Practica 1 - Let’s Go Cryptohacking

Equipo Caifanes

Integrantes

- Díaz Tinoco Gisel Maite (317020326)
- Vázquez González Melissa (317209468)
- Hernández Rojas Saúl Alejandro (315304433)
- Palma López Rossana (312047890)

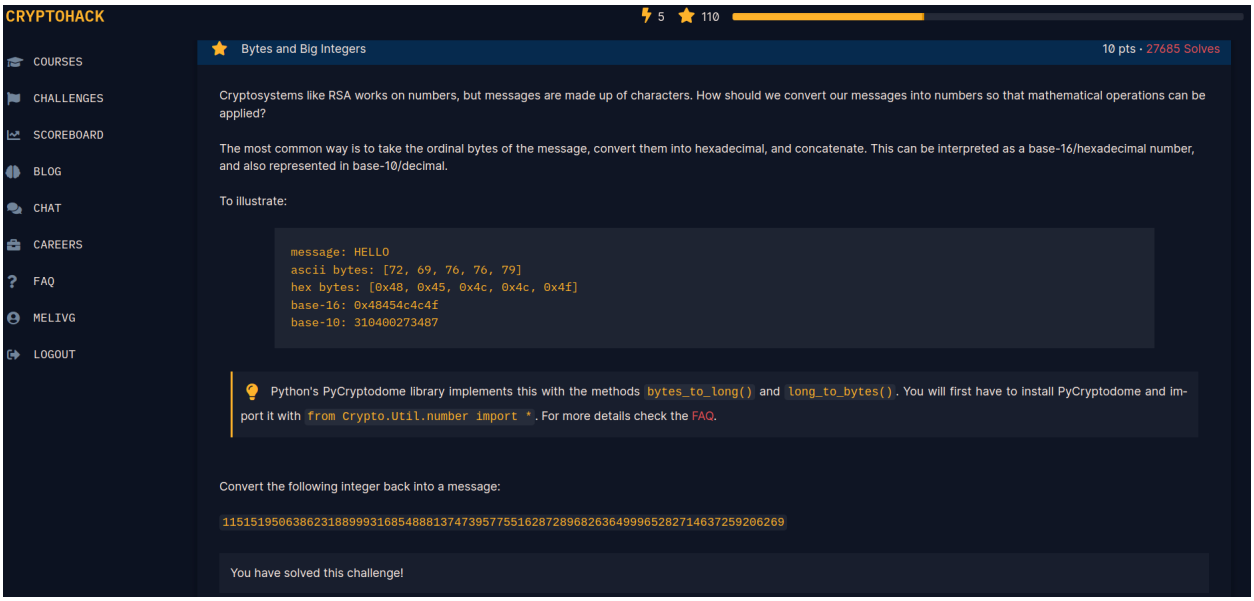
Introducción

La práctica se centró en la introducción a CryptoHack, una plataforma de entrenamiento en criptografía. Durante esta práctica, se abordaron varios conceptos fundamentales, incluyendo la codificación y decodificación de datos en diferentes formatos como ASCII, hexadecimal y Base64. Además, se exploró en detalle la operación XOR, que es fundamental en la criptografía simétrica.

Desarrollo

Dentro del equipo, cada quien realizó su curso por separado y a continuación presentamos las capturas de algunos de los ejercicios que se realizaron dentro de él con breves explicaciones sobre cómo se hicieron dentro del código anexado.

