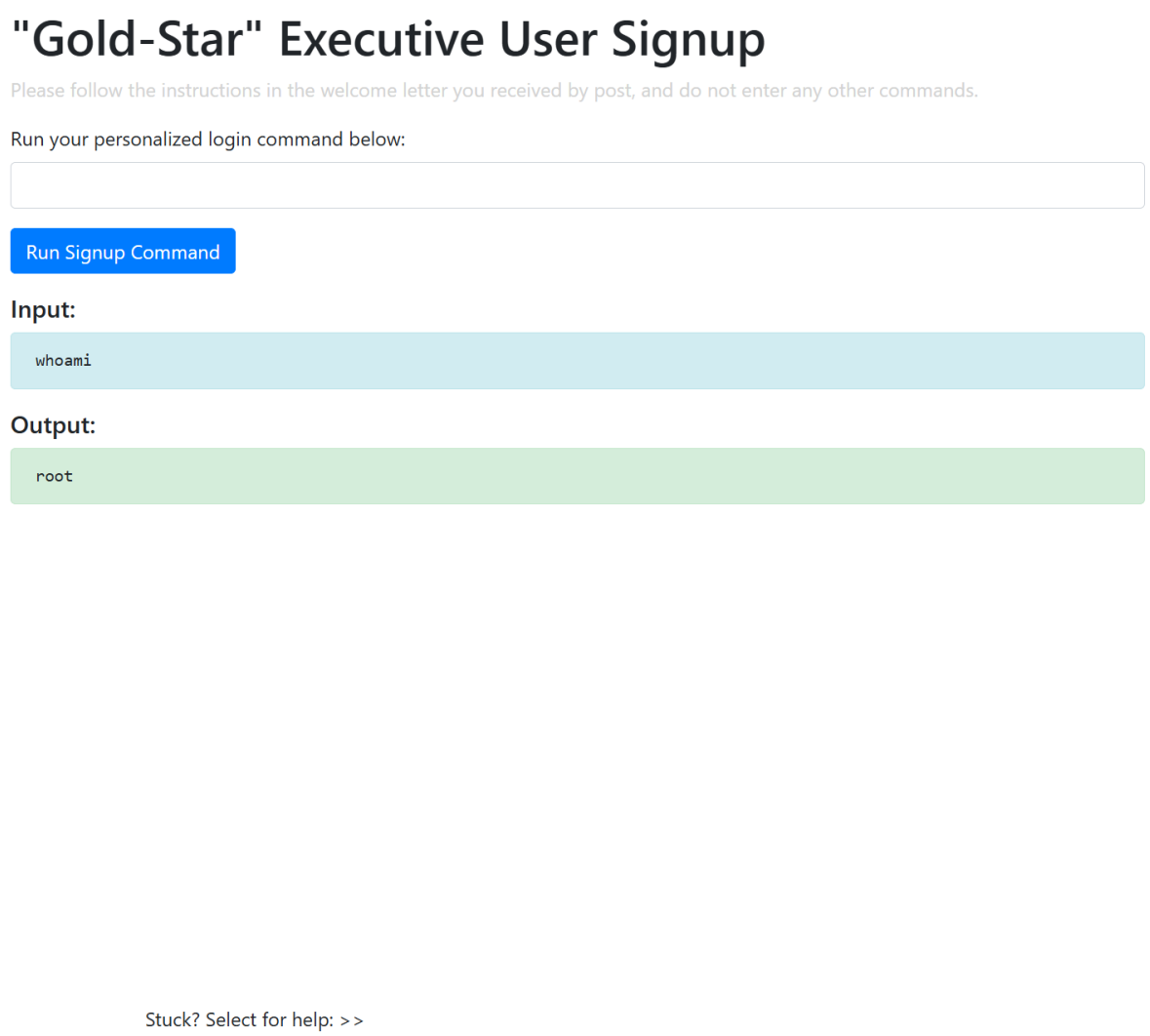
I copied the log file to local.



