Cibergal (10/11/2021)

Write up made by @informaticapau.

Reglas

- Cada reto tiene una puntuación en función de su dificultad. No hay que tener un máster para deducir que los más fáciles valdrán menos que los más difíciles.
- Algunos de los retos dispondrán de pistas (*Hints*) que restarán el número de puntos indicados a la puntuación actual del participante. Por lo tanto para poder acceder a las pistas es necesario haber resuelto previamente algún reto (que no te será muy complicado). Si se solicita una pista para un reto y finalmente el participante no es capaz de resolverlo los puntos se restarán igualmente de su puntuación total.
- Es posible que se abran nuevos retos y pistas conforme avance la competición, para darle más vidilla y tensión al asunto. (Os avisaremos para que no tengáis que hacer un F5 contínuo).
- El ganador será el participante que más puntos haya conseguido en el momento de la finalización del reto. En caso de empate este se resolverá teniendo en cuenta que usuario alcanzó antes la puntuación, que ser el más rápido (en este caso) es bien.
- La participación en el reto es individual. Si se detecta que 2 o más participantes están colaborando, podrían ser excluidos de reto, y los miraremos mal (con ojitos apretados ¬¬).
- No está permitido sabotaje entre participantes. Tenemos monitorización contínua para saber qué IP hace cosas malas para los demás participantes. También lo miraremos mal y podrá ser excluído del reto, aunque previamente le quitaremos todos los puntos para que quede con 0, muajajajaja. Los retos son muchos, es mejor que no pierdas el tiempo que si no no llegas.
- El formato de la flag que se debe introducir es el siguiente: cibergal{XXX}, somos tan buenos que en muchos retos ya es lo que teneís que encontrar, en otros tendréis que ponerlo vosotros (que tampoco se os van a caer los dedos de teclear).

Retos

Hola Flag

> Pon esta flag:
>
> cibergal{esto_es_una_flag}

Flag:

```
cibergal{esto_es_una_flag}
```

Checksum

> Por casualidad, al pasar frente al despacho de sistemas escuchas una conversación:
>
> - Cuando fue la última vez que cambiamos la clave del servidor?
> - No hace falta cambiarla, la clave del servidor es imposible de descubrir, y además cambia cada día! Es el resultado de hacer la función keccak de 224 bits sobre la fecha del día de hoy en el formato de fecha oficial de Anatolia. Quien podría saber eso?
>
> Cual es la clave del servidor?

Formato de la fecha en Anatolia: `YYYY-MM-DD`. [*No sé de dónde sacar esta info, pero confía en mí.*]

Keccak de 224bits de la fecha del CTF: `089c383363659ae305987199ff94abd0f6b0f1b529eb837f5696d331`.

Flag:

```
cibergal{089c383363659ae305987199ff94abd0f6b0f1b529eb837f5696d331}
```

Transcripción

> Creo que intenta decirme algo
>
> `message.wav`

El fichero de audio contiene el siguiente mensaje en código Morse:

```
HAZ UN MD5 DE LA PALABRA MORSE
```

"MORSE" en MD5: `fe73263580a8fc053b1f0dad16c22927`

Flag:

```
cibergal{fe73263580a8fc053b1f0dad16c22927}
```

Información oculta

> La respuesta a este reto es algo que no se ve a simple vista.
>
> `foto.jpg`

Tras revisar los metadatos o posibles archivos incrustados mediante esteganografía sin éxito probé a hacer un hex dump de la foto usando `xxd`:

```
0000c9d0: 6687 b208 2d18 98e8 2cf8 232d 969d 5663  f...-...,.#-..Vc
0000c9e0: 72d0 8cbb 4741 5760 a0f0 2be6 182d 4a38  r...GAW`..+..-J8
0000c9f0: 7486 31d4 bcbc 5631 c7c8 ffd9 4d69 6e69  t.1...V1....Mini
0000ca00: 6120 6369 6265 7274 6572 7261 2067 616c  a ciberterra gal
0000ca10: 6567 61                                  ega
```

Flag:

```
cibergal{Minia ciberterra galega}
```

Descodificando

> ¡Vaya! me han pasado esta cadena de caracteres, pero no sé qué significa. ¿Puedes ayudarme a descifrarla?
>
> `Codificaciones_encadenadas.docx`

