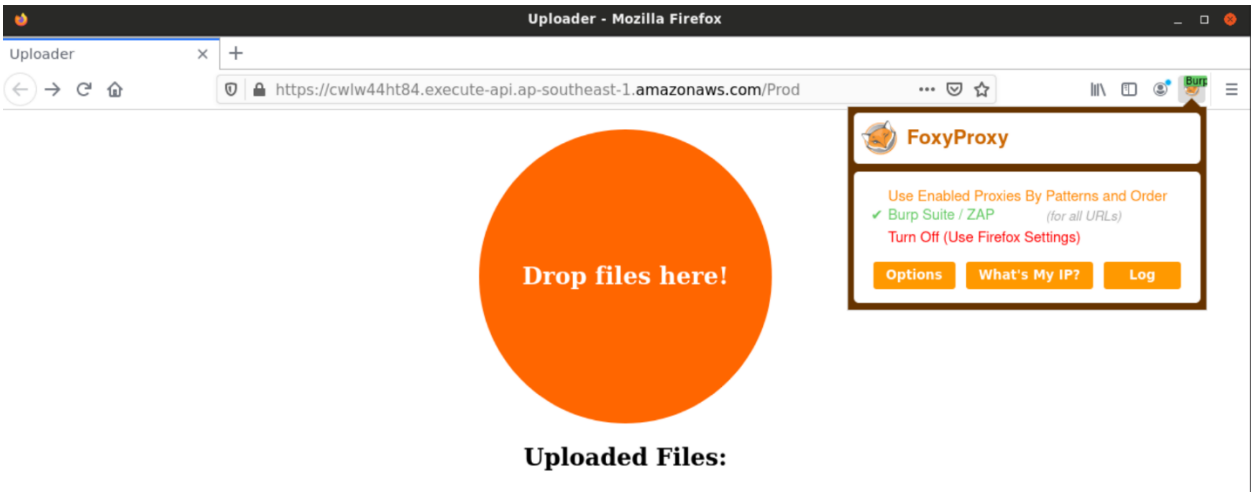
Start up the lab and the kali linux instance.

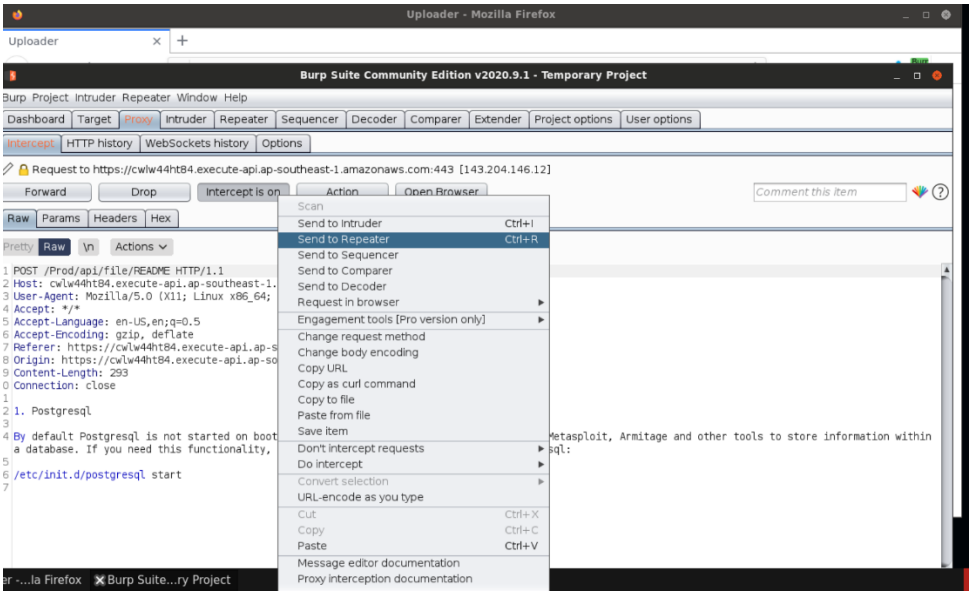
Use the given link in the lab to go to the vulnerable file upload page.

Switch FoxyProxy to the Burp suite option so you can intercept and modify the requests.

