UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Enginyeria de Sistemes TIC

Documentació del procés de desenvolupament de CTF

HackEPS2024 — Enginyeria de Sistemes TIC

TechTICs

November 24, 2024

Contents

1 Fase 1

- El primer pas va ser cambiar l'atribut de classe a <show> per mostrar la caixa de l'input per possar la contrasenya. A continuació, analitzant la metadata de la imatge vam descobrir que hi havia amagat un comentari en que hi afegia un patró de contrasenya amb una part que s'havia de completar amb les credencials generades al principi de la sessió.

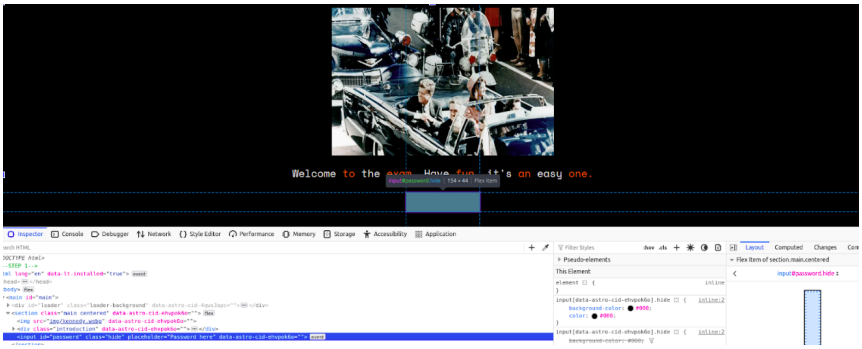

Figure 1: Foto de Kennedy.

Figure 2: Metadata.

- Després, anar al link de la resposta, substituir el path i fer-ho servir (en comptes de <exam>). Quedant de la següent manera

```
j9G2FtnXLti6vA6KTwsHL3ttzrFju6NYx8:50c1e2ce-7844-4857-80c4-ff4e9f3ea099
```

2 Fase 2

En aquest fase obtenim una pista a sobre de que tenim que escolter un audio. Així doncs:

- Inspeccionem la pàgina trobem un arxiu anomenat audio amb el path audio/audio.wav.
- Ho repdoduïm i ens adonem que a part del text narrat hi ha una subfreqüència. Per tant, vam representar son espectograma a l'audacity i vam obtenir un codi com podem veure a la imatge adjuntada.
- Amb aquestes dades, fem login a AWS ECR a partir de terminal amb la següent comanda:

Figure 4: Audacity espectograma.

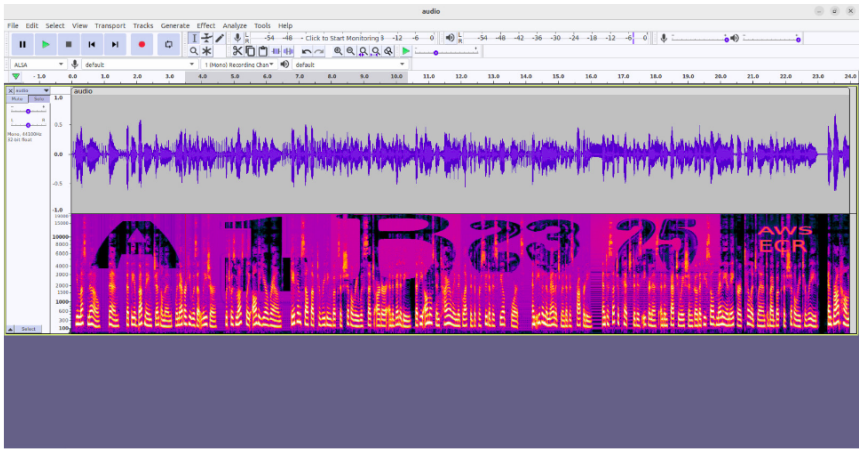

Figure 3: Audacity espectograma.