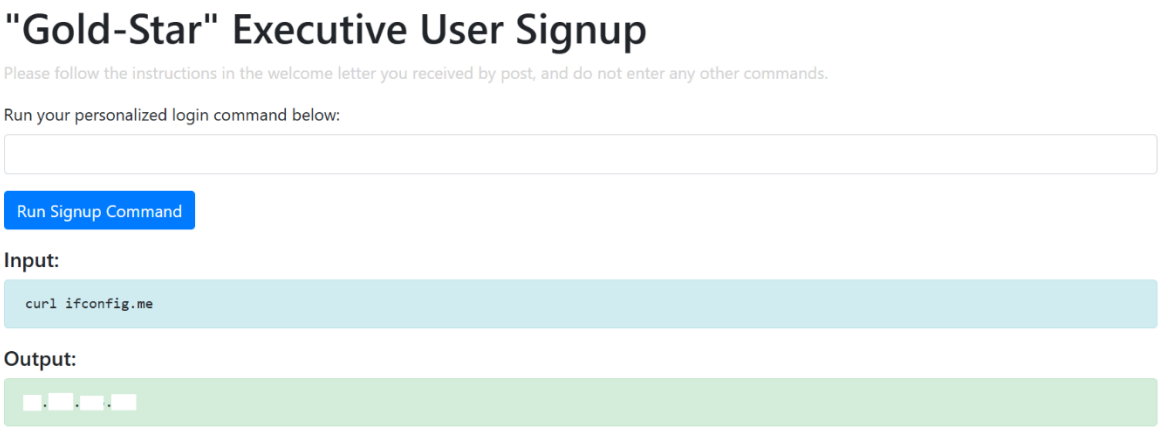
Near the end of the log file, I found an unusual link file.



When accessing that link, I found a webpage related to exploiting web vulnerabilities :D

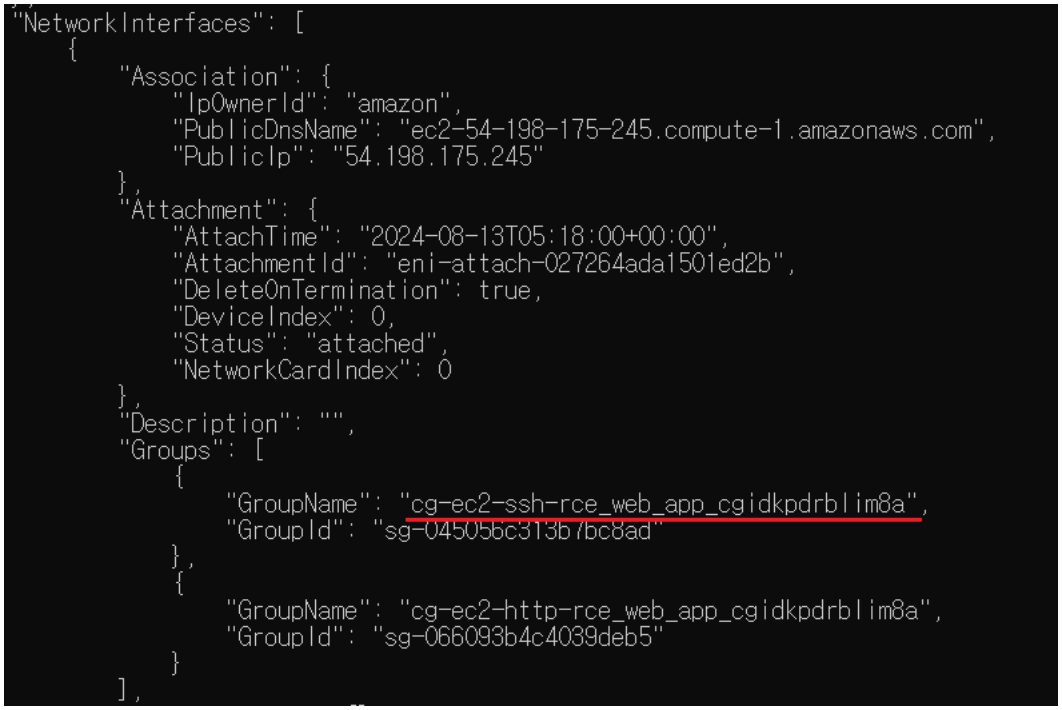


I entered the whoami command to check which user permissions it's currently running under, and surprisingly, I found out it's currently root privileges.

