

Documentació de repte HackEPS 2024:

CTF de USE-IT

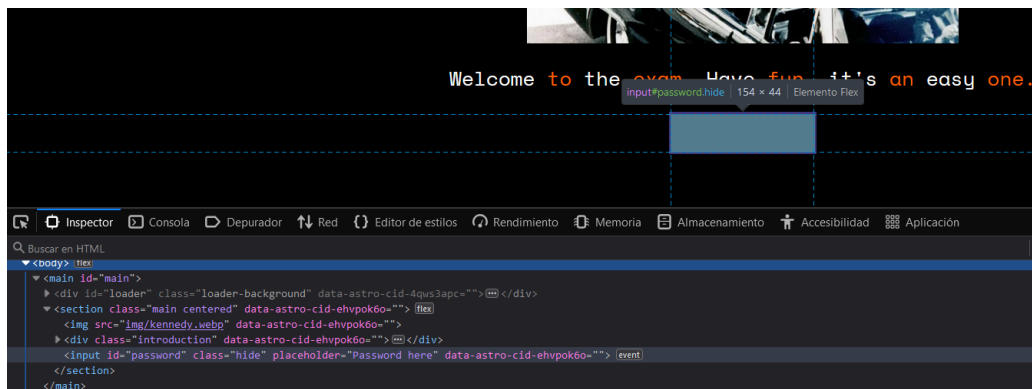
Comencem el repte amb la següent informació:

URL → <https://hackaton2024.useitapps.com/>

Codi de grup (3): SPxpKStAjefnmcofPUSDCztnYjpJGx

STEP 1

En aquest pas, el primer que vam fer va ser inspeccionar la pàgina web per veure el codi font. Vam trobar-hi que hi havia un input que tenia `class="none"`, ho vam treure i llavors va aparèixer el camp de text per introduir la contrasenya. Llavors vam provar d'introduir-hi el codi de grup i com vam veure que no succeïa res vam decidir investigar el que restava a la pàgina.

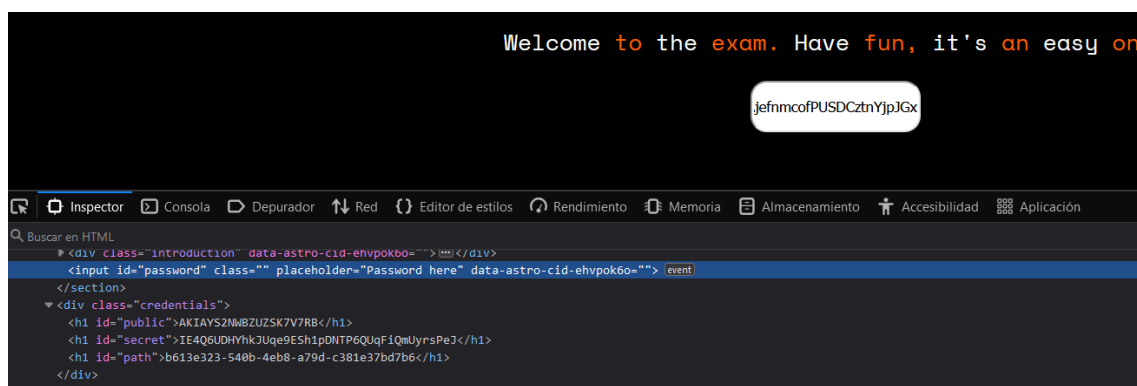


Posteriorment, vam descarregar-nos la imatge del Kennedy (*kennedy.webp*) i vam fer servir l'eina online <https://exif.tools> per revisar si tenia meta-dades. En veure el “User Comment” ràpidament vam tornar a la web i concatenant el codi de grup amb la contrasenya que acabàvem d’obtenir ja vam poder obtenir les credencials.

