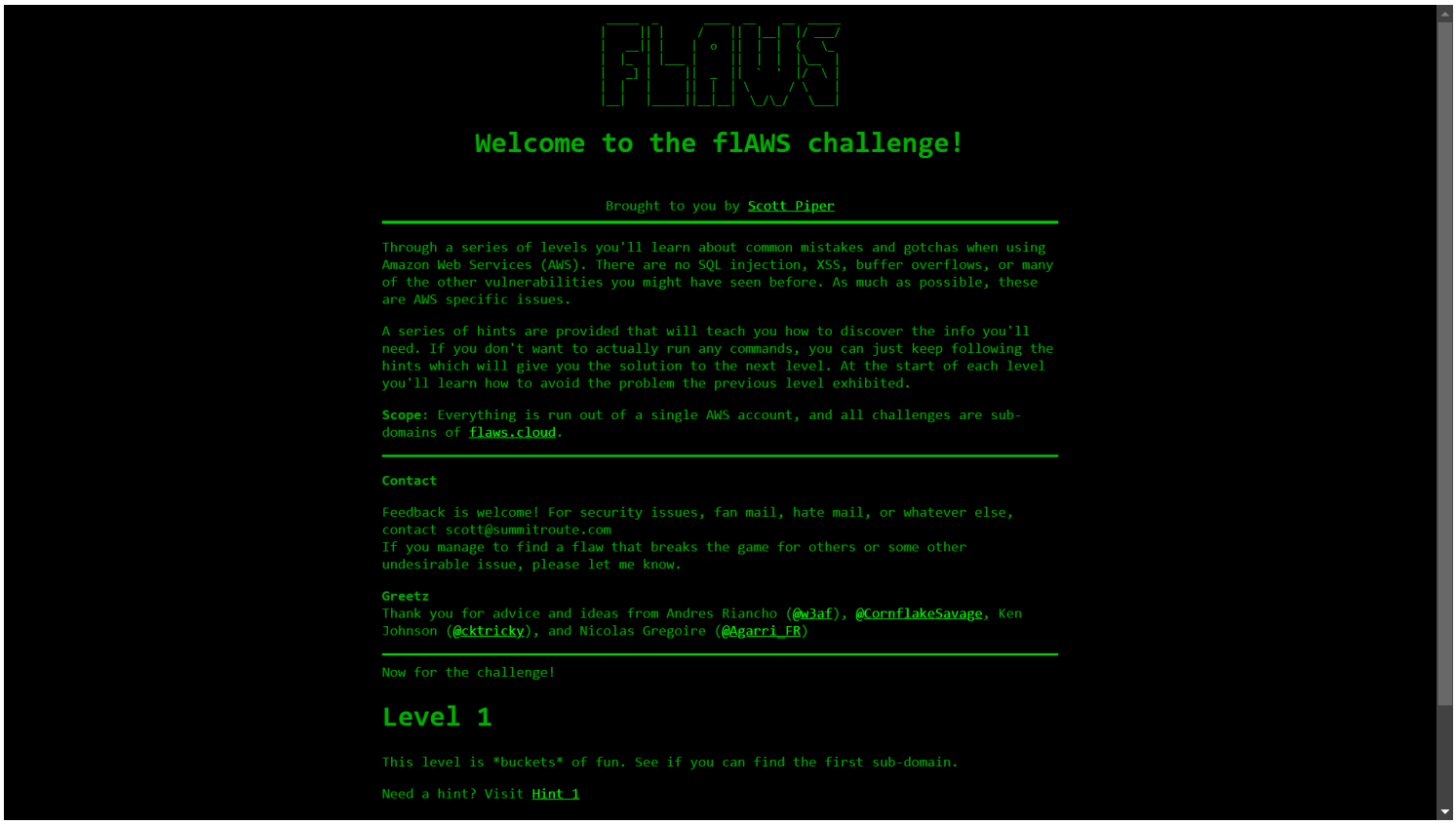
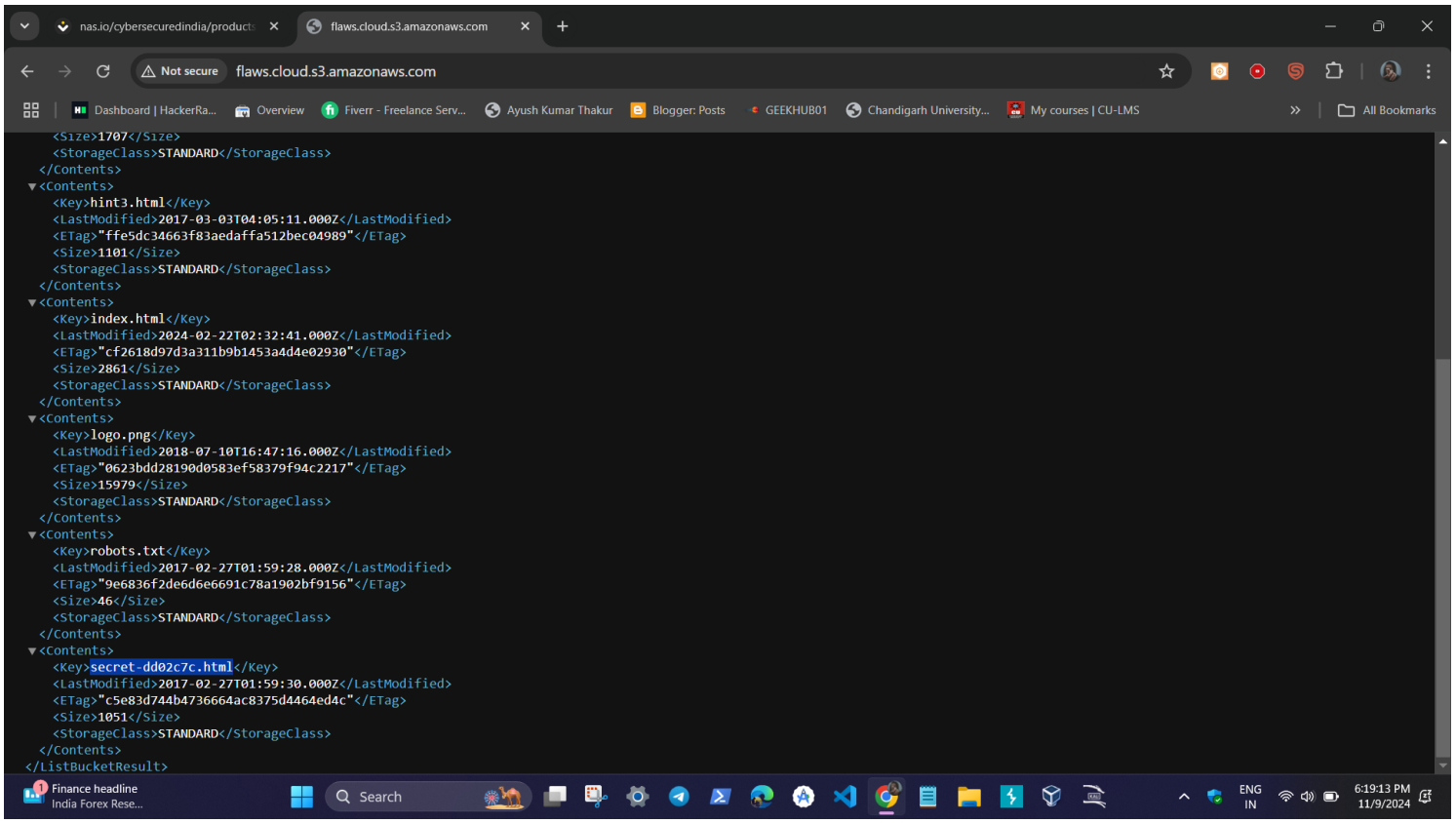
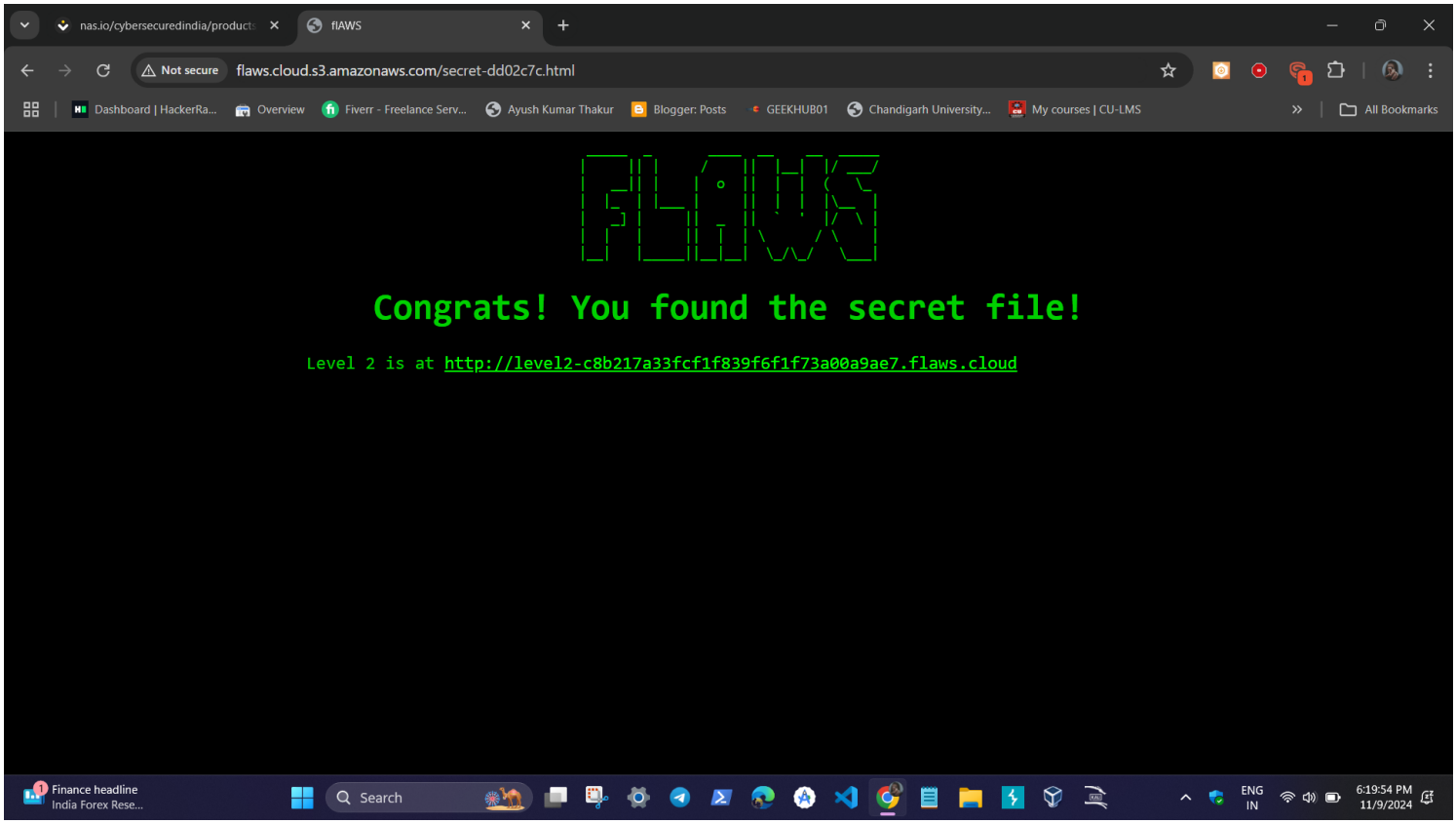
The flAWS challenge!

