Mission:

Level: Easy

Introduction:

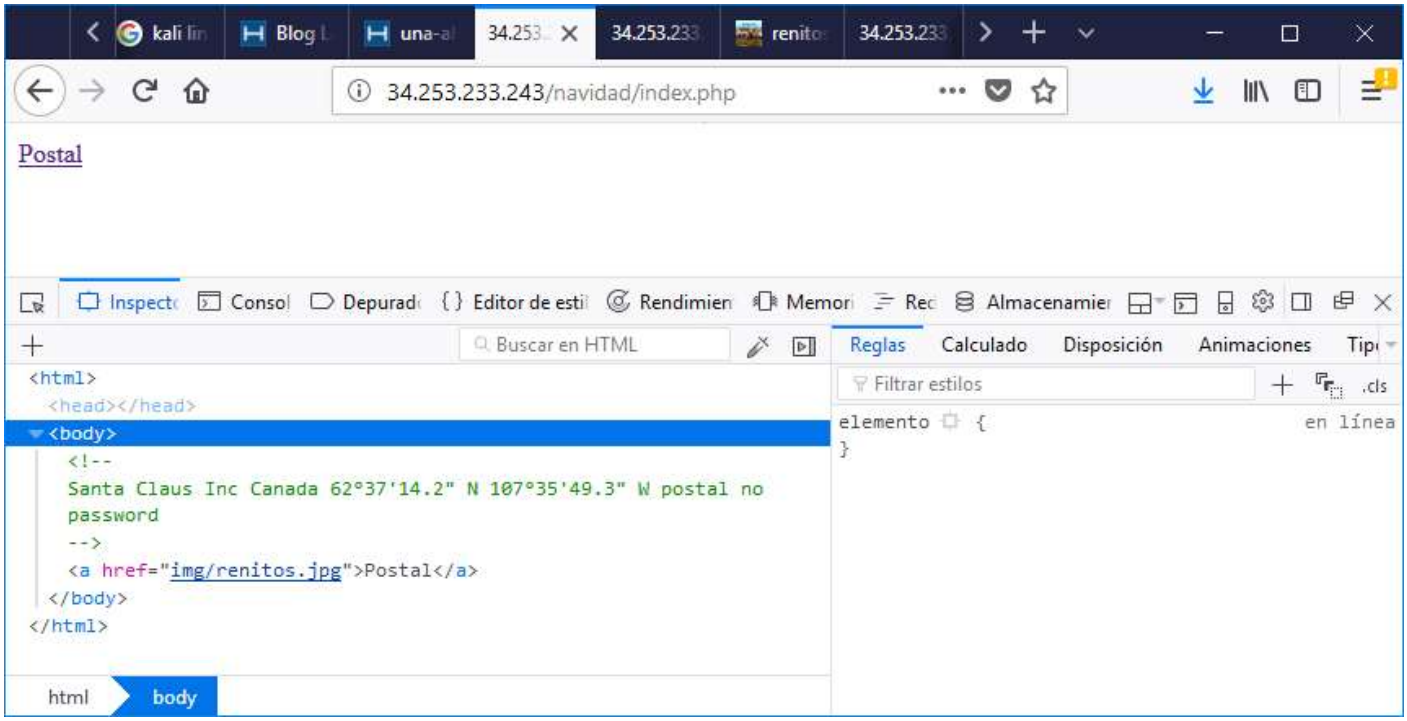
Hemos encontrado un servidor vulnerable de la empresa 'Santa Claus Inc' el cuál solo es accesible desde el país donde se encuentra la fábrica. Debemos de encontrar la manera de entrar y sacar la información oculta de la imagen que nos aparece.

Mucha suerte.

Additional Info:

URL found: http://34.253.233.243/navidad/index.php

Cuando cargamos la URL del reto, nos sale este enlace, en la parte del fuente ya nos dice que está en Canadá:

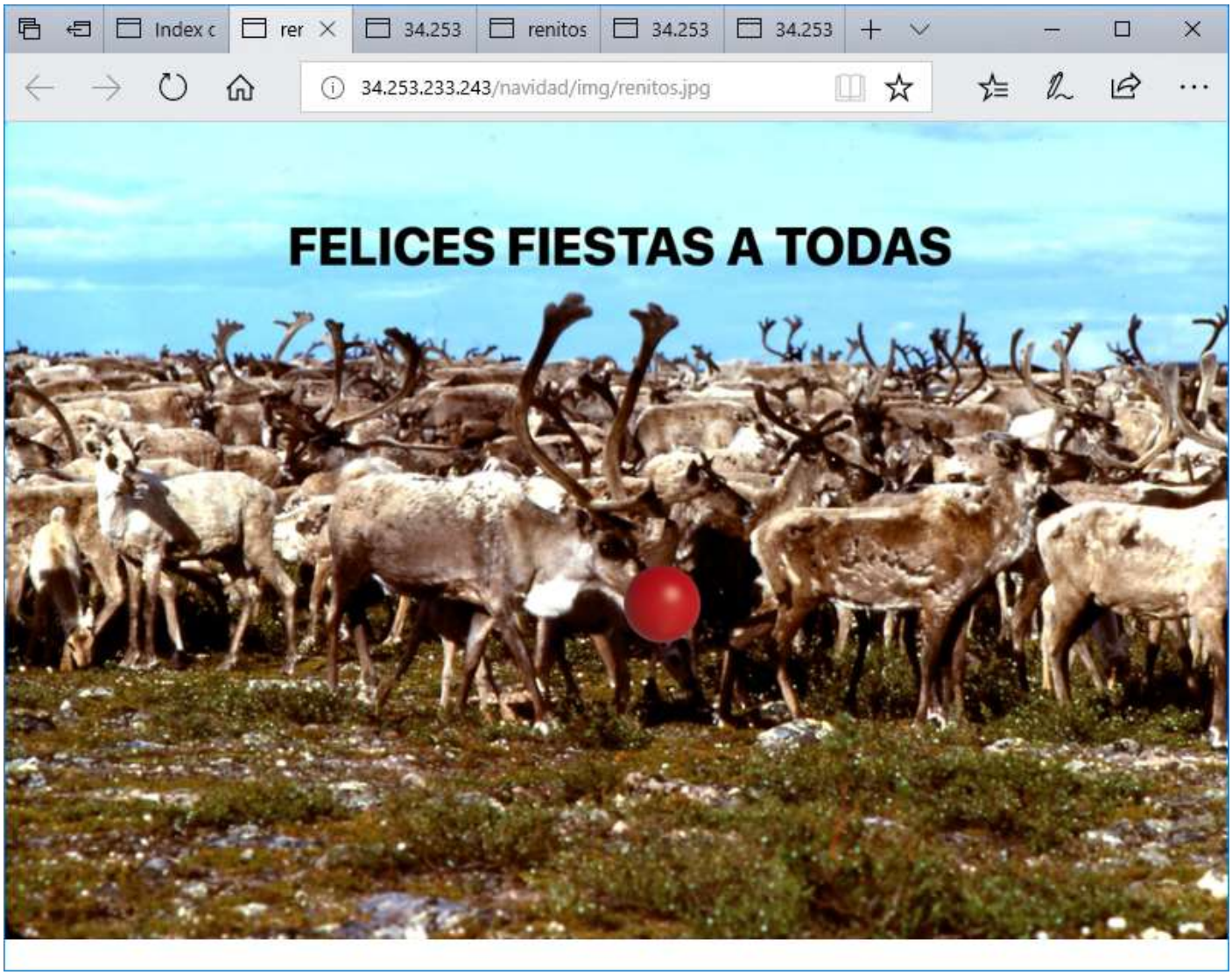


Si intentamos cargar la imagen, nos da error de permisos:

0

Por tanto, vamos a buscar un proxy anónimo de la lista de proxys que esté en Canada. Probando el que está subrayado (205.204.85.19:3128), entonces sí que nos devuelve la imagen:

IP Address	Port	Protocol	Anonymity	Country	Region	City	Uptime
47.52.144.78	3128	HTTPS	None	Canada	Ontario	Ottawa	97.7%
208.110.116.153	65301	HTTPS	High Anonymous	Canada	Alberta	Calgary	59.8%
137.74.168.174	8080	HTTPS	Anonymous	Canada	Quebec	Lachine	83.9%
205.204.85.19	3128	HTTP	None	Canada	Quebec	Laval	97.0%



Grabamos el fichero .jpg, y ahora intentamos sacar la información oculta.

- Vemos que visualmente no está escrita en ninguna parte, ni siquiera en muy pequeña fuente.
- Intentamos buscar el mismo fichero .jpg (a calidad 4:4:4 jpeg y 1599px de ancho) con los buscadores de imágenes de Internet, pero no lo encuentro igual de grande, con lo cual no me vale.

- Intentamos ver si dentro del propio fichero .jpg hay más de un fichero. Podemos meter dos ficheros juntos en el mismo archivo, que Windows solo mira hasta el primer final de fichero (ÿÙ), lo que haya después lo ignora. Intento buscar dos finales de fichero, o si después del primero hay algo, pero nada, está al final del fichero.
- Pruebo varios programas de esteranografía que son capaces de insertar información oculta en un fichero, pero no consigo encontrar ninguno. Al final pruebo con el programa "StegHide" versión (steghide-0.5.1-win32.zip), que funciona en línea de comandos:
    - steghide.exe extract -sf ../renitos.jpg
    - Genera un fichero de salida renitos.txt con esta cadena:
        - KVAU262NMVZHE6K7INUHE2LTORWWC427MFXGIX2IMFYHA6K7JZSXOX2ZMVQXEX3GOJXW2X2INFZXAYLTMVRX2===

```
C:\Users\Nacho\Downloads\steghide>steghide.exe extract -sf ../renitos.jpg
Anotar salvoconducto:
ya existe el archivo "renitos.txt". ¿lo sobreescribo? (s/n) s
anotó los datos extraídos e/"renitos.txt".

C:\Users\Nacho\Downloads\steghide>more renitos.txt
KVAU262NMVZHE6K7INUHE2LTORWWC427MFXGIX2IMFYHA6K7JZSXOX2ZMVQXEX3GOJXW2X2INFZXAYLTMVRX2===
```

    - La cadena solo tiene letras mayúsculas y números y =, vemos que es un Base32, buscamos un decodificador online y la respuesta en ASCII es:
        - UAM{Merry_Christmas_and_Happy_New_Year_from_Hispasec}

- Por tanto, esa es la FLAG.