User Comment: password=j9G2FtnXLti6vA6KTwsHL3ttzrFju6NYx8:code_delivered

Contrassenya definitiva:

j9G2FtnXLti6vA6KTwsHL3ttzrFju6NYx8:SPxpKStAjefnmcofPUSDCztnYjpJGx

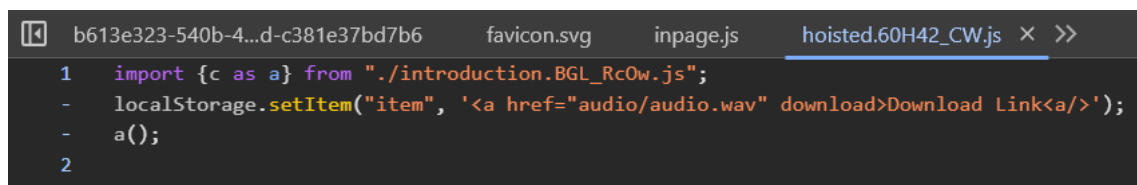


En aquestes credencials hi podíem veure “public”, “secret” i “path”. De moment les dues primeres no feien falta, posant la credencial path a la url del repte ens va portar a l'*step 2*.

<https://hackaton2024.useitapps.com/b613e323-540b-4eb8-a79d-c381e37bd7b6>

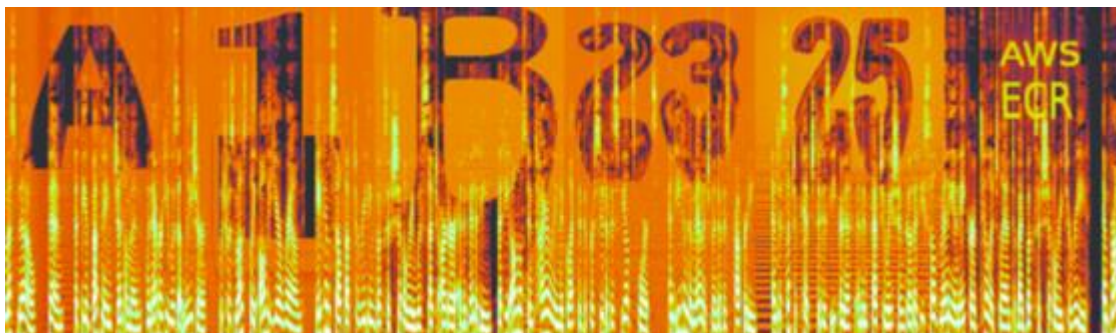
STEP 2

Primerament, vam inspeccionar la pàgina però no vam trobar-hi res al codi font. A continuació vam revisar el text i ens vam fixar que esmentava que el subjecte de vegades es gravava mentre llegia. A partir d'aquí vam decidir inspeccionar el *local storage* del navegador i vam trobar l'element que contenia la ruta per un fitxer d'àudio *.wav* el que quadrava amb el text.



Un cop descarregat, el vam escoltar i vam notar que s'escoltaven com interferències. Vam pensar que el seu espectrograma podia ocultar algun missatge i vam introduir l'àudio a l'eina online Audacity. En veure el resultat vam poder observar perfectament un codi “A1B2325” i unes altres lletres “AWS ECR”.





Com es pot veure en la imatge anterior, per continuar ens faria falta usar AWS ECR, pel que ens vam instal·lar `aws-cli`. Un cop instal·lat, vam executar la comanda `aws configuration` on vam emplenar els següents camps:

<https://docs.aws.amazon.com/cli/latest/reference/ecr/>

```
$ aws configuration

AWS Access Key ID:
$ AKIAYS2NWBZUZSK7V7RB (public)

AWS Secret Access Key:
$ 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 (secret)

Default region name:
$ us-west-2 (vam provar amb altres regions però ens donava error)

Default output format:
$ json
```

A continuació, vam executar la següent comanda per conèixer els noms dels repositoris als que podíem accedir:

```
$ aws ecr describe-repositories
```

Aquesta comanda ens va retornar les dades dels repositoris i vam poder veure que n'hi havia 1 amb el nom de "hackeps2024" i també vam obtenir l'identificador de registre "590184058473".

```
{
  "repositories": [
    {
      "repositoryArn": "arn:aws:ecr:us-west-2:590184058473:repository/hackeps2024",
      "registryId": "590184058473",
      "repositoryName": "hackeps2024",
```

```
        "repositoryUri": "590184058473.dkr.ecr.us-west-2.amazonaws.com/hackeps2024",
        "createdAt": "2024-10-16T09:22:18.732000+02:00",
        "imageTagMutability": "MUTABLE",
        "imageScanningConfiguration": {
            "scanOnPush": false
        },
        "encryptionConfiguration": {
            "encryptionType": "AES256"
        }
    }
]
}
```