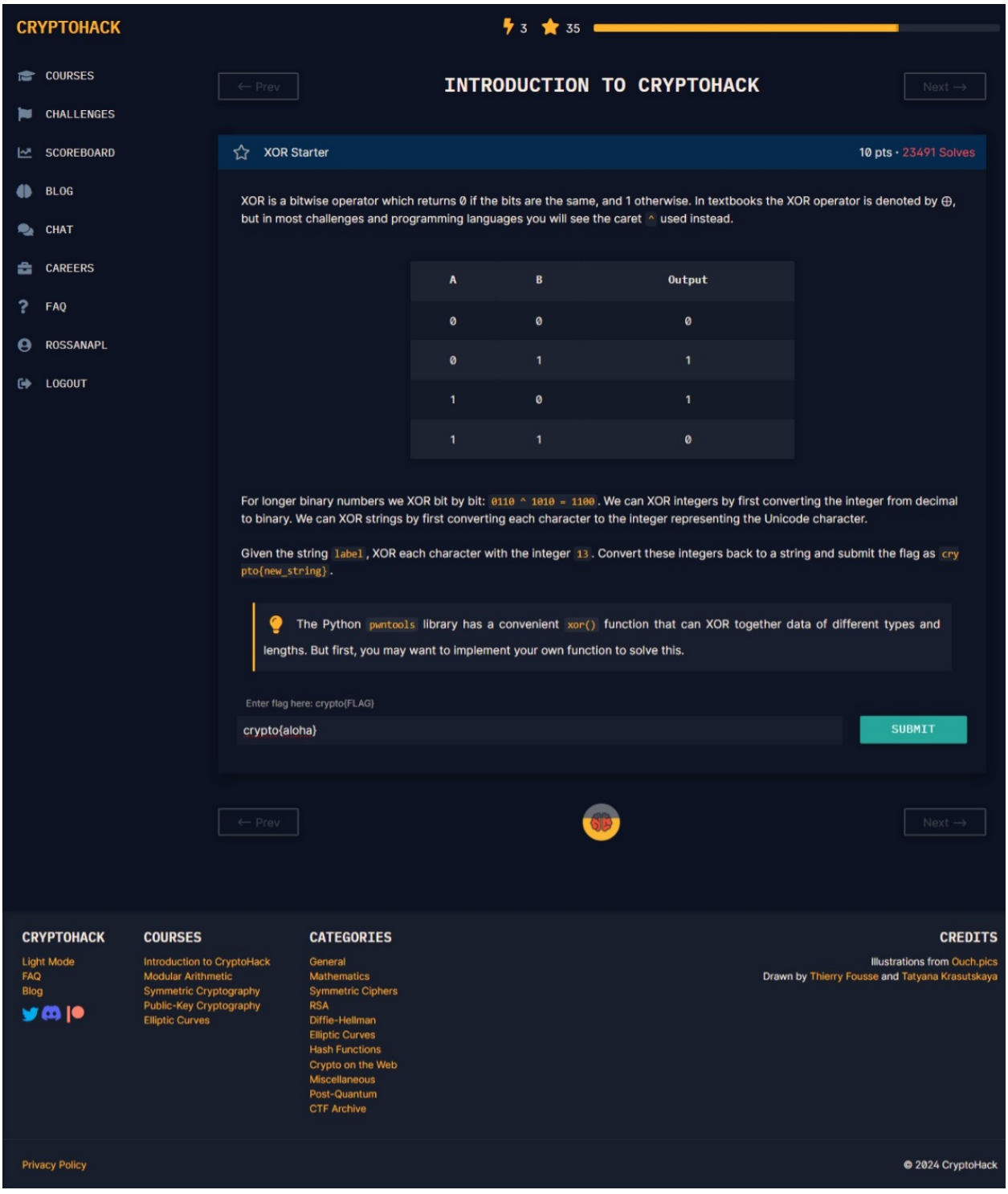
Ejercicio 6:



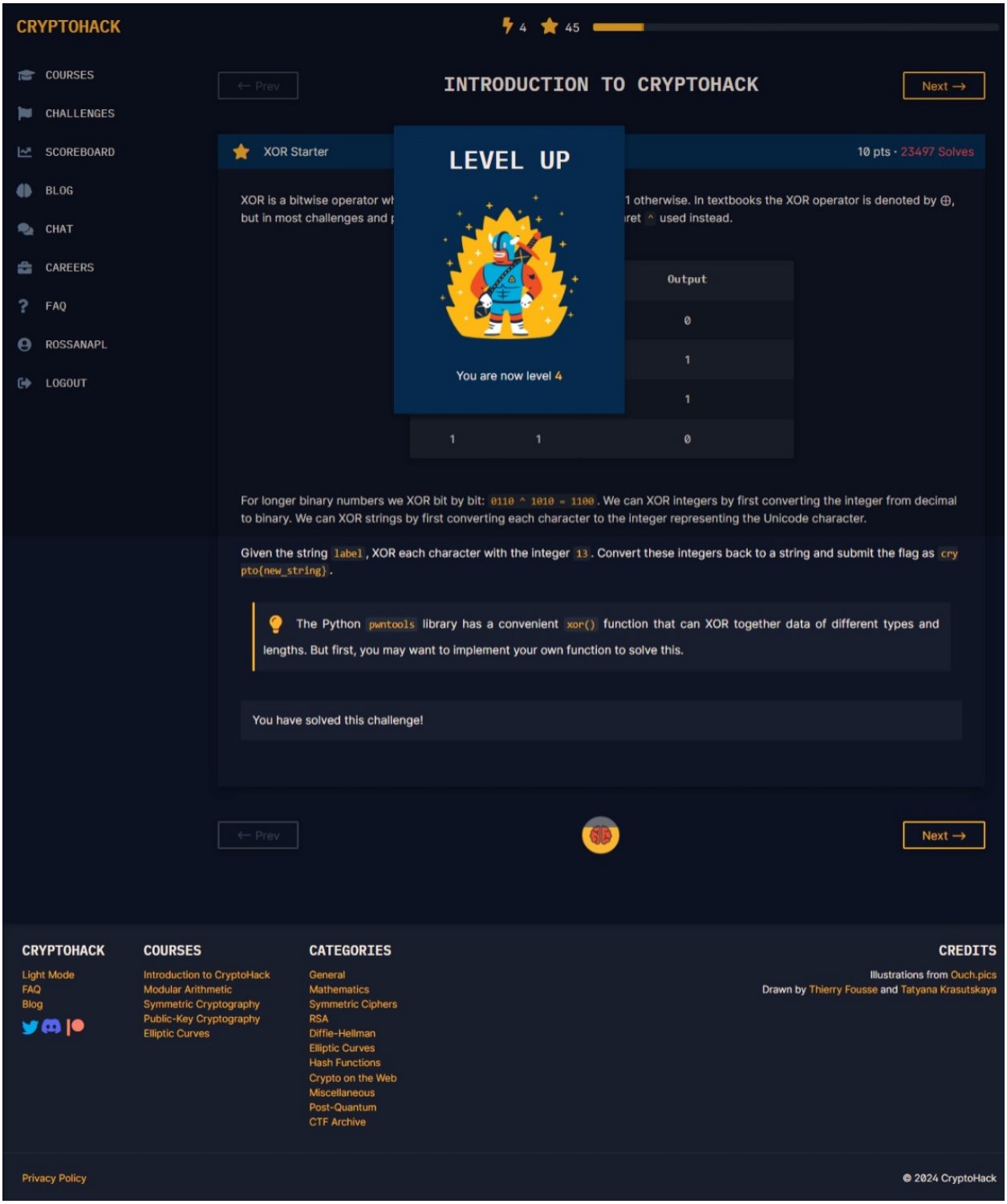

```
from Crypto.Util.number import *
intMessage = 11515195063862318899931685488813747395775516287289
print(long_to_bytes(intMessage))
```