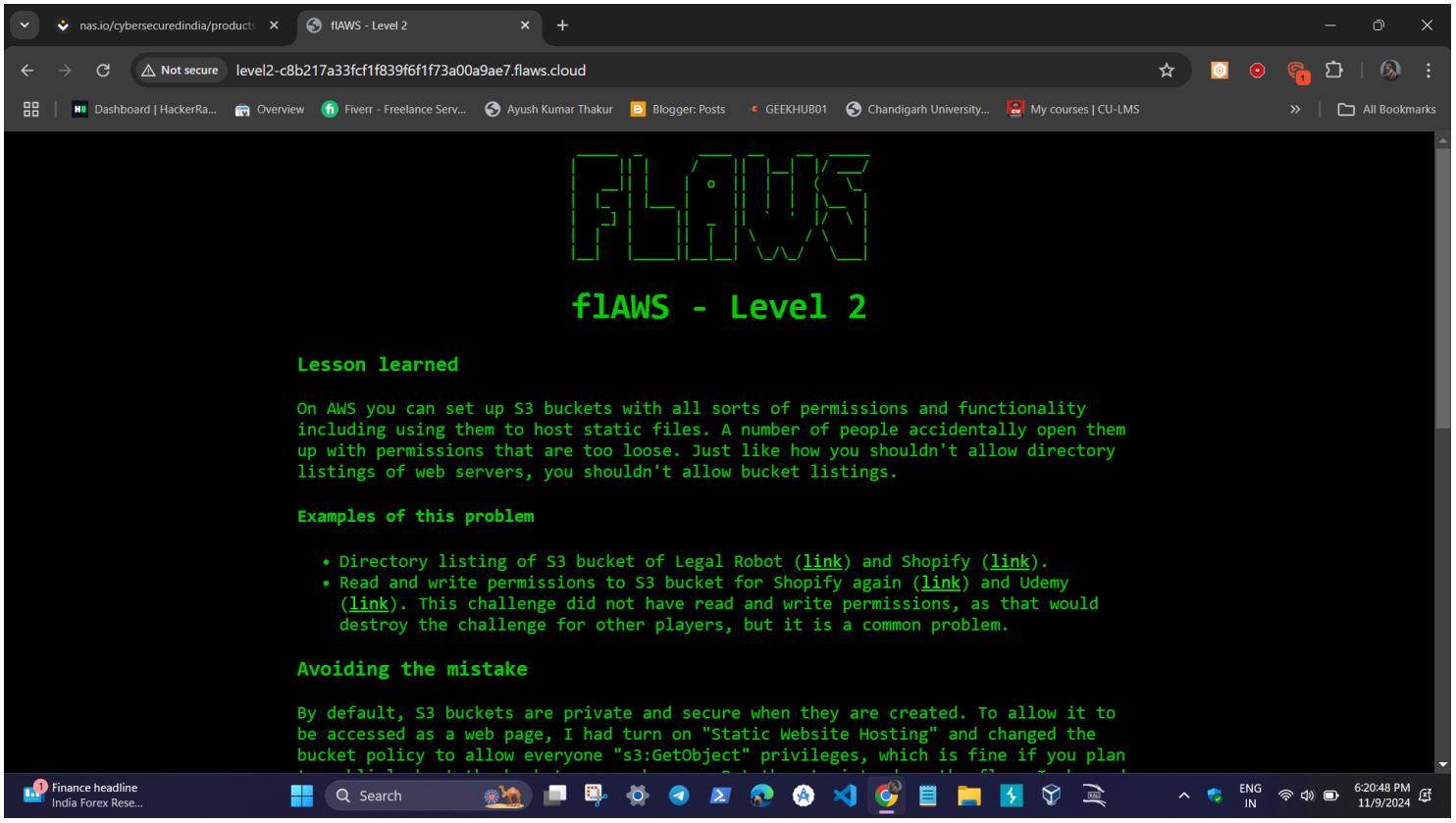
Level-1






nas.io/cybersecuredindia/product
flAWS
Not secure
flaws.cloud.s3.amazonaws.com/secret-dd02c7c.html
Dashboard | HackerRa...
Overview
Fiverr - Freelance Serv...
Ayush Kumar Thakur
Blogger: Posts
GEEKHUB01
Chandigarh University...
My courses | CU-LMS
All Bookmarks
Congrats! You found the secret file!
Level 2 is at http://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud
Finance headline
India Forex Rese...
Search
ENG
IN
6:19:54 PM
11/9/2024

Level-2

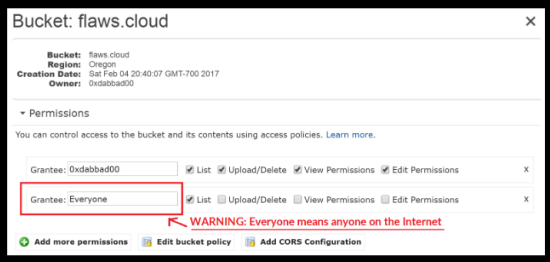

nas.io/cybersecuredindia/product
flAWS - Level 2
Not secure
level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud
Dashboard | HackerRa...
Overview
Fiverr - Freelance Serv...
Ayush Kumar Thakur
Blogger: Posts
GEEKHUB01
Chandigarh University...
My courses | CU-LMS
All Bookmarks
flAWS - Level 2
Lesson learned
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.
Examples of this problem
• Directory listing of S3 bucket of Legal Robot (link) and Shopify (link).
• Read and write permissions to S3 bucket for Shopify again (link) and Udemy (link). This challenge did not have read and write permissions, as that would destroy the challenge for other players, but it is a common problem.
Avoiding the mistake
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
Finance headline
India Forex Rese...
Search
ENG
IN
6:20:48 PM
11/9/2024

nas.io/cybersecuredindia/product | flAWS - Level 2

Not secure level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud

Dashboard | HackerRa... Overview Fiverr - Freelance Serv... Ayush Kumar Thakur Blogger: Posts GEEKHUB01 Chandigarh University... My courses | CU-LMS All Bookmarks

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.



"Everyone" means everyone on the Internet. You can also list the files simply by going to http://flaws.cloud.s3.amazonaws.com/ due to that List permission.

Level 2

The next level is fairly similar, with a slight twist. You're going to need your own AWS account for this. You just need the free tier.