Amb el nom del repositori, podem llistar les imatges disponibles en aquest:

```
$ aws ecr list-images --repository-name hackeps2024

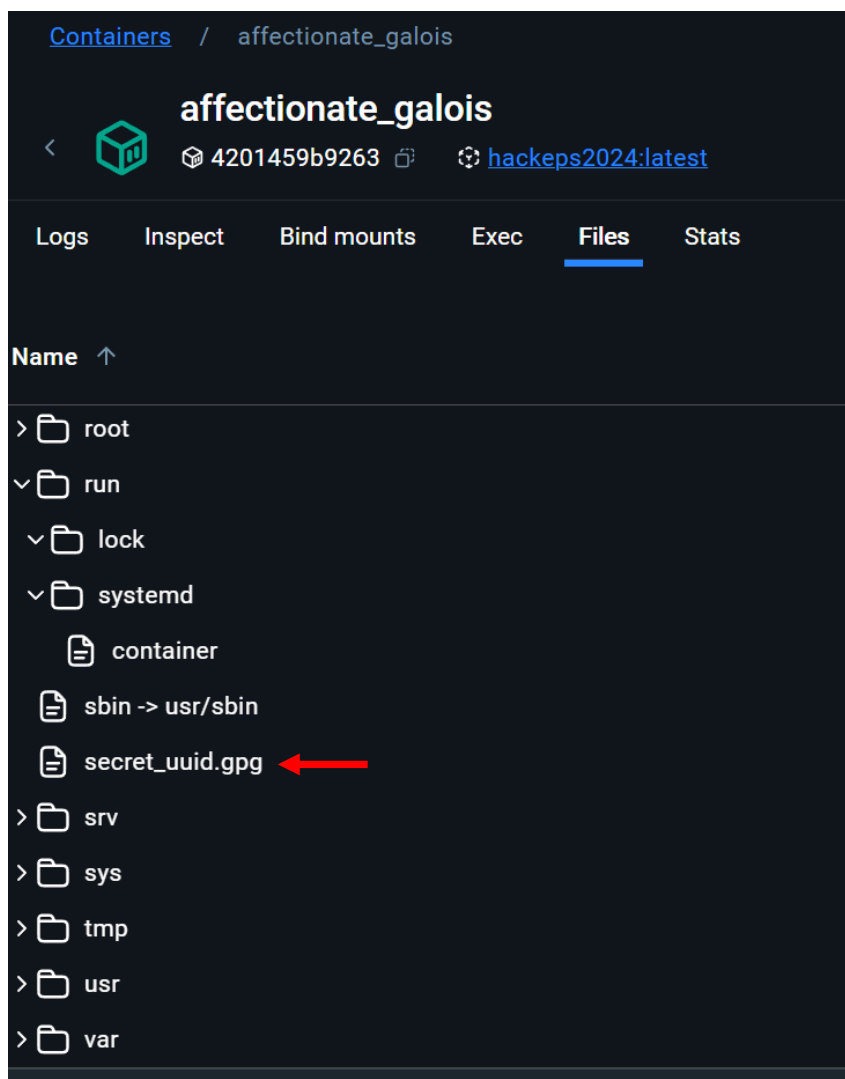
{
  "imageIds": [
    {
      "imageDigest": "sha256:0a4baafeb1020fbf42a206126c4e16292c218dfb5d9ee97c4fafe825f4be8757",
      "imageTag": "latest"
    }
  ]
}
```

A per poder-nos descarregar i examinar la imatge, vam utilitzar Docker amb les següents comandes:

```
$ aws ecr get-login-password --region us-west-2 | docker login --username AWS --password-stdin 590184058473.dkr.ecr.us-west-2.amazonaws.com

$ docker pull 590184058473.dkr.ecr.us-west-2.amazonaws.com/hackeps2024:latest
```

Amb la interfície per a Windows de Docker, vam poder examinar els fitxers del contenidor “step2”, on hi vam trobar un arxiu “secret_uuid.gpg” que apuntava a ser la clau per al continuar:



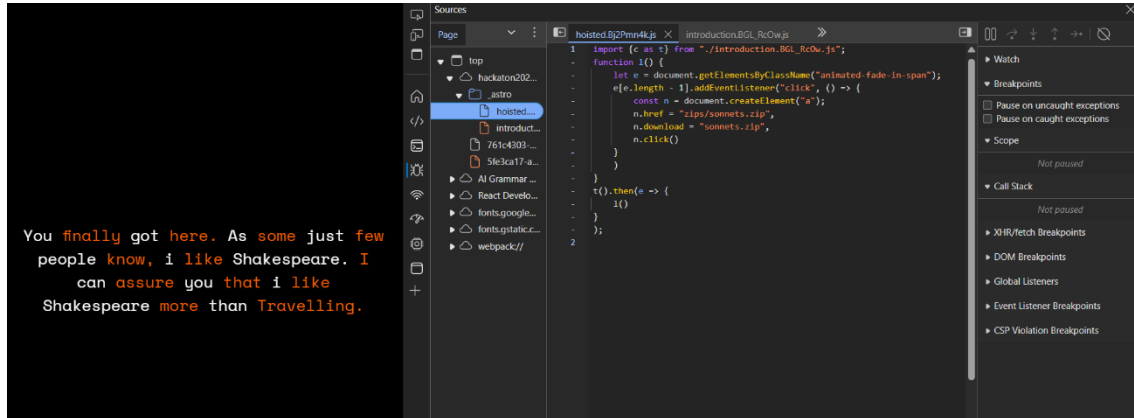
STEP 3

En la tercera fase, tornàvem a tenir un text informatiu en la pàgina web. Inspeccionant-la vam observar mirant els fitxers interns de JavaScript que si polsàvem la paraula Travelling se'ns descarregaria un fitxer *.zip*.

En aquest fitxer *.zip* hi havia uns sonets de Shakespeare. Vam haver d'analitzar-los i comparar-los amb els originals per veure les diferències. Fàcilment,

vam trobar que cada sonet tenia un país del món. Després agafant les inicials d'aquests països vam poder formar el nou *path*:

<https://hackaton2024.useitapps.com/761c4303-6381-40dc-b2e9-413ae52b1664>



<https://hackaton2024.useitapps.com/zips/sonnets.zip>

- 1: Glasgow
- 2: Quebec
- 3: Nairobi
- 4: Florence
- 5: Oslo
- 6: Warsaw
- 7: Tokyo
- 8: NewYork
- 9: Frankfurt
- 10: Zurich
- 11: Kiev
- 12: Cairo
- 13: Quito
- 14: Ulaanbaatar
- 15: Guangzhou
- 16: Havana
- 17: Fukuoka

18: Quetta

19: Amsterdam

20: Prague

21: Munich

22: Fes

23: Lisbon

24: Edinburgh

25: Sydney

26: Berlin

27: Yokohama

28: Jakarta

29: Rome

30: Ottawa

31: Vienna

32: Vancouver

33: Johannesburg

34: Istanbul

35: Xi'an

36: Xiamen

37: Helsinki

38: Krakow

39: Whashington

40: Copenhagen

41: Hyderabad

42: Utrecht

43: Qingdao

44: Rotterdam

45: Edinburgh

46: Dublin

47: Madrid

48: Athens

49: Valencia

50: Singapore

Si unim totes les inicials de les ciutats obtenim:

GQNFOWTNFZKCQUGHFQAPMFLESBYJROVVJIXXHKWCHUQREDMAVS


STEP 4

<https://hackaton2024.useitapps.com/GQNFOWTNFZKCQUGHFQAPMFLESBYJROVVJIXXHKWCHUQREDMAVS>

```
In a well-defined field, with four sides of equal measure, there is a hidden point, that balances the whole square.
It's not in any corner, nor on the border will it be found, in the center is its lair, where will it be found?

In an ancient Roman library, an archaeologist found a scroll with an encrypted message. The message said: "In the
times of ancient Rome, a famous general and emperor developed a method to send secret messages to his allies. This
method was named in his honor and has been used for centuries in various forms of cryptography." The scroll also
contained an additional clue: "The name of this general is synonymous with the word 'emperor' in many languages."
```

You are surpassing me...
I have another way of doing things.
I usually track my information with a common AWS Service.
I do that just to tell my accomplice at what point or where i am...
Police thinks they got my car model. But Ford Ranger it is not.
Unlock next step with my car brand-model with something else...
47573768-ac54-4802-8b23-f3a80b6d54c6.



