Bocadillo Accidentado

Enunciado

> Esta mañana terminé de prepararme mi bocadillo de bacon pero me dí cuenta de que no me quedaba papel de aluminio para envolverlo. A la desesperada, cogí
> DOS folios que tenía cerca para envolverlo, sin darme cuenta de que era el papel donde tenía apuntada la flag.
> Después de comermelo intenté recuperarla pero había quedado completamente ilegible.
> Lo mas importante estaba en la segunda página, ayudadme a recuperarlo por favor.

Archivos

Envoltorio_Bocadillo.pdf

Solución

Al abrir el PDF nos damos cuenta de que tiene solo una página, y el enunciado menciona que debería de tener dos páginas.
Hay que conseguir acceder a la segunda página.

Según se describe en esta página el número de páginas que contiene un fichero PDF se almacena en hexadecimal con la estructura:

```
1 0 obj
<<
/Kids [3 0 R 11 0 R]
/Type /Pages
/Count 2
>>
endobj
```

Donde /Count indica el número de páginas del documento.
Si abrimos el PDF en un editor hexadecimal, vemos que efectivamente el número de páginas está puesto a 1.

```
$ xxd Envoltorio_Bocadillo.pdf
...
00016e50: 0a2f 4b69 6473 205b 3320 3020 5220 3137  ./Kids [3 0 R 17
00016e60: 2030 2052 5d0a 2f54 7970 6520 2f50 6167   0 R]./Type /Pag
00016e70: 6573 0a2f 436f 756e 7420 310a 3e3e 0a65  es./Count 1.>>.e
00016e80: 6e64 6f62 6a0a 0a32 3720 3020 6f62 6a0a  ndobj..27 0 obj.
...
```

Si cambiamos el número de páginas a 2 podremos acceder a la segunda página del documento.

Lo mas importante de la página es el mensaje en texto plano y el mensaje cifrado:

```
No sE que voy a hacEr cUanDo dEsCubraS eSto, esPero QUe El BOCaDilLoeSTUviErA
RiCO Al meNos. ErA DE bAcon Y quEsO auNQue Te intEresA mAS sabeR que es De
bAcon. Lo hIce A la pLanCha Y el qUeso ERa CHedDAr y me qUEdo muy fUnDiDo
cuidadO no TE MancHeSSSs.



;Gj6*o7_\Pv8l{UzH+uUZneSW?f&Xk{33&'Dp}5Wyizv
```

El texto en código plano está cifrado con un **Cifrado Bacon**, el enunciado y el mensaje repiten mucho la palabra *bacon*, y la manera de intercalar mayúsculas y minúsculas lo delata.

Para obtener el mensaje descifrado debemos eliminar los espacios y signos de puntuación del mensaje, después hay que sustituir las letras mayúsculas por 1`s (o A`s) y las minúsuclas por 0`s (o B`s), para generar un mensaje en alfabeto bacon y poder descifrarlo.

```
msg = "No sE que voy a hacEr cUanDo dEsCubraS eSto, esPero QUe El BOCaDilLo
eSTUviErA RiCO Al meNos. ErA DE bAcon Y quEsO auNQue Te intEresA mAS sabeR que es
De bAcon. Lo hIce A la pLanCha Y el qUeso ERa CHedDAr y me qUEdo muy fUnDiDo
cuidadO no TE MancHeSSSs."

msg = msg.replace(",","")
msg = msg.replace(".","")
msg = msg.replace(" ","")

salida = ["1" if c.isupper() else "0" for c in msg]
print(''.join(salida))
```

```
$ python3 script.py
10010000000000100100100101000010100001000110101110100100111001011011100010010111
01000100101001100100001000010110000100000100100010010010001001001000100110110011
00000110000001010100000001001110001011110
```

Usando [cyberchef]
desciframos el Bacon y conseguimos el mensaje: `SABES QUE NO SOLO EXISTE EL BASE SESENTAYCUATRO` lo que nos da a entender que los otros caracteres están cifrados en otro tipo de BaseXX, en este caso Base92.

Si lo decodificamos obtenemos

```
HFTFH{Jfv_Irxl_Vhgzyz_Vo_Y0xzwrool}
```

Se parece mucho al formato de una flag, pero con algún tipo de cifrado de sustitución.

Usando strings en el fichero descubrimos un mensaje en el comienzo de este:

```
$ strings Envoltorio_Bocadillo.pdf | more
Ha sido una buena idea usar un cifrado Hebreo >:)
%PDF-1.5
4 0 obj
/Filter /FlateDecode
/Length 2229
```

El cifrado en hebreo al que se refiere es el **Cifrado Atbash** y descifrándolo obtendríamos la flag.

Flag

```
SUGUS{Que_Rico_Estaba_El_B0cadillo}
```