For hints, see Hint 1

Finance headline India Forex Rese... Search ENG IN 6:21:06 PM 11/9/2024

nas.io/cybersecuredindia/product | flAWS

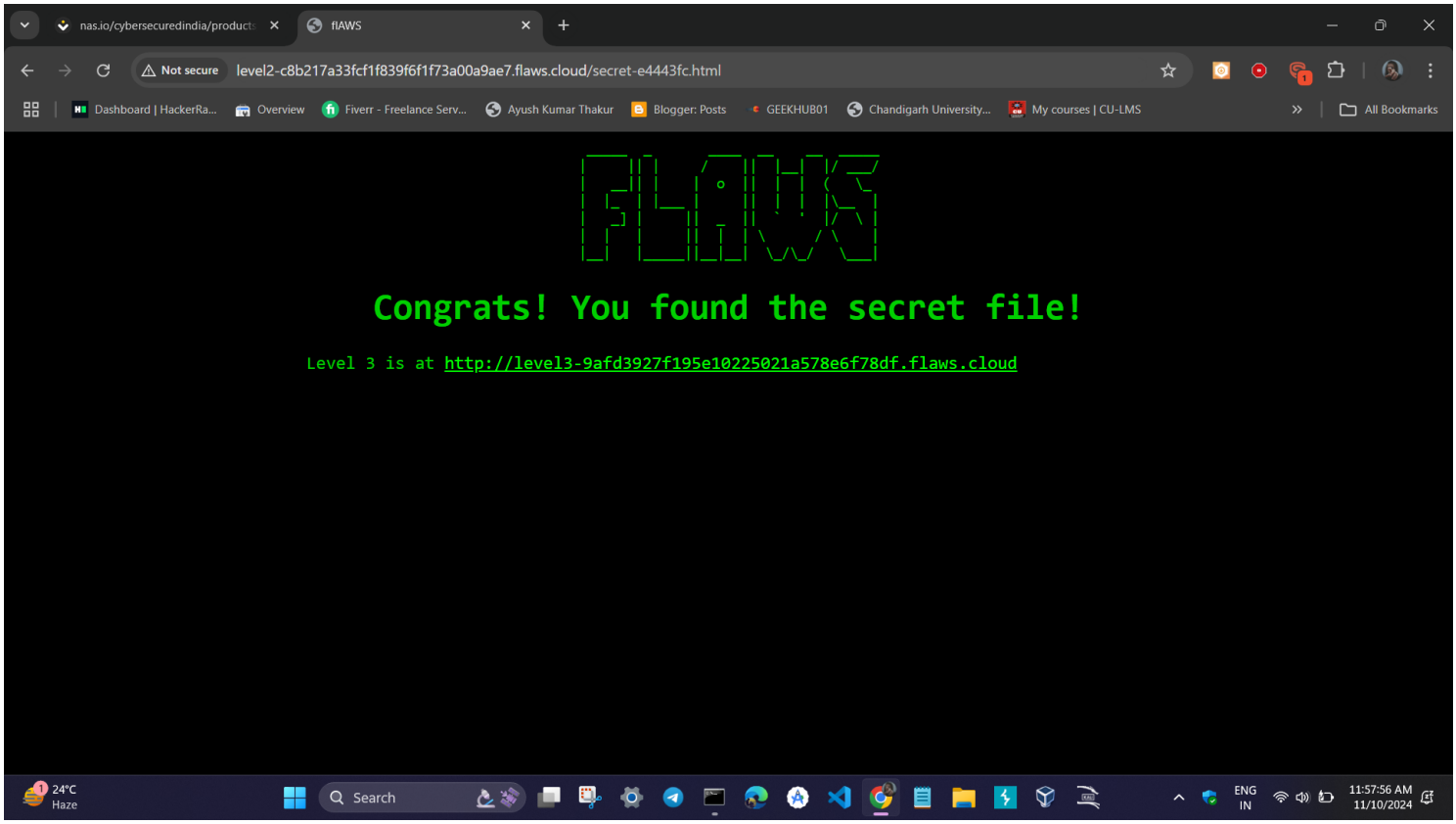
Not secure level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud/hint1.html

Dashboard | HackerRa... Overview Fiverr - Freelance Serv... Ayush Kumar Thakur Blogger: Posts GEEKHUB01 Chandigarh University... My courses | CU-LMS All Bookmarks

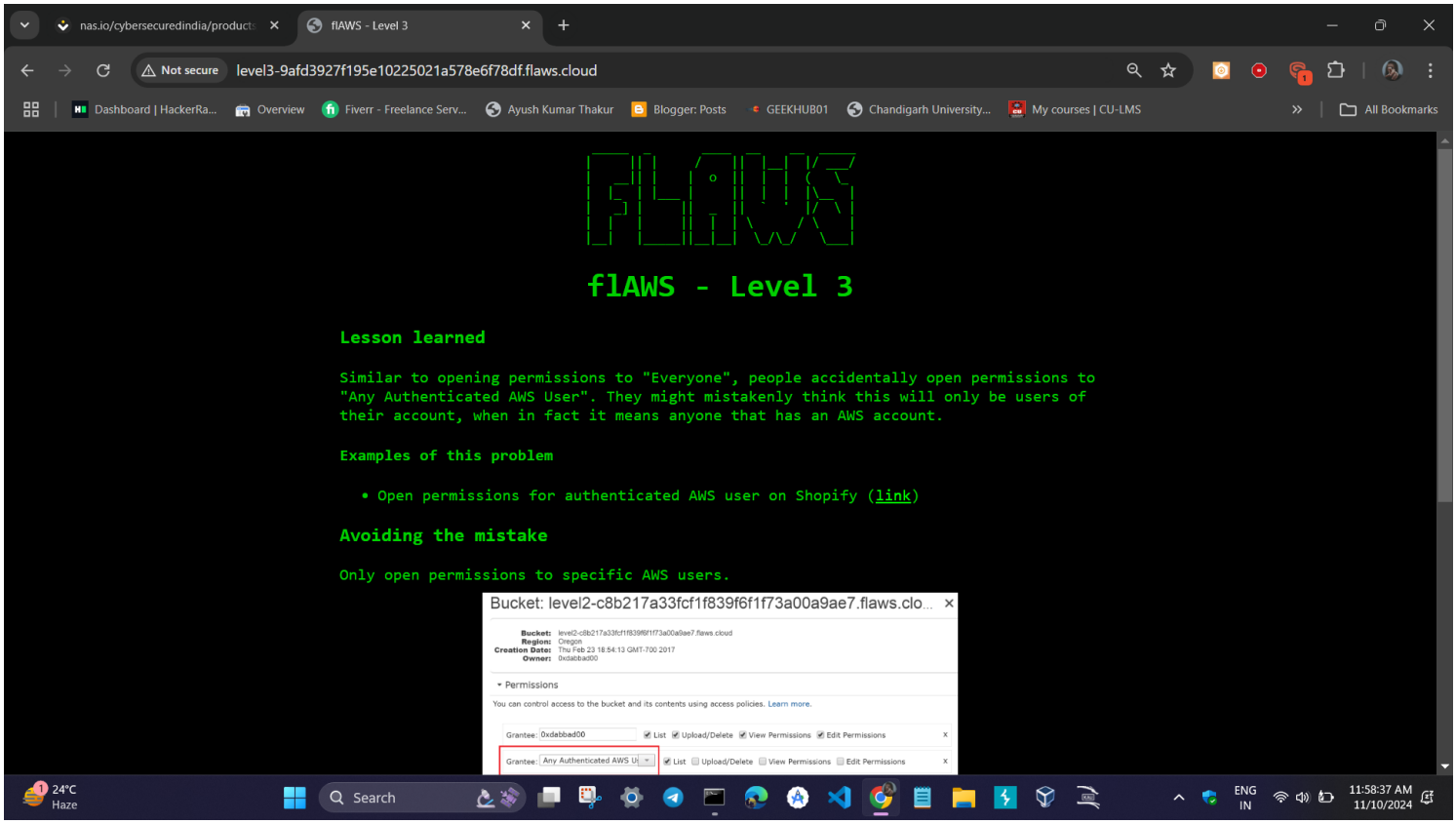
Select Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.

C:\Users\aayus>aws configure
AWS Access Key ID [****************L37Z]:
AWS Secret Access Key [****************n8Er]:
Default region name [us-east-1]:
Default output format [json]:

C:\Users\aayus>aws s3 ls s3://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud
2017-02-27 07:32:15      80751 everyone.png
2017-03-03 09:17:17       1433 hint1.html
2017-02-27 07:34:39       1035 hint2.html
2017-02-27 07:32:14       2786 index.html
2017-02-27 07:32:14         26 robots.txt
2017-02-27 07:32:15       1051 secret-e4443fc.html