Un *div* amb un *title* ens mostrava que hauríem d'usar *aws kinesis*. Com que ja teníem feta la configuració del *cli*. Tan sols ens va fer falta fer un *aws kinesis list-streams*. Aquesta comanda ens mostrava un únic stream "info-stream" del qual podíem obtenir dades amb un *shard-iterator* i amb la comanda *aws kinesis get-records*.

Per automatitzar aquest procés vam fer un script de python del qual vam obtenir múltiples coordenades que vam afegir a un mapa interactiu. Si revisàvem els punts que havíem generat, hi podíem apreciar un quadrat perfecte a Bangkok. Seguint el que ens indicava el text de la pàgina web, vam obtenir les coordenades del punt central i ens vam situar-hi amb el google maps. Allí hi podien veure una casa amb el número 235 i un honda civic aparcats, pel que havíem trobat la marca i model del cotxe que necessitàvem.

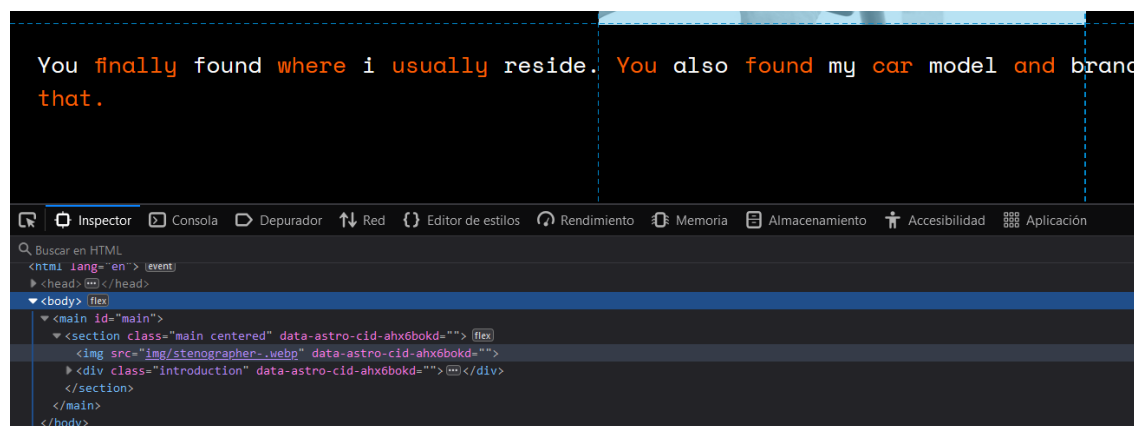
Amb aquestes dades i seguint el paràgraf de l'emperador, vam xifrar "Honda-Civic" amb el sistema Cèsar amb la clau de desplaçament 235, el que ens va servir per accedir al següent pas.

STEP 5

<https://hackaton2024.useitapps.com/lpoeb-Djwjd>

En aquest pas se'ns mostrava a la pantalla la imatge d'un estenògraf. Vam revisar el codi font i tota la pàgina i no vam trobar res. Llavors vam decidir investigar la imatge en si. La vam descarregar i li vam aplicar un filtre estenogràfic per veure si teníem alguna imatge dins de la pròpia. Així vam aconseguir eliminar la imatge principal i poder visualitzar només el codi QR.

Vam extreure els fitxers d'Amazon S3 i posteriorment vam observar com una de les carpetes que rebíem tenien una mida bastant diferent de la resta, vam decidir descomprimir-la i observar el contingut. El que vam fer va ser detectar que a cada carpeta teníem diferents fitxers amb hash com a nom. Llavors vam decidir recórrer els diferents directoris dins la carpeta descomprimida i observar si n'hi havia algun amb contingut diferent dels altres, fent això vam trobar una carpeta on teníem uns fitxers .txt que contenien com accedir al següent pas, entre altres dades.