- Un cop dins, després de descarregar la màquina, cal accedir a un arxiu i de desencriptar el arxiu amb :

```
cd /
sudo gpg --decrypt secret_uuid.gpg
password = A1B2325
```

- Finalment, desencriptem l'arxiu i obtenim el següent path:

```
761c4303-6381-40dc-b2e9-413ae52b1664
```

3 Fase 3

Una vegada avanCem al següent step, trobem les sonates de Shakespeare a partir d'inspeccionar la pagina web que acabem de trobar i agafem el link que disposa per proporcionar el zip. En les quals hi han ciutats, que a partir de ajuntarles i agafant la primera lletra, aconseguim un conjunt de dades que podem fer servir com a url per avançar a la següent etapa.

Obtenint un enllaç com el següent:

```
https://hackaton2024.useitapps.com/
GQNFOWTNFZKCQUGHFQAPMFLESBYJROVVJIXXHKWCHUQREDMAVS
```

4 Fase 4

Després de tot aquest procés i d'haver aconseguit aquesta nova url, llegint el contingut de la pagina podem deduir una direcció d'un carrer que podem introduir en google maps. Amb aixo

ens trobem la seguent imatge:

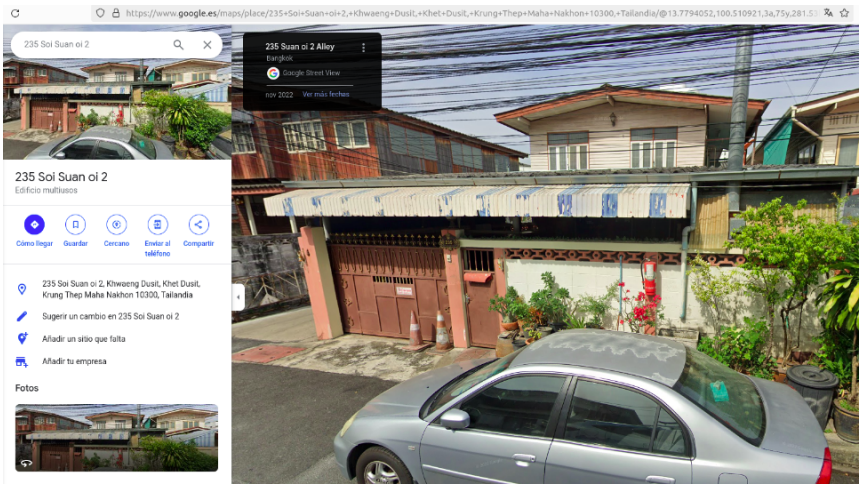

Figure 5: Imatge google maps.

Visualitzant la imatge i el text de la url, deduim que la paraula que necessitem per el enigma i que fem servir es el model de cotxe, el qual es, Honda Civic.

A més a més, segons el que es pot deduïr del text haviem de fer servir cèsar per encriptar el nombre de Honda-Civic. Aquest format funciona desplaçant tantes vegades com indiquem cada lletra de l'abecedari, com és módul 235 vam concloure que s'havia de moure una vegada cada lletra.

Per tant, la paraula Honda-Civic xifrada resulta com Ipoeb-Djwjd.

5 Fase 5

En aquest pas apareix una imatge d'un estenògraf, que podem descarregar i convertir a un codi QR gràcies al missatge en format d'estenografia, si mirem la informació d'aquest codi QR obtenim aquesta direcció d'AWS.

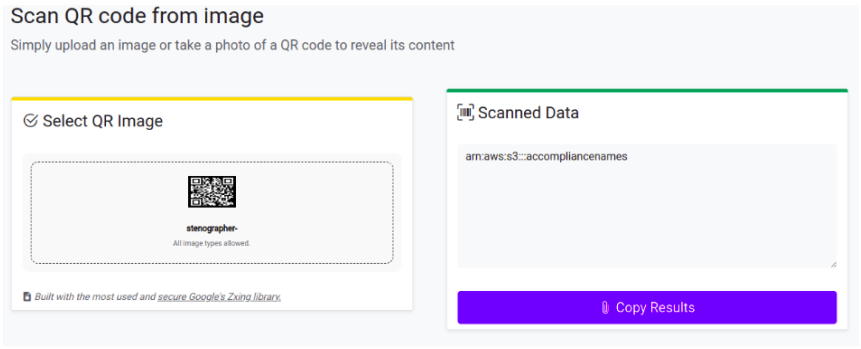

Figure 6: Imatge informació del QR.