C:\Users\aayus>
```

24°C Haze Search ENG IN 11:57:05 AM 11/10/2024


nas.io/cybersecuredindia/product
flAWS
Not secure
level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud/secret-e4443fc.html
Dashboard | HackerRa...
Overview
Fiverr - Freelance Serv...
Ayush Kumar Thakur
Blogger: Posts
GEEKHUB01
Chandigarh University...
My courses | CU-LMS
All Bookmarks
Congrats! You found the secret file!
Level 3 is at http://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud
24°C
Haze
Search
ENG
IN
11:57:56 AM
11/10/2024

Level-3


nas.io/cybersecuredindia/product
flAWS - Level 3
Not secure
level3-9afd3927f195e10225021a578e6f78df.flaws.cloud
Dashboard | HackerRa...
Overview
Fiverr - Freelance Serv...
Ayush Kumar Thakur
Blogger: Posts
GEEKHUB01
Chandigarh University...
My courses | CU-LMS
All Bookmarks
flAWS - Level 3
Lesson learned
Similar to opening permissions to "Everyone", people accidentally open permissions to "Any Authenticated AWS User". They might mistakenly think this will only be users of their account, when in fact it means anyone that has an AWS account.
Examples of this problem
Open permissions for authenticated AWS user on Shopify (link)
Avoiding the mistake
Only open permissions to specific AWS users.
Bucket: level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.clo...
Permissions
You can control access to the bucket and its contents using access policies. Learn more.
Grantee: 0xdabbad00
Grantee: Any Authenticated AWS U
24°C
Haze
Search
ENG
IN
11:58:37 AM
11/10/2024

nas.io/cybersecuredindia/product | flAWS - Level 3

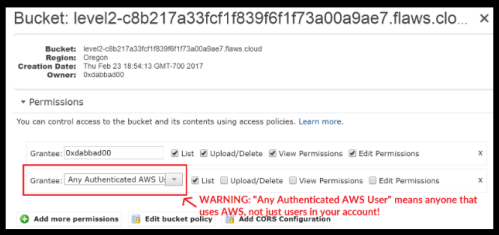
Not secure level3-9afd3927f195e10225021a578e6f78df.flaws.cloud

Dashboard | HackerRa... Overview Fiverr - Freelance Serv... Ayush Kumar Thakur Blogger: Posts GEEKHUB01 Chandigarh University... My courses | CU-LMS All Bookmarks

- Open permissions for authenticated AWS user on Shopify (link)

Avoiding the mistake

Only open permissions to specific AWS users.



This screenshot is from the webconsole in 2017. This setting can no longer be set in the webconsole, but the SDK and third-party tools sometimes allow it.

Level 3

The next level is fairly similar, with a slight twist. Time to find your first AWS key! I bet you'll find something that will let you list what other buckets are.

For hints, see Hint 1

24°C Haze Search ENG IN 11:58:50 AM 11/10/2024

nas.io/cybersecuredindia/product | flAWS

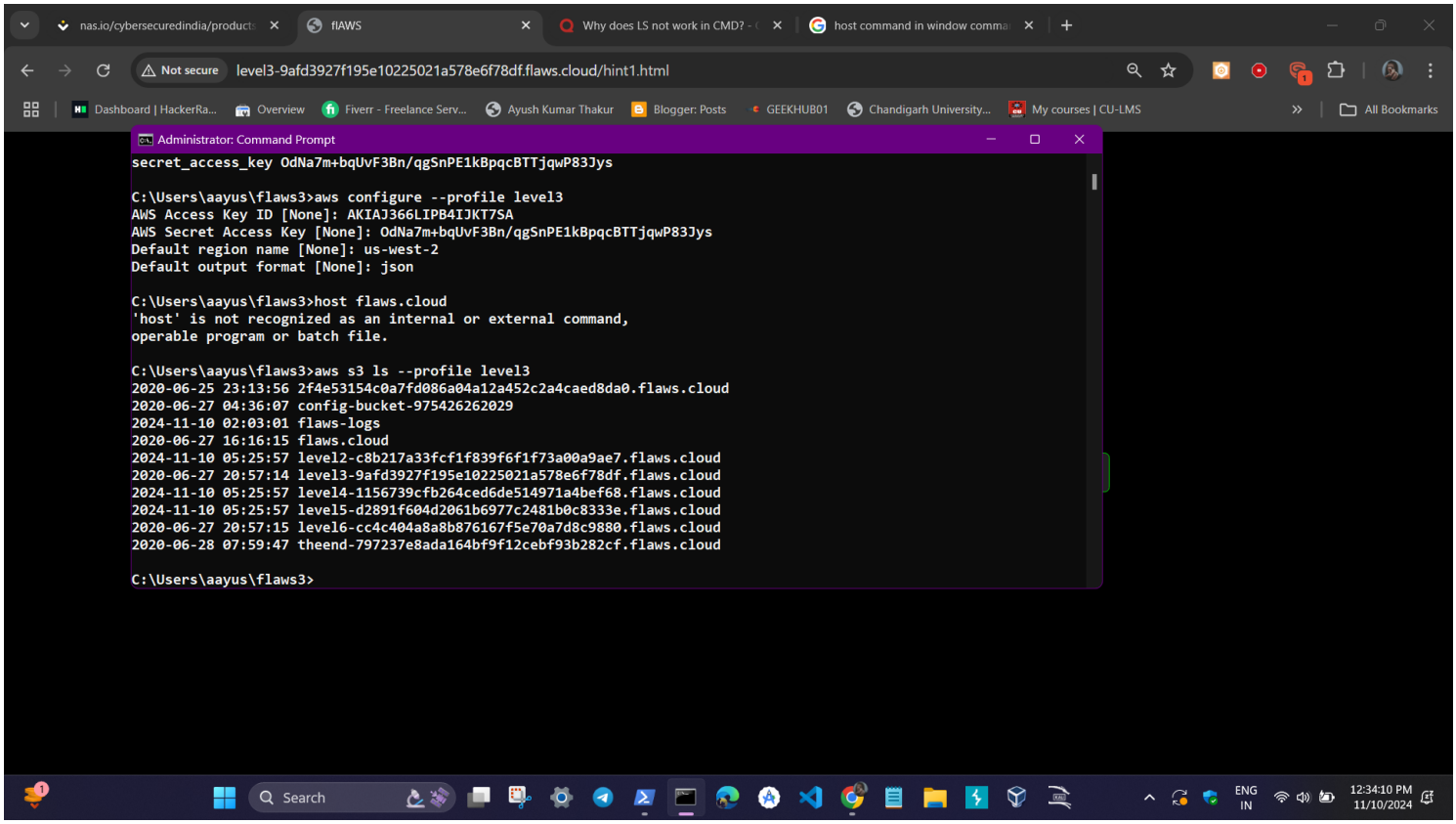