FLAG : `crypto{3nc0d1n6_4ll_7h3_w4y_d0wn}`

Ejercicio 7 (Rossana Palma López):



Flag resultante Ejercicio 7



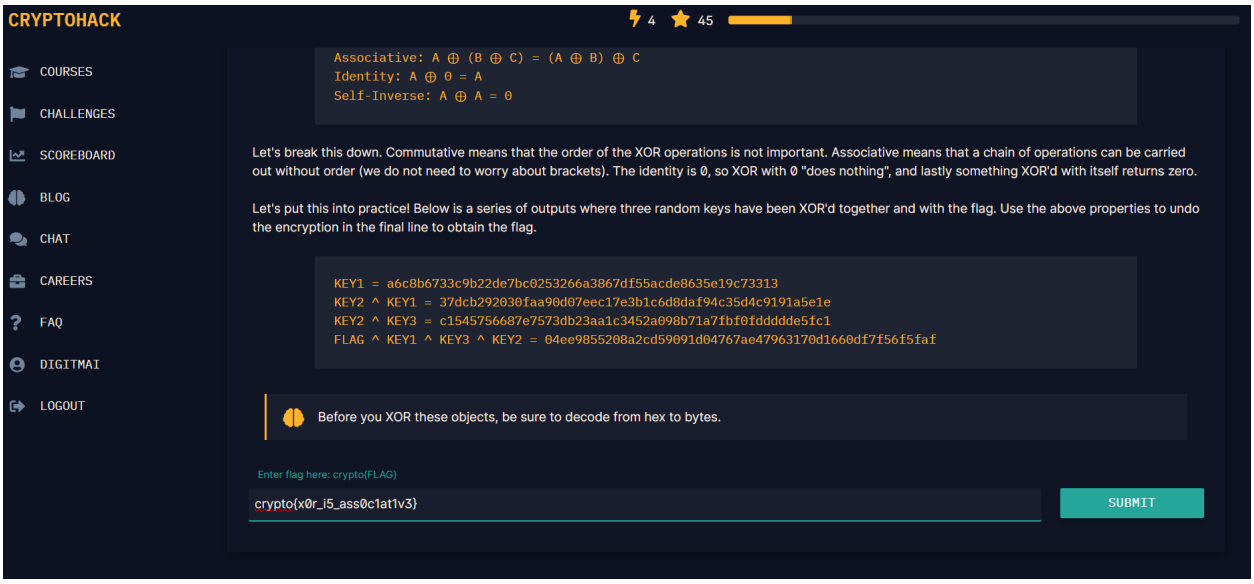
Captura Ejercicio 7 exitoso

FLAG: `crypto{aloha}`

Recurso empleado

```
str = "label"
#Define la funcion xor usando el operador ^
def XOR(A, B):
    return '{0:b}'.format(int(A,2) ^ int(B,2))
#Guardamos en un arreglo los codigos ascii de 'label'
ascii_array = [ord(c) for c in str]
#Cada codigo en ascii_array es transformado a su forma binaria
binary_array = [bin(c)[2:] for c in ascii_array]
#Creamos un nuevo arreglo donde se opera la representación binar
#con la representación binaria de 13
new_binary_array = [XOR(a,bin(13)[2:]) for a in binary_array]
#Obtenemos la representacion decimal de cada elemento en new_bi
result_ascii = [int(x, 2) for x in new_binary_array]
#Guardamos el nuevo string resultante de xor 'label' con 13
result_string = "".join(chr(i) for i in result_ascii)
#impresiones de verificación
print(binary_array)
print(new_binary_array)
print(result_ascii)
#Impresion del nuevo string
print(result_string)
```