Aqui podem trobar diversos fitxers ZIP on hi ha un més gran que la resta. Dins d'aquest veiem una gran quantitat de carpetes anomenades amb noms de persona i diversos fitxers .txt dins. Una d'aquestes carpetes pesa més que la resta ja que té la imatge que hem vist abans a google maps.

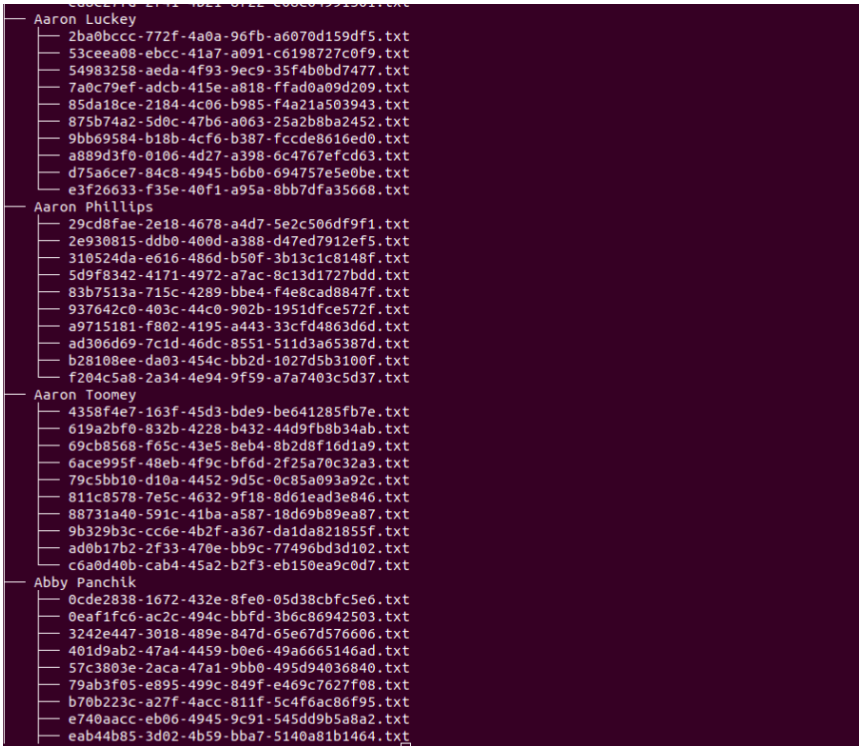

Figure 7: Diferents carpetes.

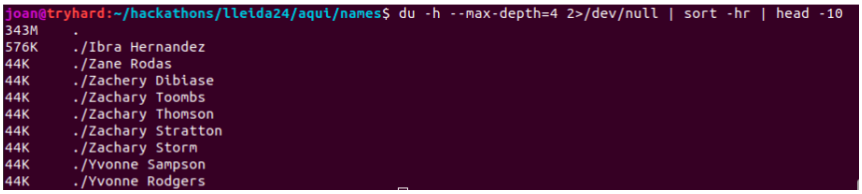

Figure 8: Carpeta amb més pes.

Aqui trobem un fitxer step.txt amb el qual podem afegir a la URL per passar a la fase 6.

6 Fase 6

Dins de la pàgina, inspeccionant el contingut, ens trobem un arxiu csv, que ens podem descarregar.

Dins, tenim el contingut de totes les persones presents en l'escena del crim.

7 Fase 7.1

A partir de la informació anterior, coneixem que les dades que hem de tindre en consideració dins dels perfils, són els fills que tenen, que han de ser 2 i la seva ciutat, que ha de ser Bangkok.

Dins d'aquests casos, tenint en consideració que les dades comencen un número més tard, les dades que ens coincideixen, si les introduïm en la web es donen informació, per poder traduir la informació final.

8 Fase 7.2

Un cop a partir d'obtenir totes aquestes parts, podem fer les permutacions necessàries, per modificar les dades i extreure el nom, que finalment era Heriberto Seda.