Not secure level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/hint1.html

Dashboard | HackerRa... Overview Fiverr - Freelance Serv... Ayush Kumar Thakur Blogger: Posts GEEKHUB01 Chandigarh University... My courses | CU-LMS All Bookmarks

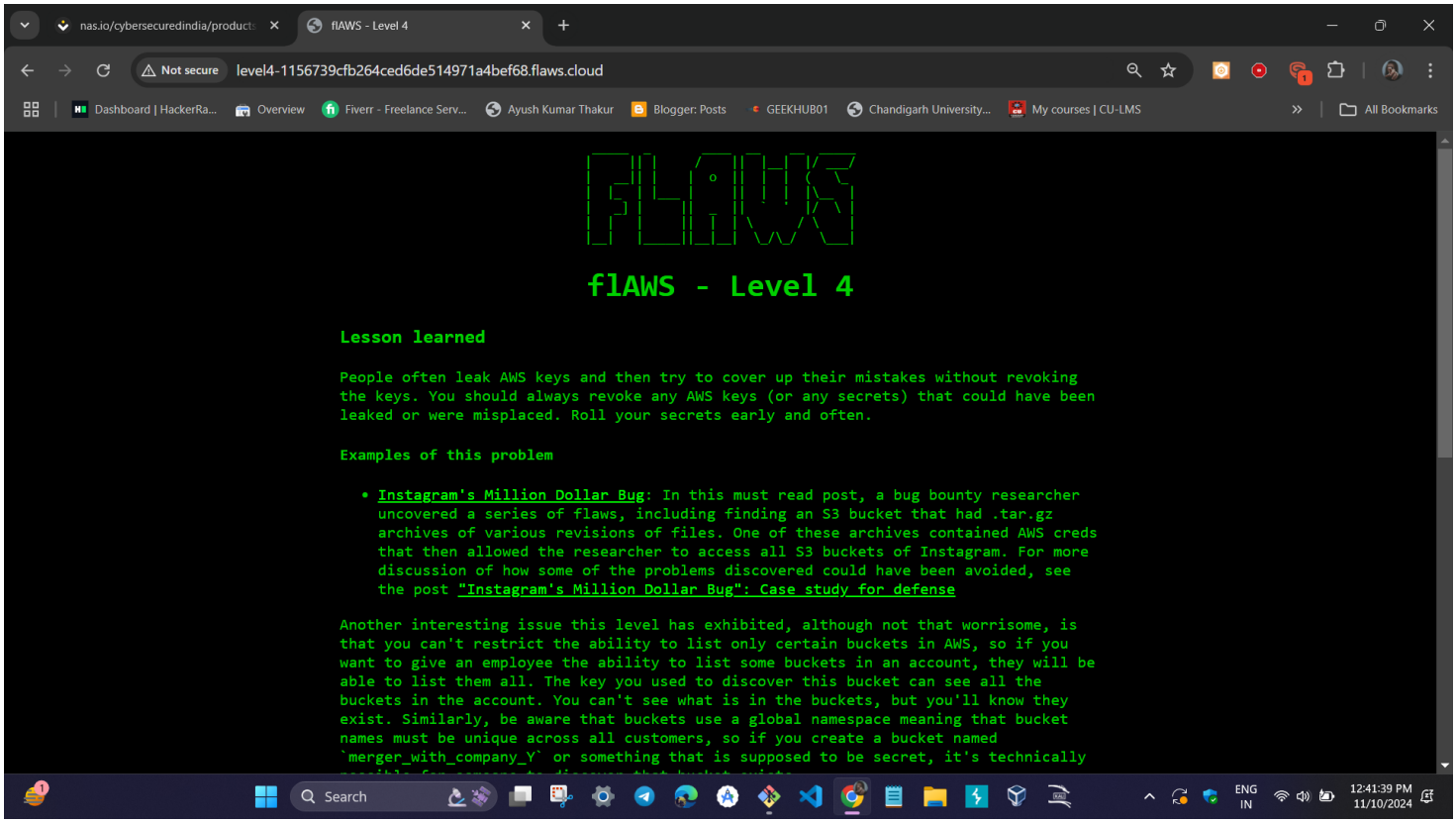
Administrator: Windows PowerShell (x86)

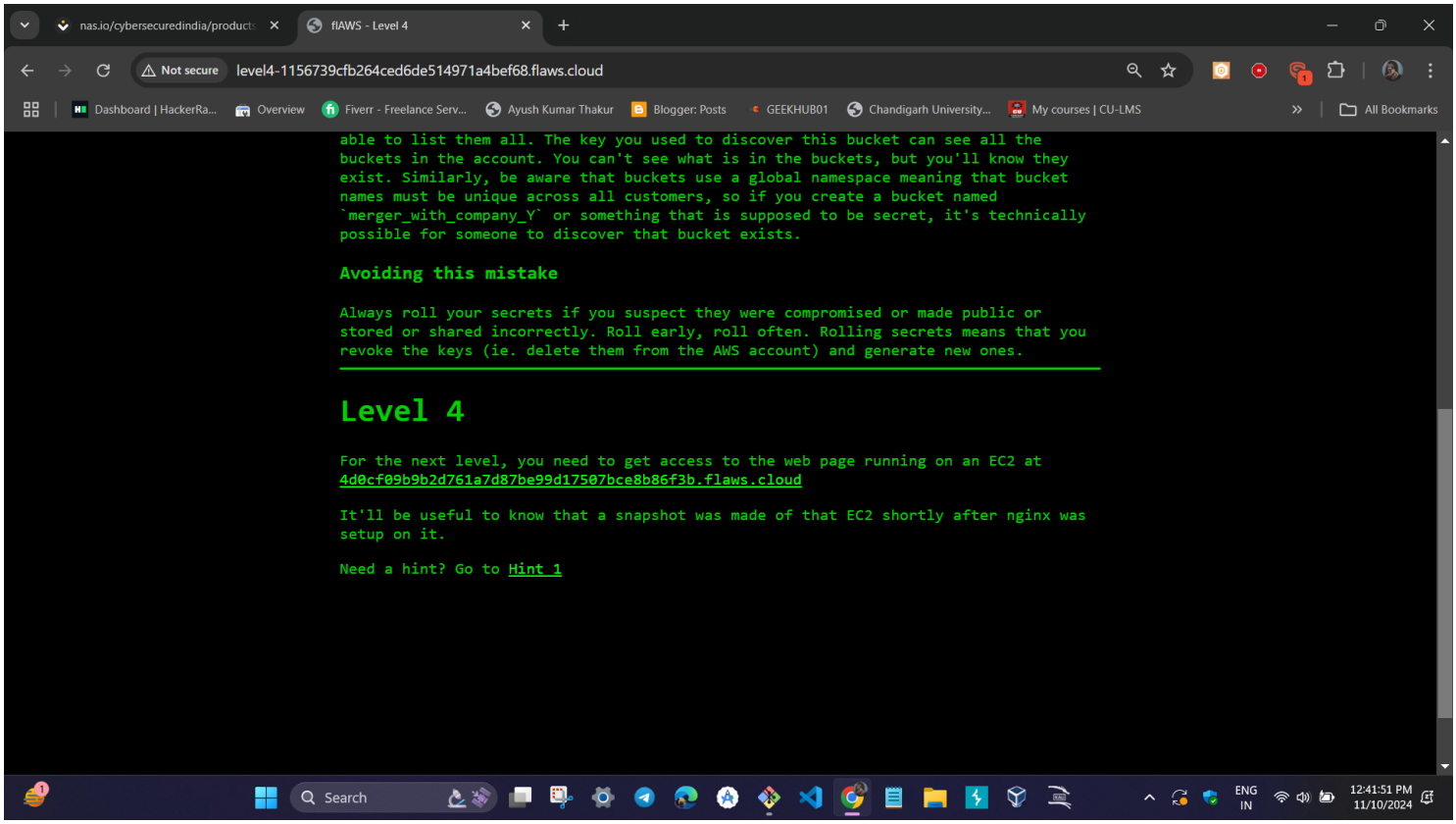
```
PS C:\Users\aayus> aws s3 ls s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud
                           PRE .git/
2017-02-27 05:44:33     123637 authenticated_users.png
2017-02-27 05:44:34       1552 hint1.html
2017-02-27 05:44:34       1426 hint2.html
2017-02-27 05:44:35       1247 hint3.html
2017-02-27 05:44:33       1035 hint4.html
2020-05-22 23:51:10       1861 index.html
2017-02-27 05:44:33         26 robots.txt
PS C:\Users\aayus>
```

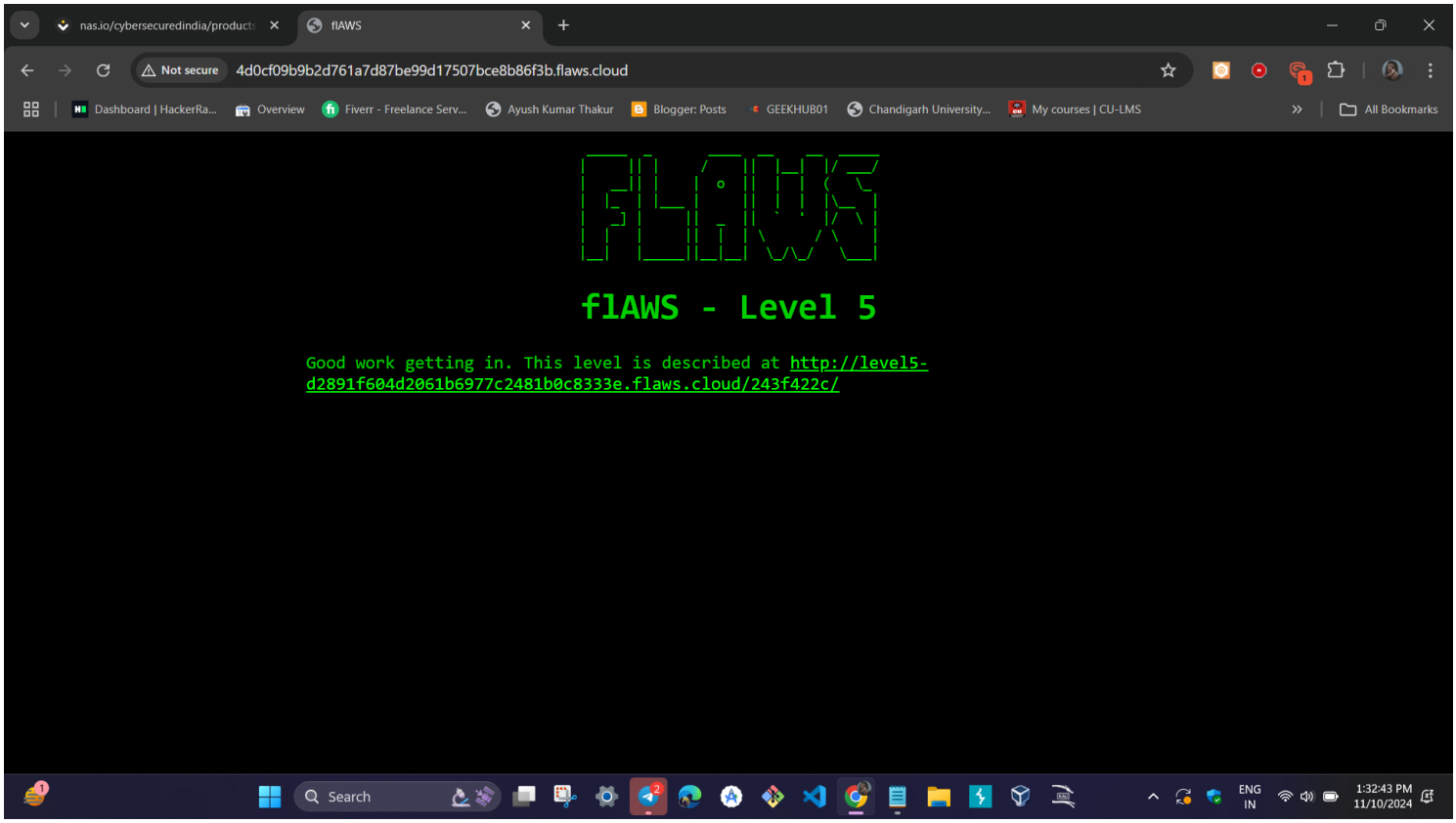
24°C Haze Search ENG IN 12:10:33 PM 11/10/2024


nas.io/cybersecuredindia/product
flAWS
Why does LS not work in CMD? -
host command in window comma
Not secure
level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/hint1.html
Dashboard | HackerRa...
Overview
Fiverr - Freelance Serv...
Ayush Kumar Thakur
Blogger: Posts
GEEKHUB01
Chandigarh University...
My courses | CU-LMS
All Bookmarks
Administrator: Command Prompt
secret_access_key OdNa7m+bqUvF3Bn/qgSnPE1kBpqcBTTjqwP83Jys
C:\Users\aayus\flaws3>aws configure --profile level3
AWS Access Key ID [None]: AKIAJ366LIPB4IJKT7SA
AWS Secret Access Key [None]: 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
Default region name [None]: us-west-2
Default output format [None]: json
C:\Users\aayus\flaws3>host flaws.cloud
'host' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\aayus\flaws3>aws s3 ls --profile level3
2020-06-25 23:13:56 2f4e53154c0a7fd086a04a12a452c2a4caed8da0.flaws.cloud
2020-06-27 04:36:07 config-bucket-975426262029
2024-11-10 02:03:01 flaws-logs
2020-06-27 16:16:15 flaws.cloud
2024-11-10 05:25:57 level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud
2020-06-27 20:57:14 level3-9afd3927f195e10225021a578e6f78df.flaws.cloud
2024-11-10 05:25:57 level4-1156739cfb264ced6de514971a4bef68.flaws.cloud
2024-11-10 05:25:57 level5-d2891f604d2061b6977c2481b0c8333e.flaws.cloud
2020-06-27 20:57:15 level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud
2020-06-28 07:59:47 theend-797237e8ada164bf9f12cebf93b282cf.flaws.cloud
C:\Users\aayus\flaws3>
Search
ENG
IN
12:34:10 PM
11/10/2024