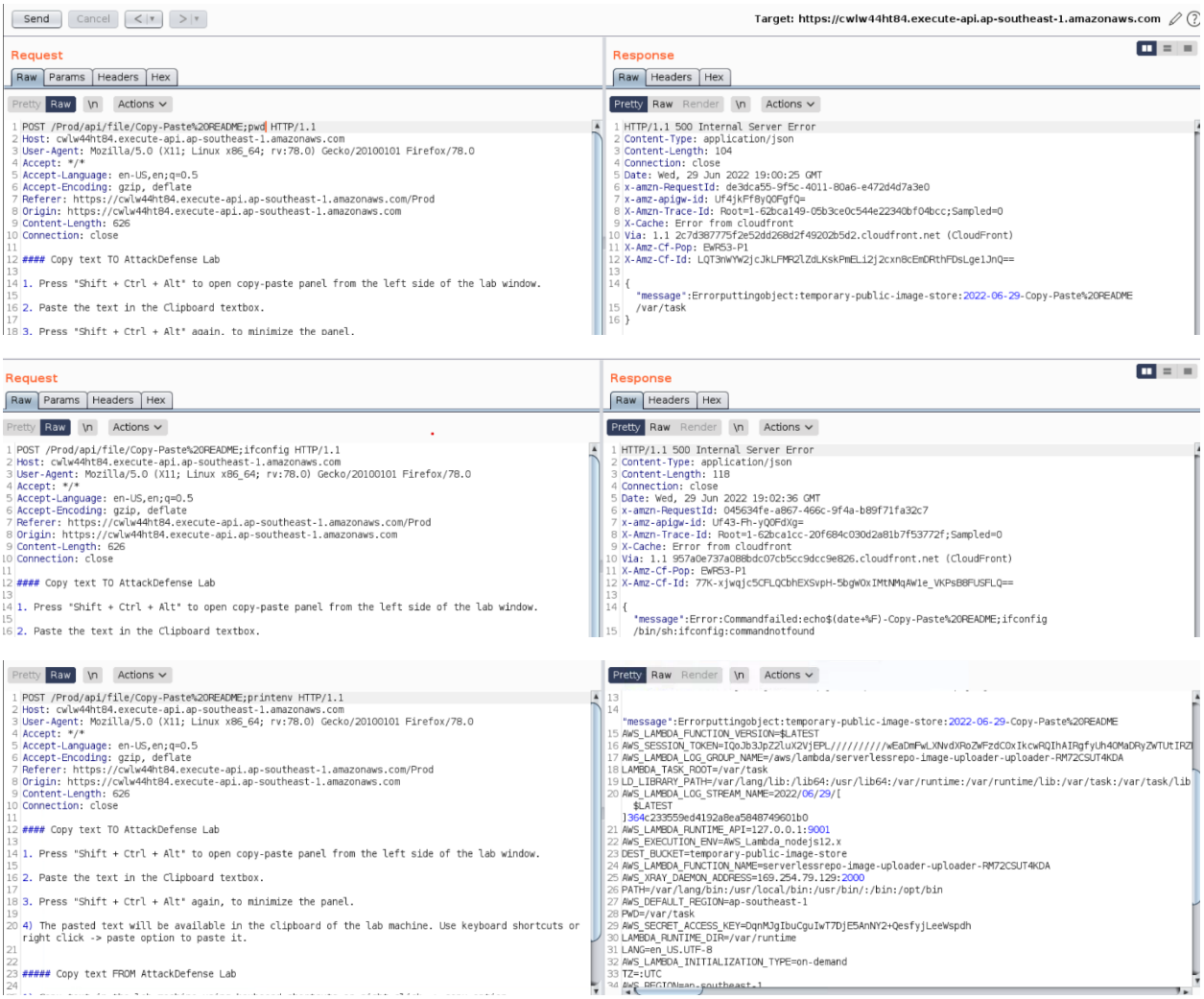



Attempt to upload a file that is less than 4 mb (error was received when I tried to drop an application on the file upload page)

Intercept the request and send it to the repeater.



From here, append a ';' to the end of the post request and see if you can run simple commands.