Ejercicio 8:



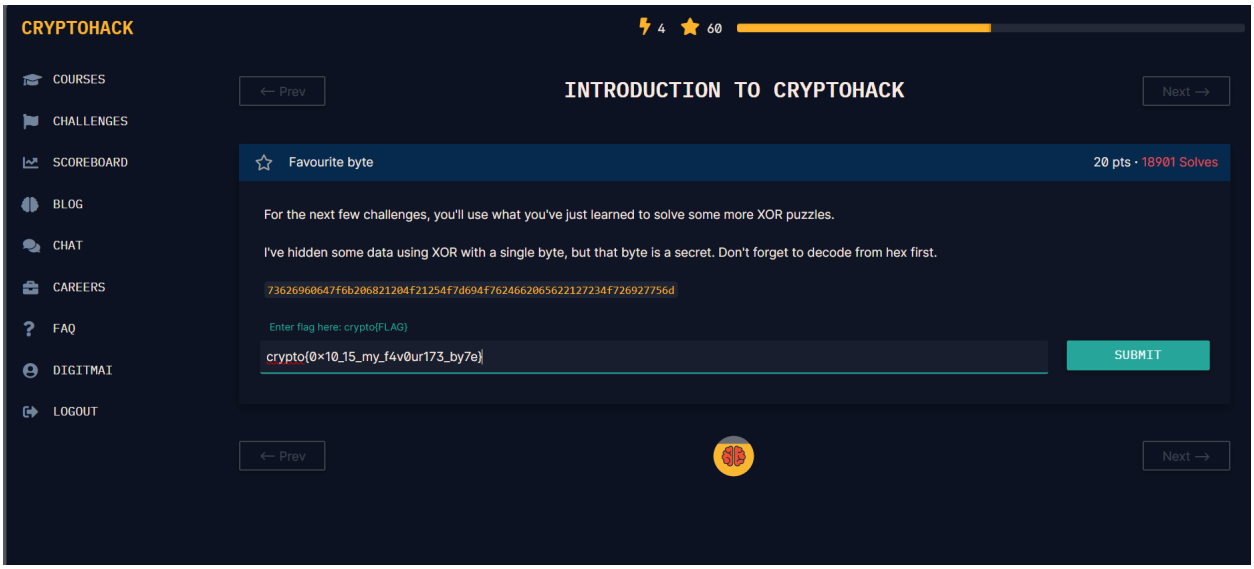
FLAG: crypto{x0r_i5_ass0c1at1v3}

Recurso empleado:

```
from pwn import xor


k1 = bytes.fromhex("a6c8b6733c9b22de7bc0253266a3867df55acde8635e
k21 = bytes.fromhex("37dcb292030faa90d07eec17e3b1c6d8daf94c35d4c
k23 = bytes.fromhex("c1545756687e7573db23aa1c3452a098b71a7fbf0fc
all = bytes.fromhex("04ee9855208a2cd59091d04767ae47963170d1660df
# Por la propiedad de inverso obtenemos k2 a partir de k21 que t
k2 = xor(k21, k1)
k3 = xor(k23, k2) # Ya teniendo el valor de k2, de igual manera
# Teniendo el valor de cada key independiente, podemos obtener e
# Notamos que no debe de preocuparnos el orden en el que se llev
# Ya que XOR es asociativa
flag = xor(xor(all, k2), xor(k3, k1))
print(flag.decode())
```

Ejercicio 9:

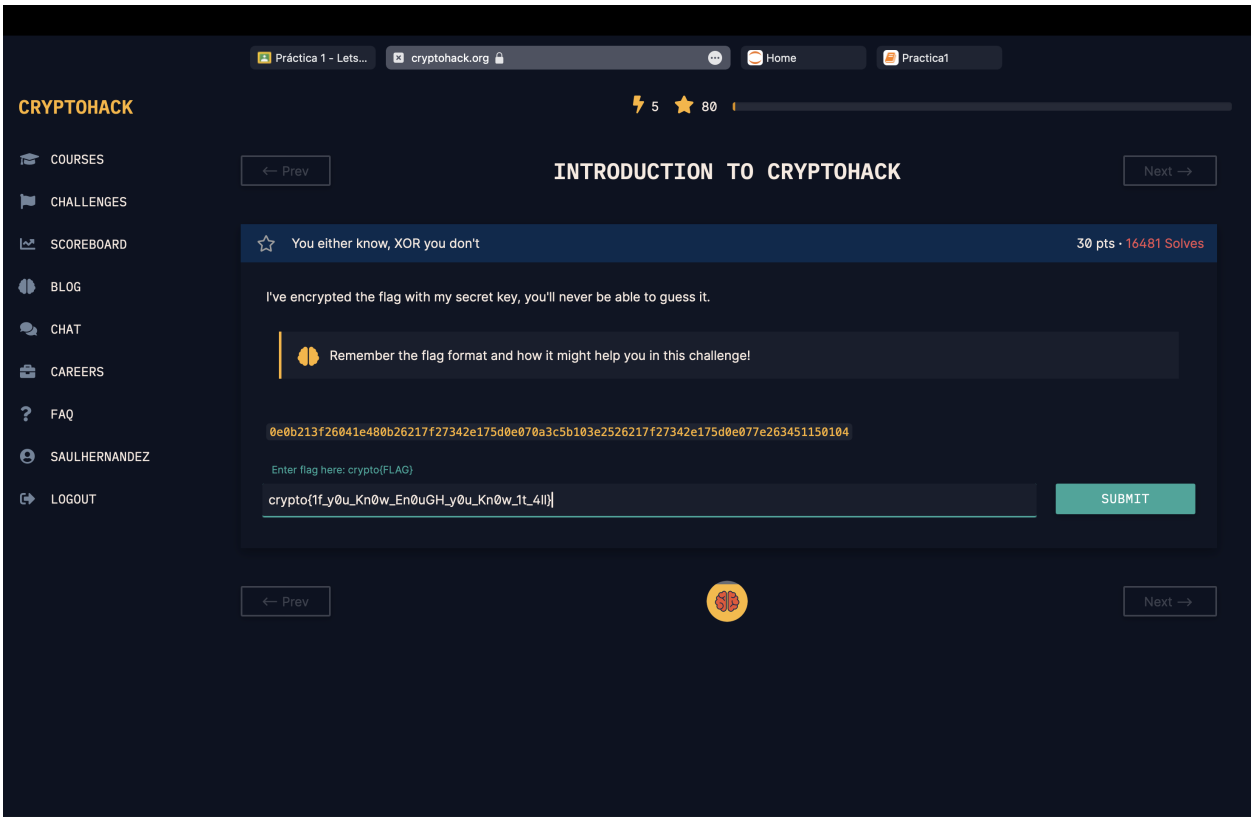


FLAG: crypto{0x10_15_my_f4v0ur173_by7e}

Recurso empleado:

```
dat = bytearray.fromhex("73626960647f6b206821204f21254f7d694f762
# Como no sabemos que byte se usó, intentamos todos por fuerza b
for num in range(256):
    par = [chr(p^num) for p in dat]
    flag = "".join(par)
        # Como sabemos el formato de las banderas, sabemos cuand
    if flag.startswith("crypto"):
        print(flag)
        break
```

Ejercicio 10



crypto{1f_y0u_Kn0w_En0uGH_y0u_Kn0w_1t_4ll}

Recurso empleado:

```
from pwn import *
# Se tomaron los bytes de el hex proporcionado
input = bytes.fromhex("0e0b213f26041e480b26217f27342e175d0e070a3
#primero, se hizo un xor entre los bytes y la estructura general
print(xor(input, "flag{}"))
# Con esto obtuvimos como resultado una cadena que contenía la c
#la cual tomamos como llave para finalmente obtener la bandera c
print (xor (input, "myXORkey") )
```

Curso Completado:

Nombre: Gisel Maite Díaz Tinoco

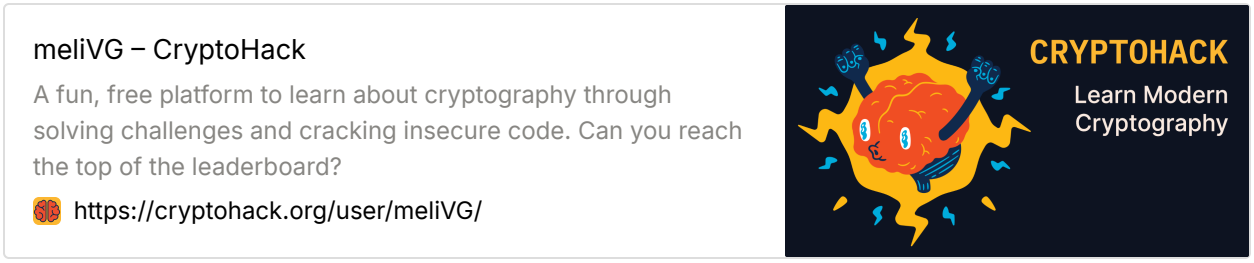
No. de cuenta: 317020326

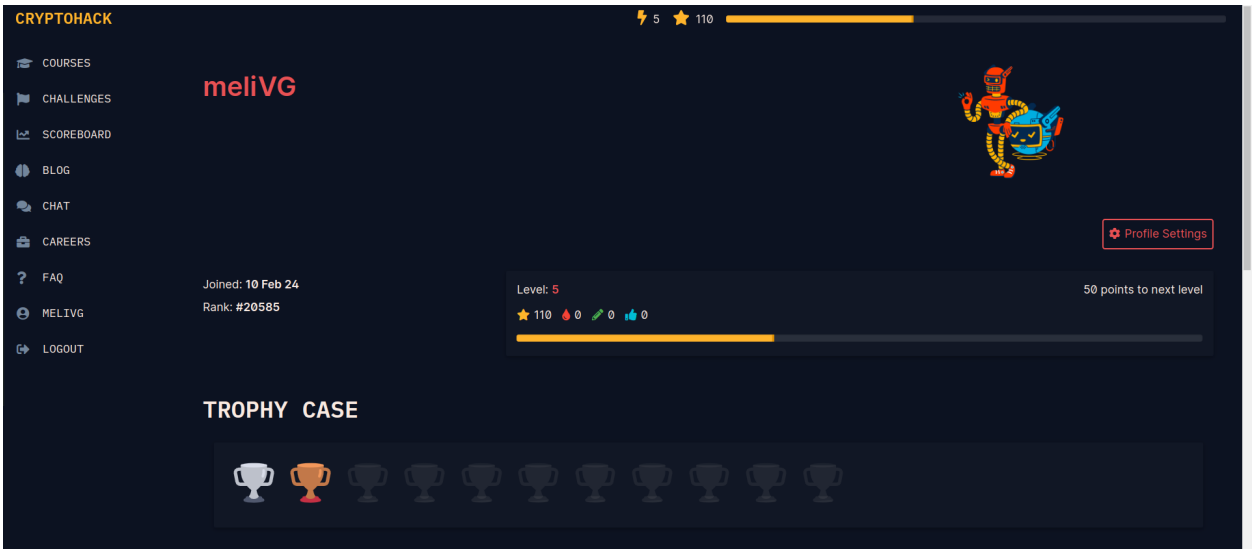
URL: CryptoHack – digitmai

Nombre: Melissa Vázquez González

No. de cuenta: 317209468

URL:

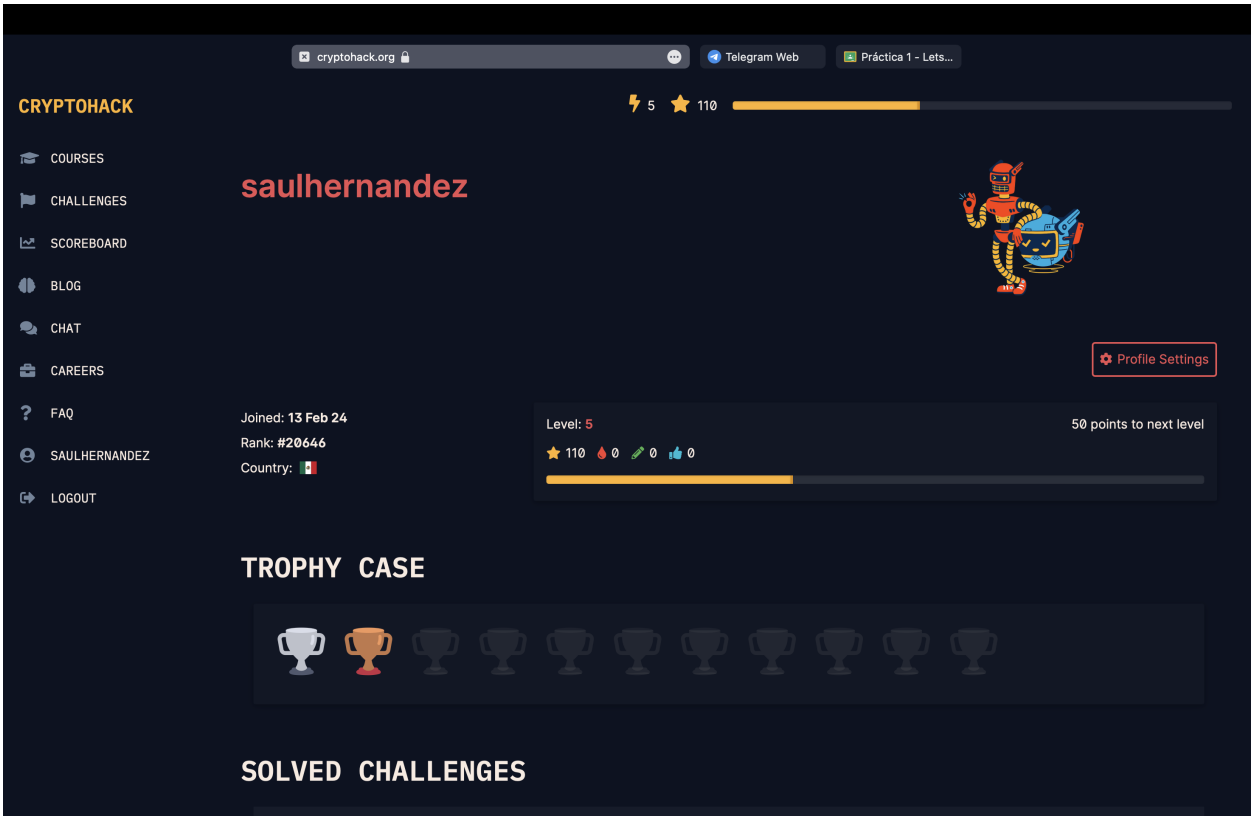




Nombre: Hernández Rojas Saúl Alejandro

No. de cuenta: 315304433

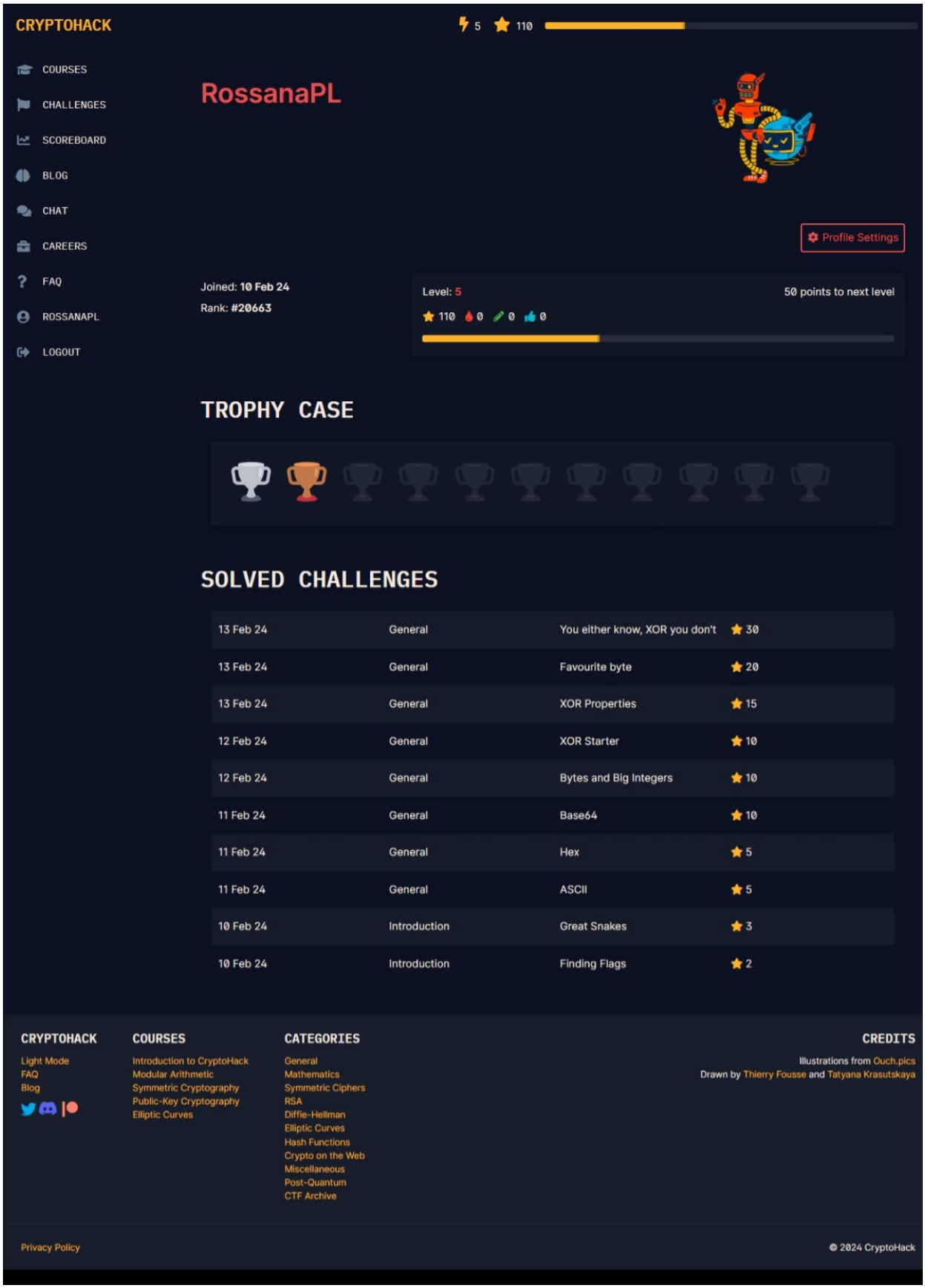
URL: https://cryptohack.org/user/saulhernandez/