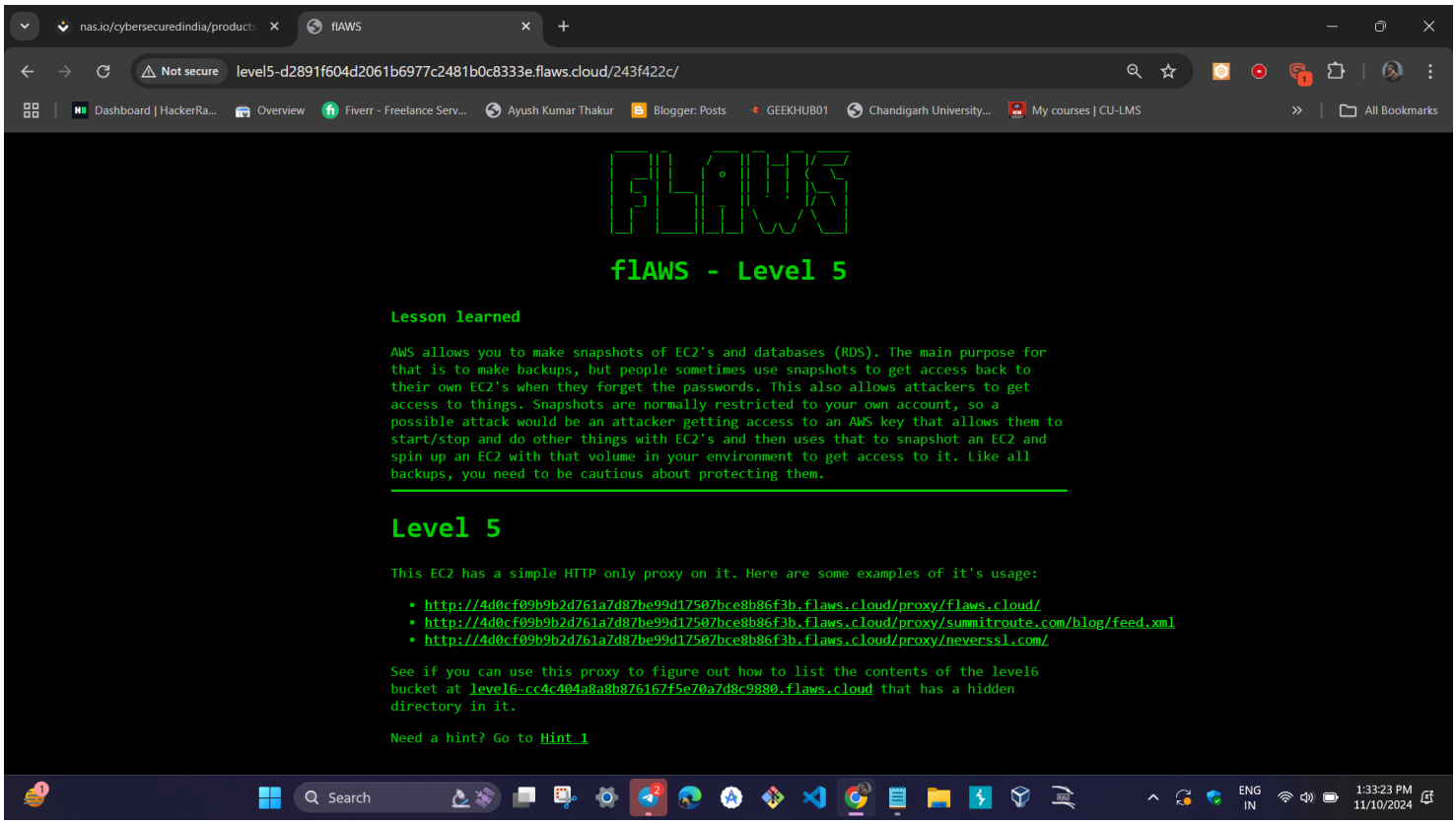
Level-4

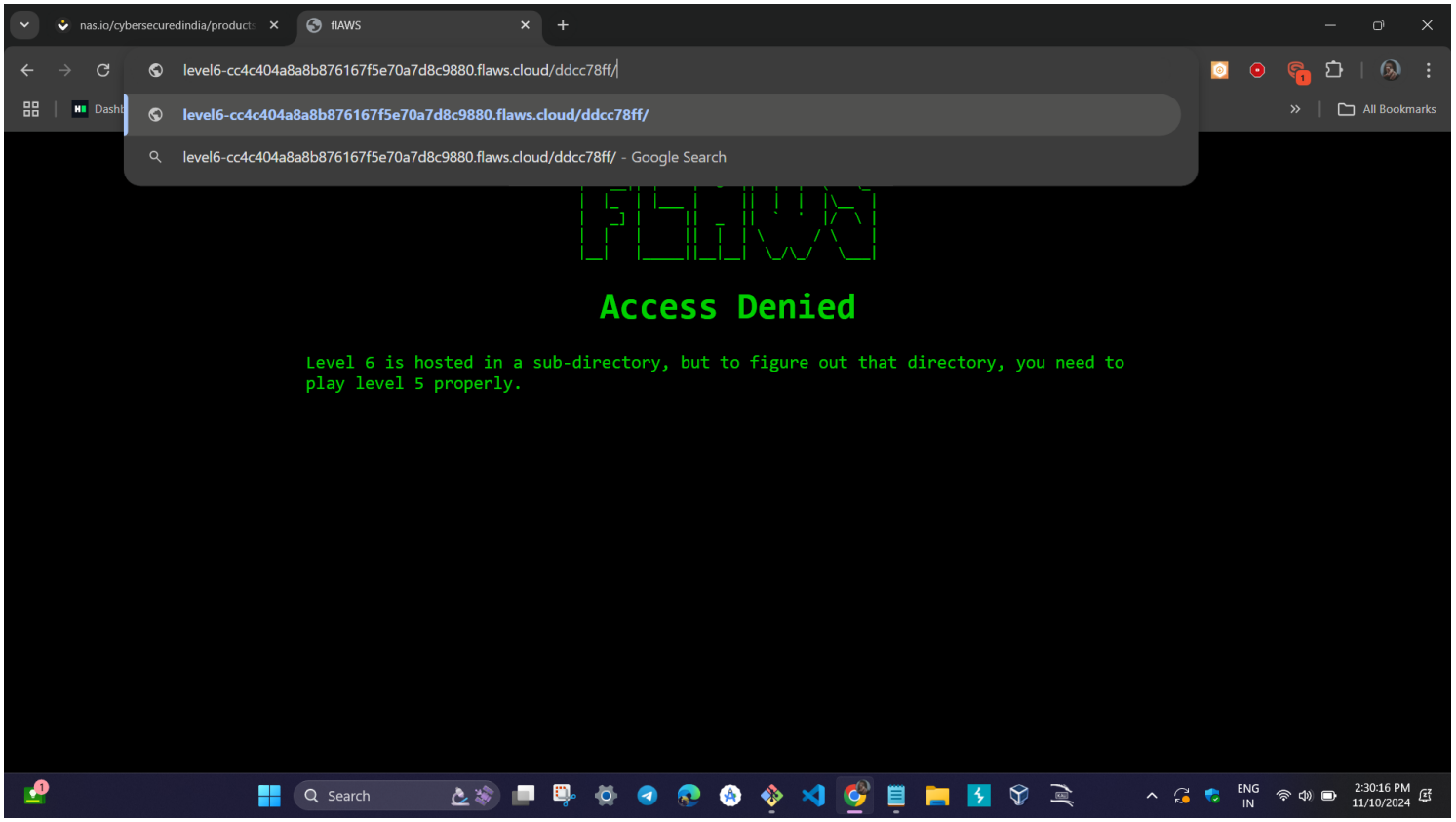

nas.io/cybersecuredindia/product
flAWS - Level 4
Not secure
level4-1156739cfb264ced6de514971a4bef68.flaws.cloud
Dashboard | HackerRa...
Overview
Fiverr - Freelance Serv...
Ayush Kumar Thakur
Blogger: Posts
GEEKHUB01
Chandigarh University...
My courses | CU-LMS
All Bookmarks
flAWS - Level 4
Lesson learned
People often leak AWS keys and then try to cover up their mistakes without revoking the keys. You should always revoke any AWS keys (or any secrets) that could have been leaked or were misplaced. Roll your secrets early and often.
Examples of this problem
Instagram's Million Dollar Bug: In this must read post, a bug bounty researcher uncovered a series of flaws, including finding an S3 bucket that had .tar.gz archives of various revisions of files. One of these archives contained AWS creds that then allowed the researcher to access all S3 buckets of Instagram. For more discussion of how some of the problems discovered could have been avoided, see the post "Instagram's Million Dollar Bug": Case study for defense
Another interesting issue this level has exhibited, although not that worrisome, is that you can't restrict the ability to list only certain buckets in AWS, so if you want to give an employee the ability to list some buckets in an account, they will be able to list them all. The key you used to discover this bucket can see all the buckets in the account. You can't see what is in the buckets, but you'll know they exist. Similarly, be aware that buckets use a global namespace meaning that bucket names must be unique across all customers, so if you create a bucket named `merger_with_company_Y` or something that is supposed to be secret, it's technically
Search
ENG
IN
12:41:39 PM
11/10/2024


nas.io/cybersecuredindia/products
flAWS - Level 4
Not secure
level4-1156739cfb264ced6de514971a4bef68.flaws.cloud
Dashboard | HackerRa...
Overview
Fiverr - Freelance Serv...
Ayush Kumar Thakur
Blogger: Posts
GEEKHUB01
Chandigarh University...
My courses | CU-LMS
All Bookmarks
able to list them all. The key you used to discover this bucket can see all the buckets in the account. You can't see what is in the buckets, but you'll know they exist. Similarly, be aware that buckets use a global namespace meaning that bucket names must be unique across all customers, so if you create a bucket named `merger_with_company_Y` or something that is supposed to be secret, it's technically possible for someone to discover that bucket exists.