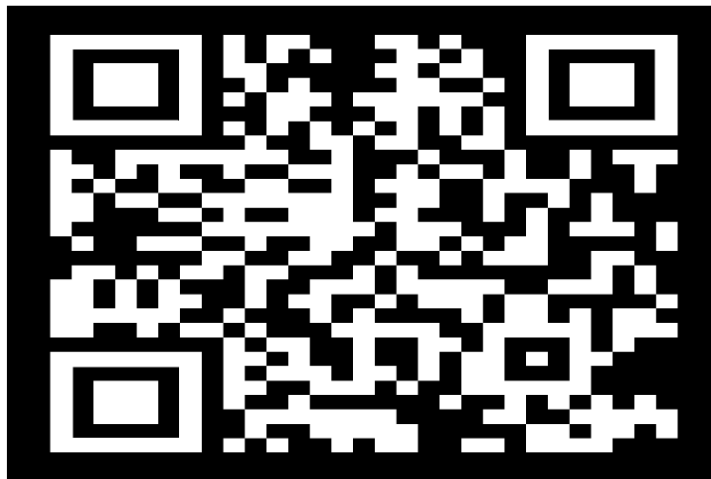
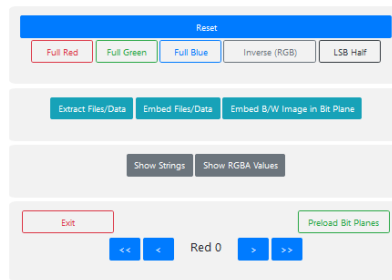


<https://hackaton2024.useitapps.com/img/stenographer-.webp>

<https://georgeom.net/StegOnline/image>

LSB-Half → Browse Bit Planes

Image Options



Extract QR: `arn:aws:s3:::compliancenames`

<https://docs.aws.amazon.com/cli/latest/reference/s3/>

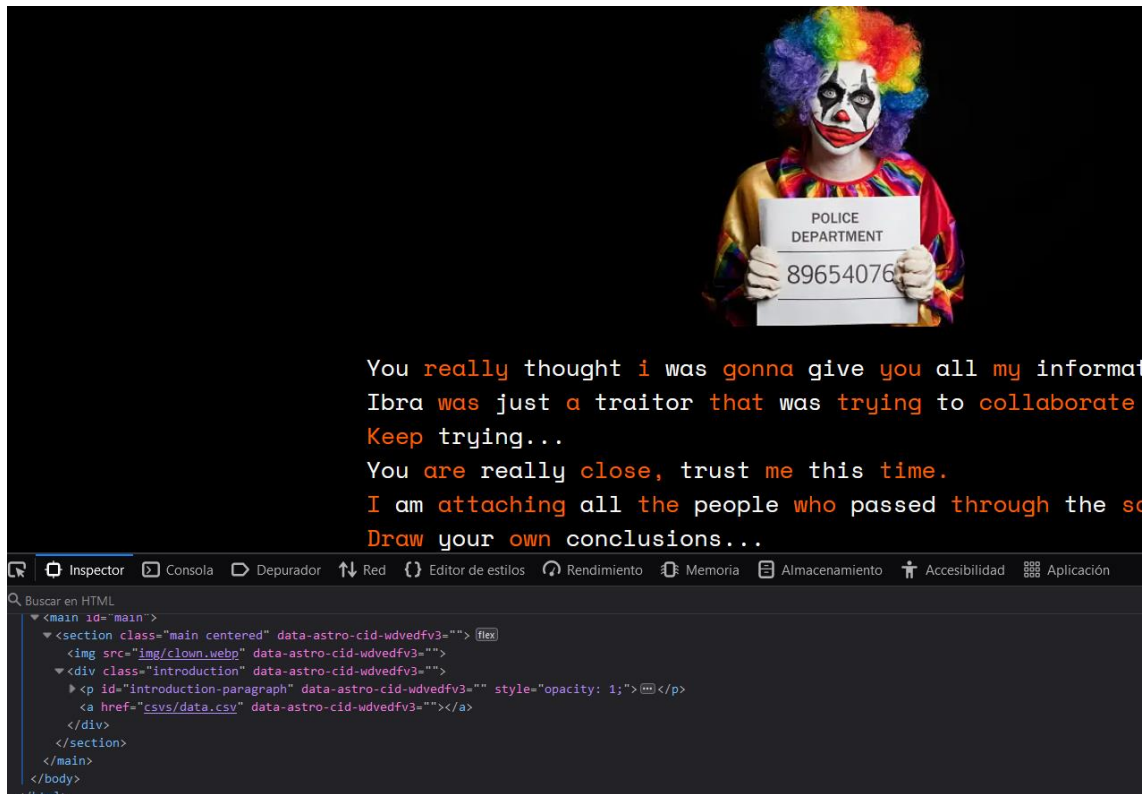
924d5efa-588a-42bc-9640-09c8abe9f239.zip

```
for dir in /; do for file in "$dir"; do size=$(du -k "$file" | cut -f1); if [ "$size" -eq 4 ]; then  
cat "$file"; fi; done; done
```