Se nos entrega un fichero con el siguiente contenido:

```
00110011 00110010 00100000 00110110 00110101 00100000 00110110 01100101 00100000 00110101
00110100 00100000 00110110 00110100 00100000 00110011 00110000 00100000 00110101 00110101
00100000 00110100 00110010 00100000 00110100 01100100 00100000 00110111 00110011 00100000
00110101 00110101 00100000 00110110 00111000 00100000 00110011 00110011 00100000 00110100
01100011 00100000 00110100 00110100 00100000 00110110 00110001 00100000 00110100 00111000
00100000 00110011 00111000 00100000 00110111 00110111 00100000 00110011 00111001 00100000
00110011 00110110 00100000 00110111 00111000 00100000 00110110 00111001 00100000 00110110
01100001 00100000 00110100 00110101 00100000 00110100 01100101 00100000 00110110 00111001
00100000 00110110 00111001 00100000 00110011 00110011 00100000 00110111 00110111 00100000
00110011 00111000 00100000 00110100 00110100 00100000 00110111 00111000 00100000 00110101
00110111 00100000 00110100 00110011 00100000 00110100 00110011 00100000 00110111 01100001
00100000 00110100 00110111 00100000 00110110 00110111 00100000 00110011 00110111 00100000
00110011 00110010 00100000 00110110 00110101 00100000 00110110 00110010 00100000 00110011
00110100 00100000 00110100 01100110 00100000 00110011 00110110 00100000 00110011 00110010
00100000 00110111 00110111 00100000 00110111 00110110 00100000 00110100 00110001 00100000
00110100 00110100 00100000 00110011 00110111 00100000 00110100 00111001 00100000 00110100
01100110 00100000 00110011 00110111 00100000 00110110 00110101 00100000 00110101 00110111
00100000 00110110 00111000 00100000 00110111 00111000 00100000 00110011 00111001 00100000
00110111 00111000 00100000 00110011 00110001 00100000 00110100 00110100 00100000 00110101
00110000 00100000 00110111 00110000
```

Decodificado de binario:

```
32 65 6e 54 64 30 55 42 4d 73 55 68 33 4c 44 61 48 38 77 39 36 78 69 6a 45 4e 69 69 33 77
38 44 78 57 43 43 7a 47 67 37 32 65 62 34 4f 36 32 77 76 41 44 37 49 4f 37 65 57 68 78 39
78 31 44 50 70
```

Decodificado de hexadecimal:

```
2enTdOUBMsUh3LDaH8w96xijENii3w8DxWCCzGg72eb4O62wvAD7IO7eWhx9x1DPp
```

Decodificado de Base62:

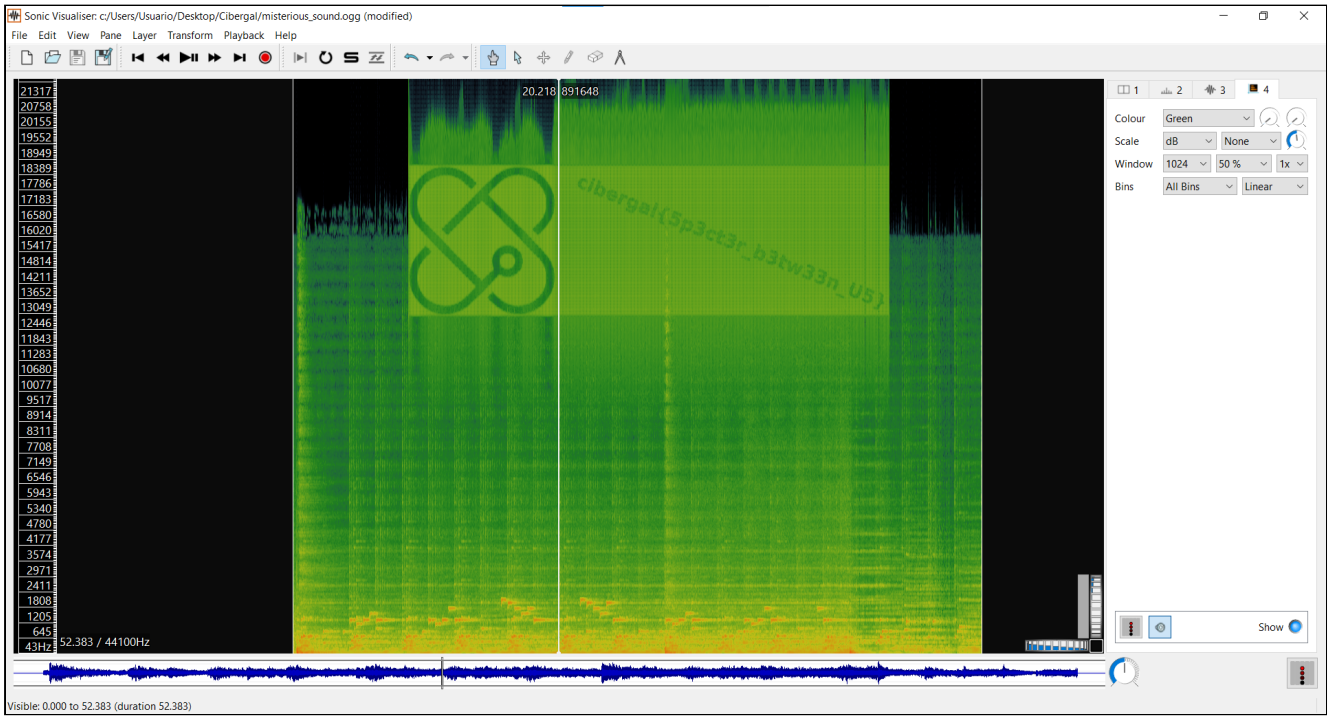
```
Y2liZXJnYWx7SGFzX2Rlc2NvZGlmaWNhZG9fbGFfZmxhZ30=
```

Decodificado de Base64:

```
cibergal{Has_descodificado_la_flag}
```

Expediente X

> Creo que intentan decirnos algo
>
> `misterious_sound.ogg`



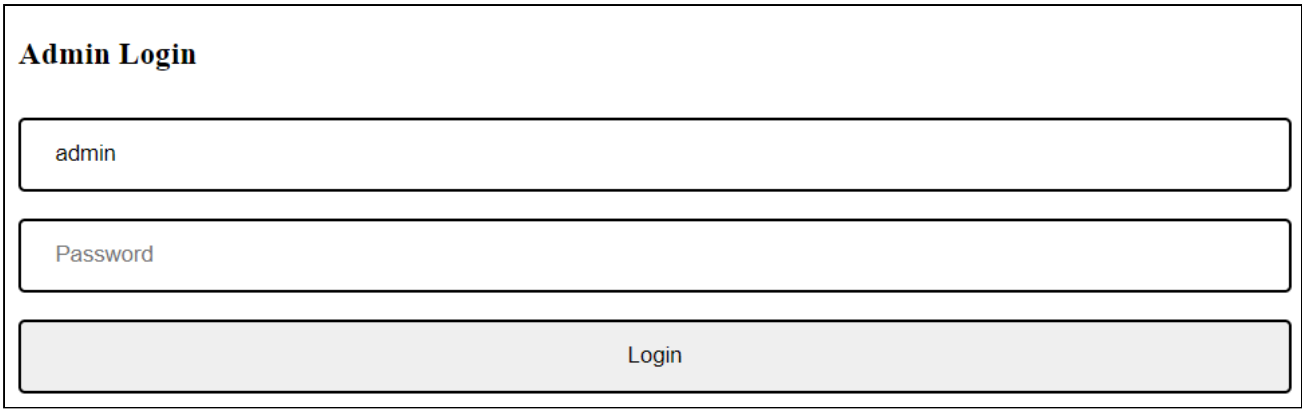
Usando Sonic Visualiser y mirando el espectro del fichero de audio encontramos la flag:

```
cibergal{5p3ct3r_b3tw33n_U5}
```

Entrevista

> La empresa Aura Technologies ha publicado un par de ofertas de trabajo que te interesan. Has probado a mandar tu currículum, pero no te han contestado. ¿Serías capaz de conseguirte una entrevista?
>
> < website >

En la página web no encontramos nada relevante. Buscando urls típicas se encuentra `admin.php` con un formulario como este:



Utilizando el usuario `admin` y la inyección SQL `' or ''='` nos aparece la flag:

```
cibergal{you_got_the_job}
```