Avoiding this mistake
Always roll your secrets if you suspect they were compromised or made public or stored or shared incorrectly. Roll early, roll often. Rolling secrets means that you revoke the keys (ie. delete them from the AWS account) and generate new ones.
Level 4
For the next level, you need to get access to the web page running on an EC2 at 4d0cf09b9b2d761a7d87be99d17507bce8b86f3b.flaws.cloud
It'll be useful to know that a snapshot was made of that EC2 shortly after nginx was setup on it.
Need a hint? Go to Hint 1
Search
ENG
IN
12:41:51 PM
11/10/2024

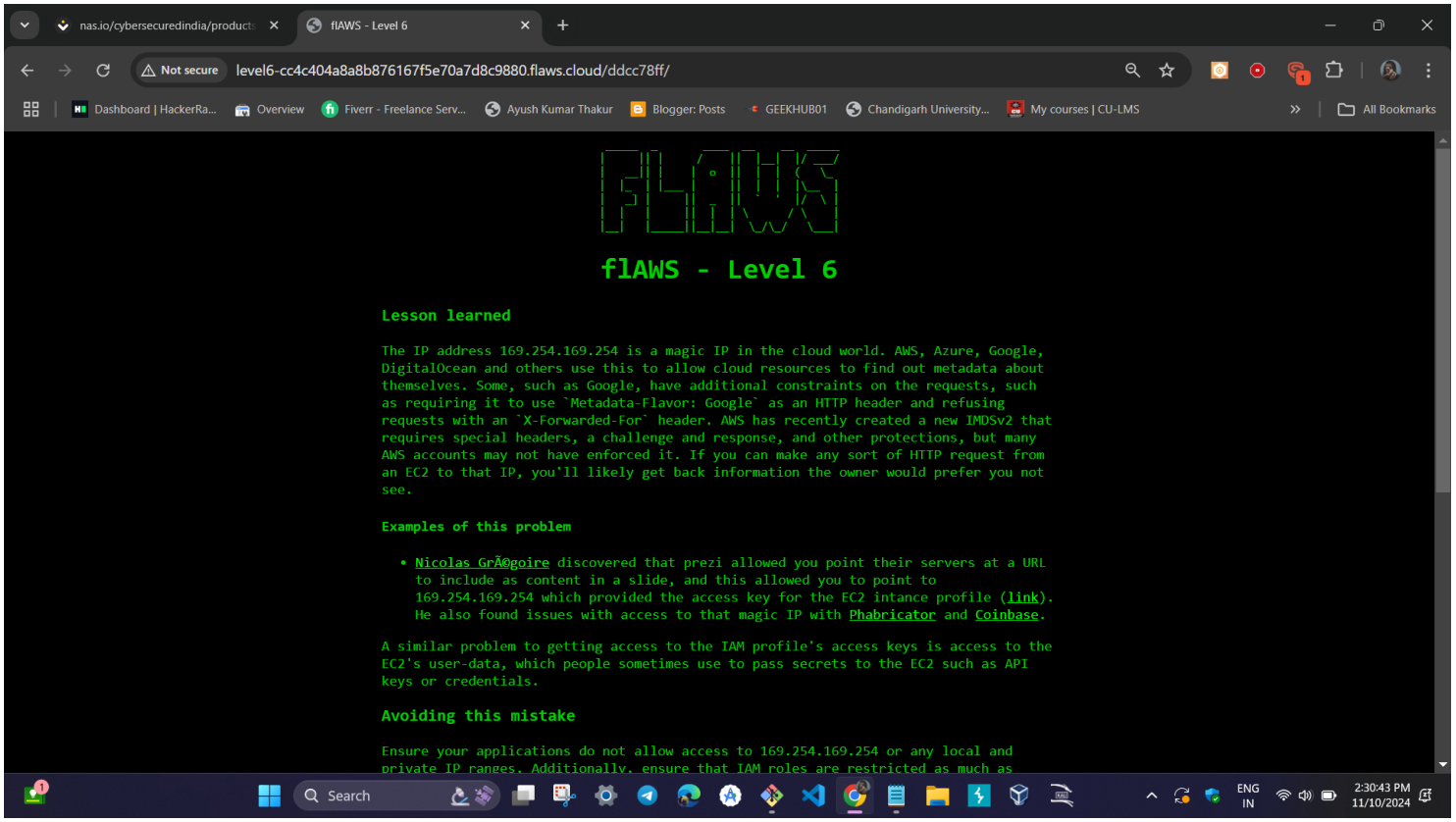

nas.io/cybersecuredindia/products
flAWS
Not secure
4d0cf09b9b2d761a7d87be99d17507bce8b86f3b.flaws.cloud
Dashboard | HackerRa...
Overview
Fiverr - Freelance Serv...
Ayush Kumar Thakur
Blogger: Posts
GEEKHUB01
Chandigarh University...
My courses | CU-LMS
All Bookmarks
flAWS - Level 5
Good work getting in. This level is described at http://level5-d2891f604d2061b6977c2481b0c8333e.flaws.cloud/243f422c/
Search
ENG
IN
1:32:43 PM
11/10/2024

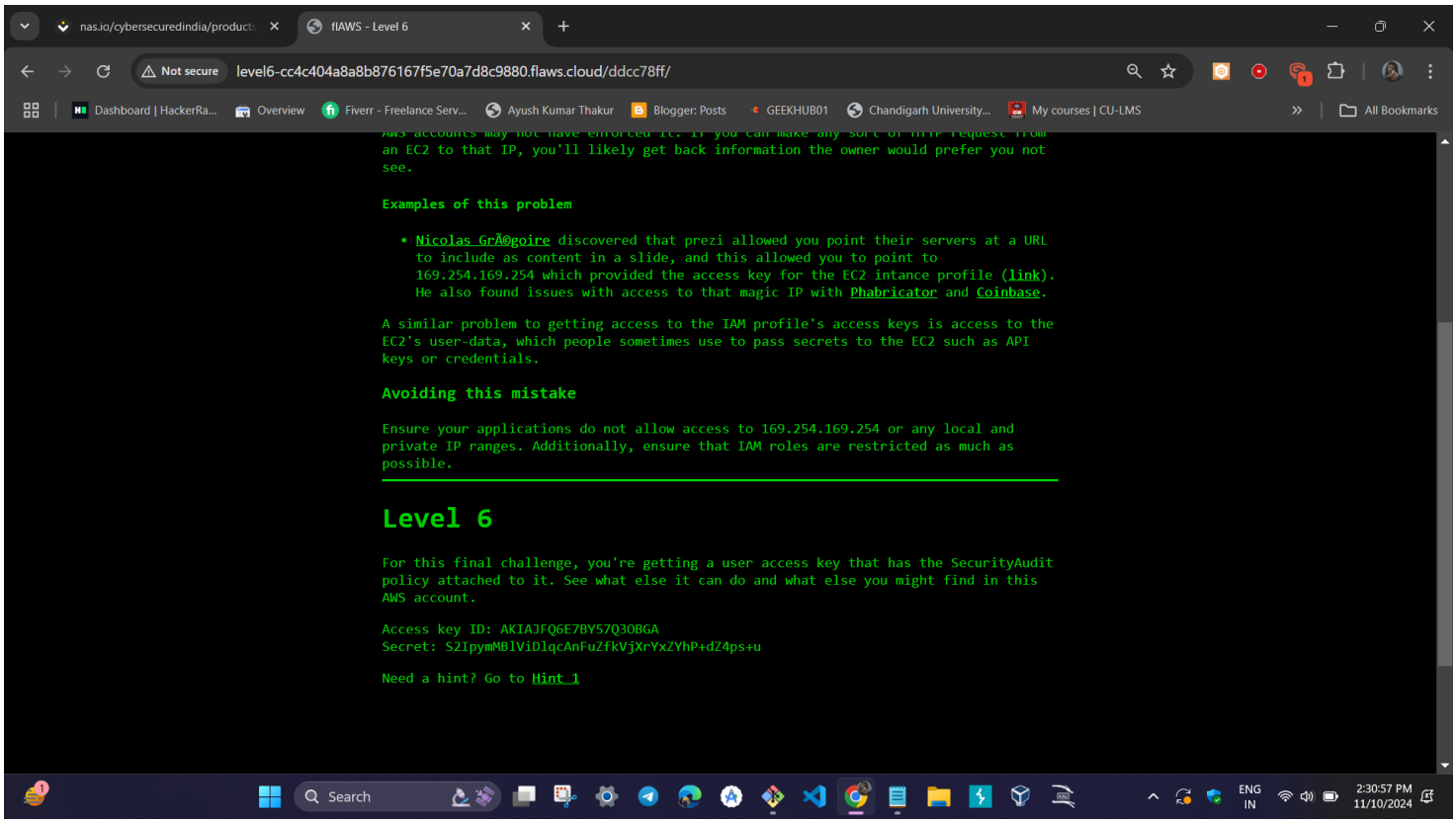
Level-5

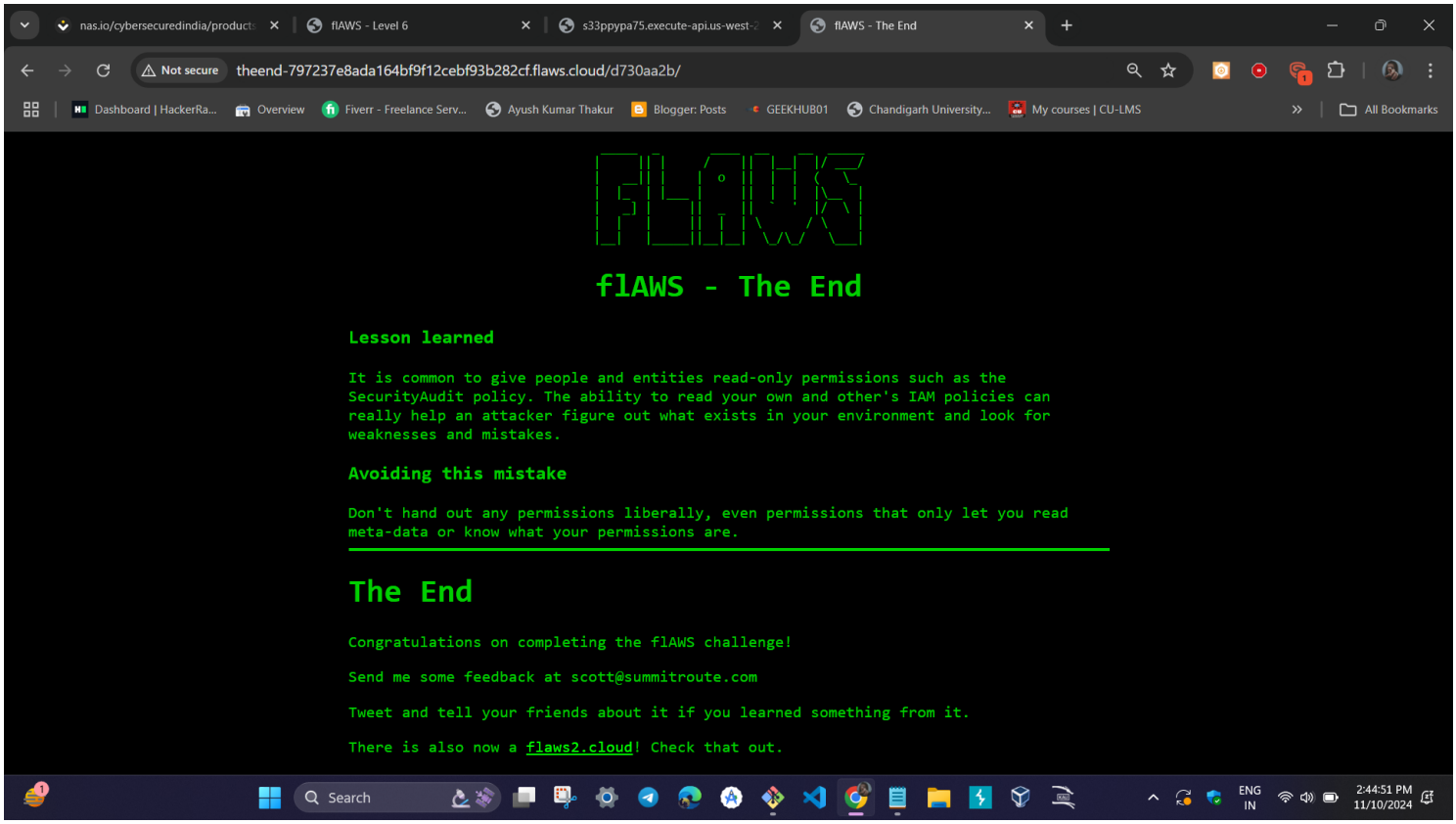




Level-6


nas.io/cybersecuredindia/product
flAWS - Level 6
Not secure
level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud/ddcc78ff/
Dashboard | HackerRa...
Overview
Fiverr - Freelance Serv...
Ayush Kumar Thakur
Blogger: Posts
GEEKHUB01
Chandigarh University...
My courses | CU-LMS
All Bookmarks
flAWS - Level 6
Lesson learned
The IP address 169.254.169.254 is a magic IP in the cloud world. AWS, Azure, Google, DigitalOcean and others use this to allow cloud resources to find out metadata about themselves. Some, such as Google, have additional constraints on the requests, such as requiring it to use `Metadata-Flavor: Google` as an HTTP header and refusing requests with an `X-Forwarded-For` header. AWS has recently created a new IMDSv2 that requires special headers, a challenge and response, and other protections, but many AWS accounts may not have enforced it. If you can make any sort of HTTP request from an EC2 to that IP, you'll likely get back information the owner would prefer you not see.
Examples of this problem
Nicolas GrÃ©goire discovered that prezi allowed you point their servers at a URL to include as content in a slide, and this allowed you to point to 169.254.169.254 which provided the access key for the EC2 intance profile (link). He also found issues with access to that magic IP with Phabricator and Coinbase.