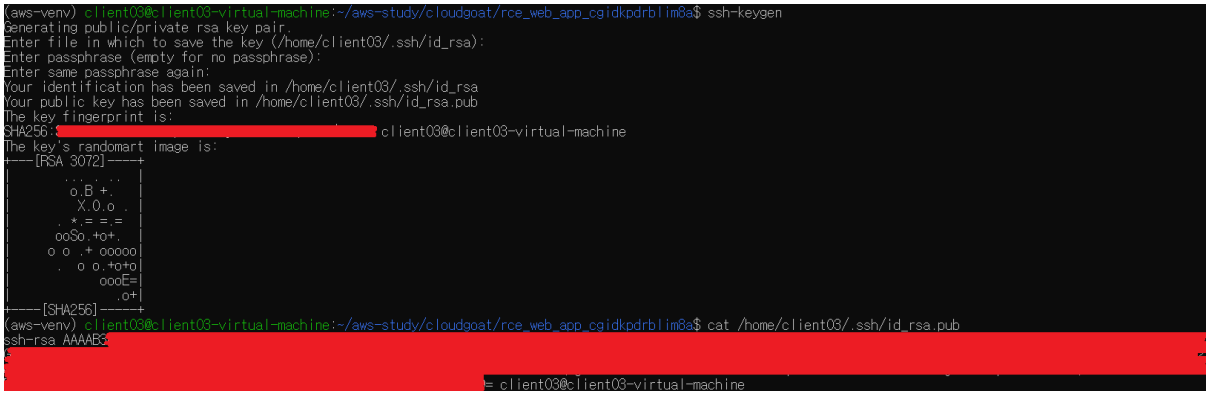


Also, I was curious about the public IP address of the current cloud and found it out.

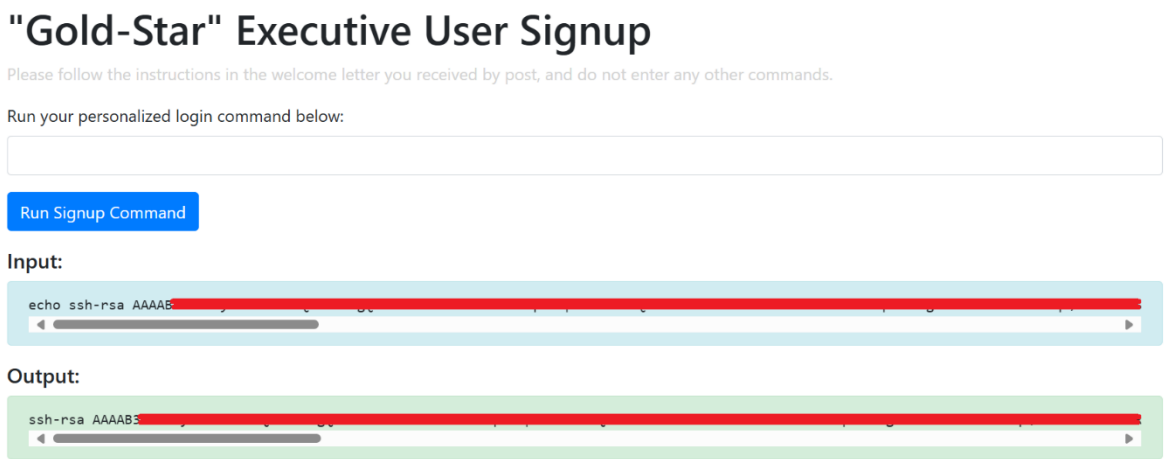
The reason for finding out the public IP address is because when performing the above command,



As shown in the image above, I discovered that ssh can also be used.



Therefore, I generated an ssh key locally,



And inserted the ssh public key into the vulnerable webpage I found earlier.

This concludes the report on cloudgoat's rce_web_app. Thank you for reading.