Nombre: Rossana Palma López

N° Cuenta: 312047890

URL: https://cryptohack.org/user/RossanaPL/


CRYPTOHACK
5
110
COURSES
CHALLENGES
SCOREBOARD
BLOG
CHAT
CAREERS
FAQ
ROSSANAPL
LOGOUT
RossanaPL
Profile Settings
Joined: 10 Feb 24
Rank: #20663
Level: 5
50 points to next level
110 0 0 0
TROPHY CASE
SOLVED CHALLENGES
13 Feb 24 General You either know, XOR you don't 30
13 Feb 24 General Favourite byte 20
13 Feb 24 General XOR Properties 15
12 Feb 24 General XOR Starter 10
12 Feb 24 General Bytes and Big Integers 10
11 Feb 24 General Base64 10
11 Feb 24 General Hex 5
11 Feb 24 General ASCII 5
10 Feb 24 Introduction Great Snakes 3
10 Feb 24 Introduction Finding Flags 2
CRYPTOHACK
Light Mode
FAQ
Blog
COURSES
Introduction to CryptoHack
Modular Arithmetic
Symmetric Cryptography
Public-Key Cryptography
Elliptic Curves
CATEGORIES
General
Mathematics
Symmetric Ciphers
RSA
Diffie-Hellman
Elliptic Curves
Hash Functions
Crypto on the Web
Miscellaneous
Post-Quantum
CTF Archive
CREDITS
Illustrations from Ouch.pics
Drawn by Thierry Fousse and Tatyana Krasutskaya
Privacy Policy
© 2024 CryptoHack

Investigación

- **Malware:** Son las aplicaciones o código que se pueden presentar en distintas formas (un correo electrónico de phishing, un archivo o unidad USB infectada, etc.) y se usan de manera maliciosa para dañar, alterar el dispositivo y muchas veces, obtener acceso a tu información personal.
- **Spam:** Se le dice al tipo de correo que es enviado a usuarios de manera anónima y masiva. El contenido de los correos spam puede variar desde publicidad, engaños, estafas, spam con malware.

Conclusiones

Creemos que el curso fue una manera interactiva de acercarnos a estos conceptos básicos que nos van a servir más adelante, además, de repasar o volver a empaparnos en la sintaxis de Python, que como también sabemos, vamos a tener que seguir usando a lo largo del curso.

En cuanto a las dificultades, fue difícil lograr instalar las herramientas necesarias de manera correcta en las computadoras de todas las personas en el equipo. También fue un poco complicado manejar todos los tipos de datos involucrados al momento de operarlos ya que en Python no existen funciones por defecto para operar hexadecimales con binarios.

Punto Extra: 👾

Preguntas Ep: 000 - *Operation Aurora*

1. **¿Qué sucedió el 14 de Diciembre de 2009 en Google?**

   El 14 de diciembre, a un empleado de Google le llegó un mensaje con un link. Cuando le dio click, se le empezó a descargar malware a su computadora. Así, los atacantes se metieron a la red de Google.

2. **¿En qué consiste el proyecto Aurora?**

   Fue la respuesta que tuvo Google hacia el ataque.

3. **¿Qué relevancia tiene el nombre "Aurora"?**

   Es el nombre del barco de guerra que disparó un misil y dio inicio a la revolución rusa. Así como este barco marcó las décadas siguientes a su disparo, la operación Aurora hizo lo mismo en el mundo de la ciberseguridad.

4. **Describe en tus propias palabras ¿qué es el análisis forense?**

   Es analizar el hardware afectado por un malware, específicamente el disco duro.

5. **¿Qué es un Galimatías?**

   Es un algo que no tiene mucho sentido y es difícil de entender.

6. **¿Cómo entró en acción el equipo de Google para erradicar el ataque?**

   Se basó en juntar a expertos en ciberseguridad de todo el mundo en el campus, analizar el hardware de las computadoras infectadas, y finalmente reiniciar la información de acceso de todos las las personas empleadas en la empresa. Logrando así eliminar al atacante de su red.

7. **¿De dónde provenía el ataque?**

   De China, se tomó como un ataque del gobierno Chino hacia Estado Unidos.

Preguntas Ep: 002 - ***Threat Analysis Group***

1. **¿Internet está lleno de personas que intentan hacer cosas malas? ¿Cuál es el deber por parte del equipo de Google?**

   Toni Giswani, manager de ingeniería en seguridad, dijo que sí. Su trabajo es entender quienes son los atacantes y cómo operan para prevenir ataques.

2. **Menciona algunas amenazas monitoreadas por Google**

   vigilan amenazas al gobierno, amenazas financieras como ransomware y amenazas de desinformación, donde grupos pretenden esparcir datos falsos.

3. **¿Qué significa *TAG*? ¿Qué tipo de contenido bloquea?**

   Significa Threat Analysis Group. Bloquea ransomware, mensajes de fishing.

4. **¿Qué es WannaCry? Explica brevemente lo que hace y de donde proviene**

Es un ataque de ransomware, los atacantes secuestran la computadora de la víctima y piden un rescate para liberarla. Esta vez los responsables fueron los norcoreanos.

5. **Con tus propias palabras, ¿qué es el phishing?**

   Es un ataque en donde se tienta a al usuario con contenido llamativo que lo convence de entrar a un enlace malicioso que podría robarle su información.

Referencias:

1. ¿Qué es el malware? Definición y tipos | Seguridad de Microsoft
2. ¿Qué es Spam? (uach.mx)
3. ¿Qué es el Spam? | Enciclopedia de Kaspersky