A similar problem to getting access to the IAM profile's access keys is access to the EC2's user-data, which people sometimes use to pass secrets to the EC2 such as API keys or credentials.
Avoiding this mistake
Ensure your applications do not allow access to 169.254.169.254 or any local and private IP ranges. Additionally, ensure that IAM roles are restricted as much as
Search
ENG
IN
2:30:43 PM
11/10/2024


nas.io/cybersecuredindia/product
flAWS - Level 6
Not secure
level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud/ddcc78ff/
Dashboard | HackerRa...
Overview
Fiverr - Freelance Serv...
Ayush Kumar Thakur
Blogger: Posts
GEEKHUB01
Chandigarh University...
My courses | CU-LMS
All Bookmarks
an EC2 to that IP, you'll likely get back information the owner would prefer you not see.
Examples of this problem
Nicolas GrÃ©goire discovered that prezi allowed you point their servers at a URL to include as content in a slide, and this allowed you to point to 169.254.169.254 which provided the access key for the EC2 intance profile (link). He also found issues with access to that magic IP with Phabricator and Coinbase.
A similar problem to getting access to the IAM profile's access keys is access to the EC2's user-data, which people sometimes use to pass secrets to the EC2 such as API keys or credentials.
Avoiding this mistake
Ensure your applications do not allow access to 169.254.169.254 or any local and private IP ranges. Additionally, ensure that IAM roles are restricted as much as possible.
Level 6
For this final challenge, you're getting a user access key that has the SecurityAudit policy attached to it. See what else it can do and what else you might find in this AWS account.
Access key ID: AKIAJFQ6E7BY57Q3OBGA
Secret: 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
Need a hint? Go to Hint 1
Search
ENG
IN
2:30:57 PM
11/10/2024


nas.io/cybersecuredindia/product
flAWS - Level 6
s33ppypa75.execute-api.us-west-2
flAWS - The End
Not secure
theend-797237e8ada164bf9f12cebf93b282cf.flaws.cloud/d730aa2b/
Dashboard | HackerRa...
Overview
Fiverr - Freelance Serv...
Ayush Kumar Thakur
Blogger: Posts
GEEKHUB01
Chandigarh University...
My courses | CU-LMS
All Bookmarks
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.
Search
ENG
IN
2:44:51 PM
11/10/2024