Tested:

--dir, no response

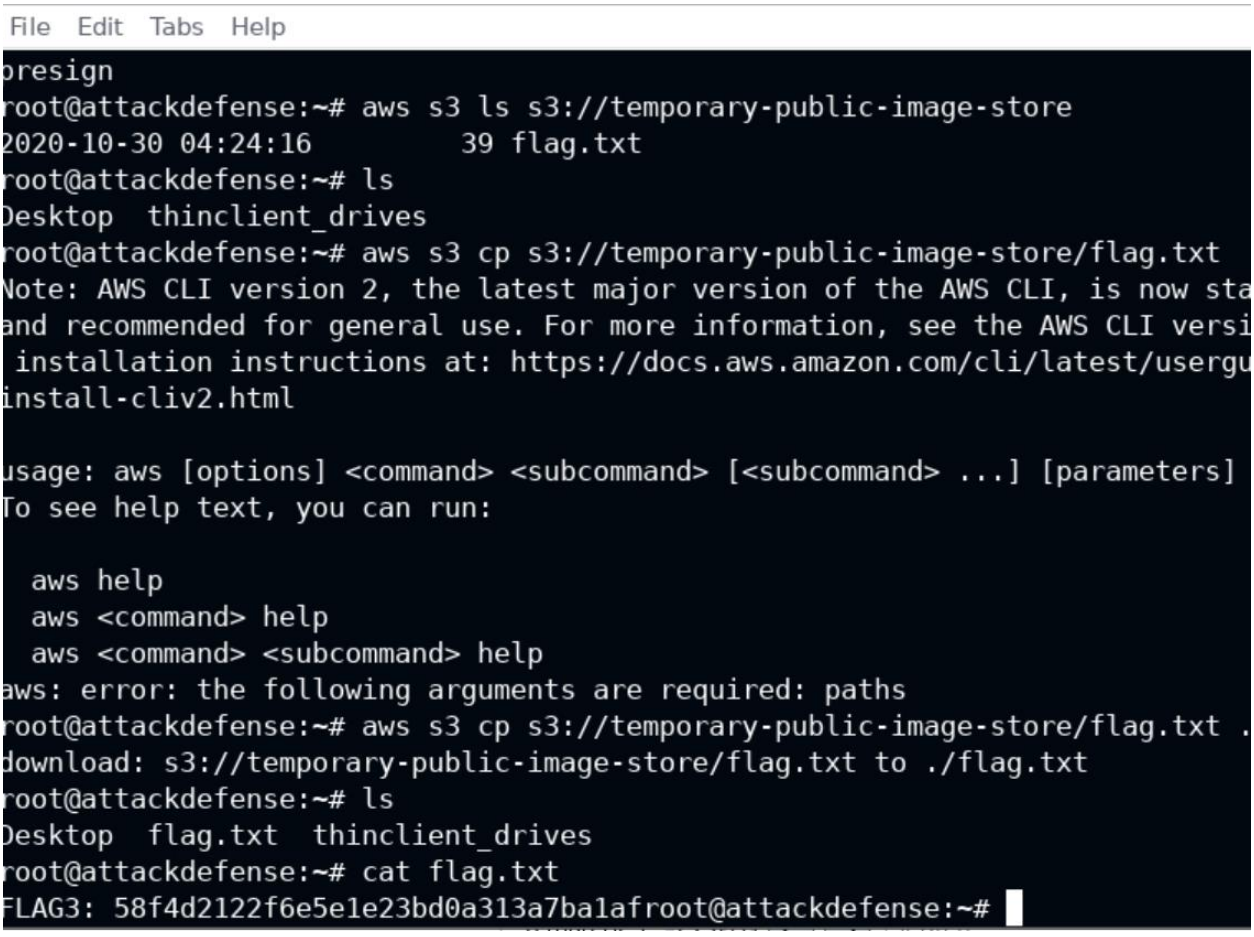
--ifconfig, shows a response 'command not found' << well hey at least I got a response and it's looking like we're dealing with a linux/unix based system.

--printenv, shows ALL of the environmental variables

Now that I have the variables, I can see all of the information needed to access the AWS account connected to this computer/server.

Attempted access the S3 bucket directly using the DEST_BUCKET variable and AWS documentation for S3 bucket endpoints. DENIED


Attempt to access bucket through terminal with keys: SUCCESS!



Lessons learned:

- These hands on labs are going to be seriously addicting xD

- Poke around and see if you can make responses in your favor for more information or access.

- Documentation is key for being able to find out and understand how information/resources are accessed. << AWS website for S3 buckets, hosted videos for using burpsuite, etc.

- I'm thinking with enough hands on practice, everything you do as a pentester becomes second nature. What is this, what does it do, what documentation can I find about how it works, etc.