STEP 6

<https://hackaton2024.useitapps.com/f081ced9-2c7b-4505-973a-630979eb8100>

En aquest pas l'assassí ens adjuntava un fitxer en format .csv amb les dades de la gent que va passar per la zona aquell dia. I buscant pels usuaris vam observar que una de les files contenia un nom en format UUID. Llavors vam pensar que seria la ruta a la següent pantalla i així va ser.



<https://hackaton2024.useitapps.com/csvs/data.csv>

Row: 8a4398cf-896b-4d72-999c-4db47ad73400

FINAL STEP

<https://hackaton2024.useitapps.com/8a4398cf-896b-4d72-999c-4db47ad73400>

```
Unfortunately, it is the end of our beautiful
adventure.
One last step, and you got me.
Remember all what you learned from here.
You have enough information in the csv to discover
me, have fun...
```

Pistes:

- 2 fills
- Residència Bangkok

```
i have two little kids.
```

Per obtenir les dades que volíem, vam usar la llibreria de Python Pandas per filtrar les dades. Vam escollir entre les persones que tenien dos fills i que residien a Bangkok, seguint les pistes que havíem recollit anteriorment. Una vegada fet això vam trobar que posant l'ID d'una fila obteníem una nova pantalla amb la descripció de la persona i un número. Per comprovar si en teníem més així, vam fer un script en el qual per força bruta recorríem les files filtrades i llençàvem l'URL amb l'ID de cadascuna, després comprovàvem de quines rebíem un codi d'estat 200 i així vam obtenir totes les descripcions de les persones.

FINAL STEP PART 2

Per l'última part vam haver de fer servir els nombres que apareixien a les pantalles on hi havia la descripció de certes persones. En una d'elles apareixia un quadrat i amb aquesta pista i amb el vídeo que ens van passar, en el que parlava de Polibi, vam esbrinar que va inventar un sistema de xifratge fent servir una matriu on usant dos nombres obtenim una lletra. Finalment, una vegada vam obtenir tota la seqüència de lletres havíem de realitzar les permutacions necessàries per tenir el nom de l'assassí. Vam crear un script que segons un nom o cognom, amb les lletres sobrants trobava les possibles permutacions.

<https://hackaton2024.useitapps.com/196>

<https://hackaton2024.useitapps.com/757>

<https://hackaton2024.useitapps.com/1014>

<https://hackaton2024.useitapps.com/2259>

<https://hackaton2024.useitapps.com/2369>

<https://hackaton2024.useitapps.com/2741>

<https://hackaton2024.useitapps.com/4762>

<https://hackaton2024.useitapps.com/6005>

<https://hackaton2024.useitapps.com/6117>

<https://hackaton2024.useitapps.com/6183>

<https://hackaton2024.useitapps.com/6229>

<https://hackaton2024.useitapps.com/7595>

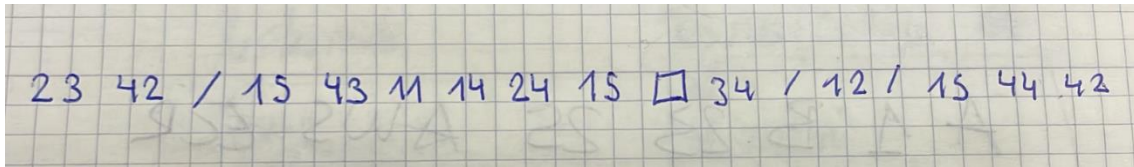
<https://hackaton2024.useitapps.com/8035>

<https://hackaton2024.useitapps.com/8403>

<https://hackaton2024.useitapps.com/8562>

<https://hackaton2024.useitapps.com/8929>

<https://hackaton2024.useitapps.com/9386>



Codi transcrit usant <https://cryptii.com/pipes/polybius-square>: HRESADIEOBETR --> Heriberto Seda.