Universidad de Talca
Facultad de Ingeniería
Departamento de Ciencias de la Computación

Seguridad Informática

Laboratorio 5

Erik Regla
eregla09@alumnos.utalca.cl

12 de julio de 2020

Índice

1. Actividades

Para esta actividad deberá crearse una cuenta en el portal Hack The Box (https://www.hackthebox.eu/).

1.1. Desarrollo

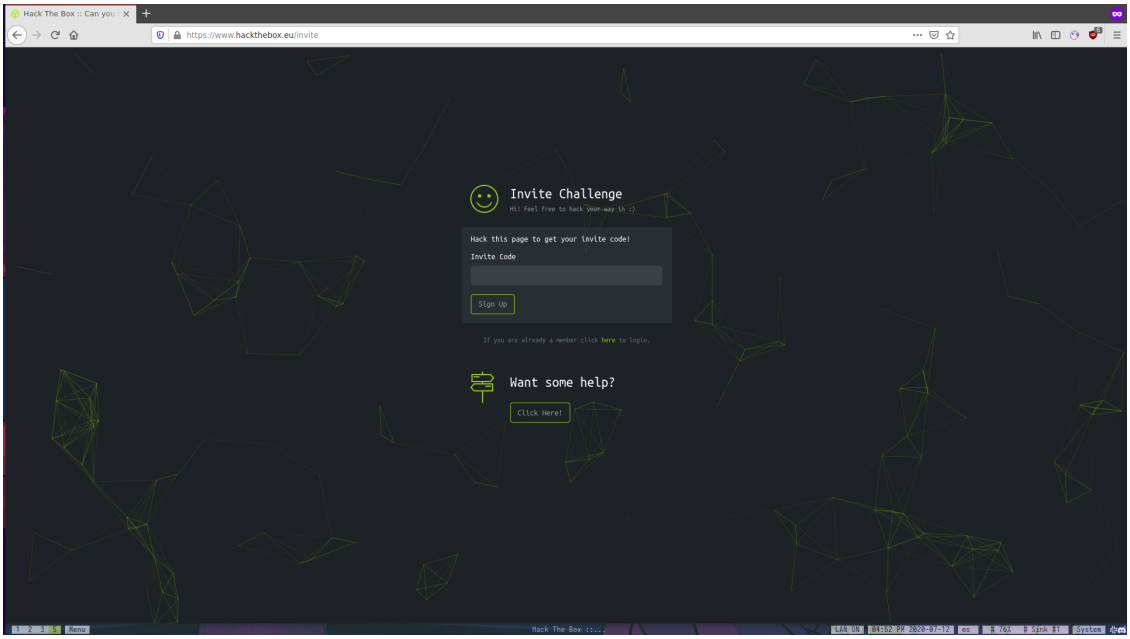

Figura 1: Al ingresar para crear la cuenta, se solicita utilizar un código de invitación, sin embargo no se explicita de donde este ses obtenido.

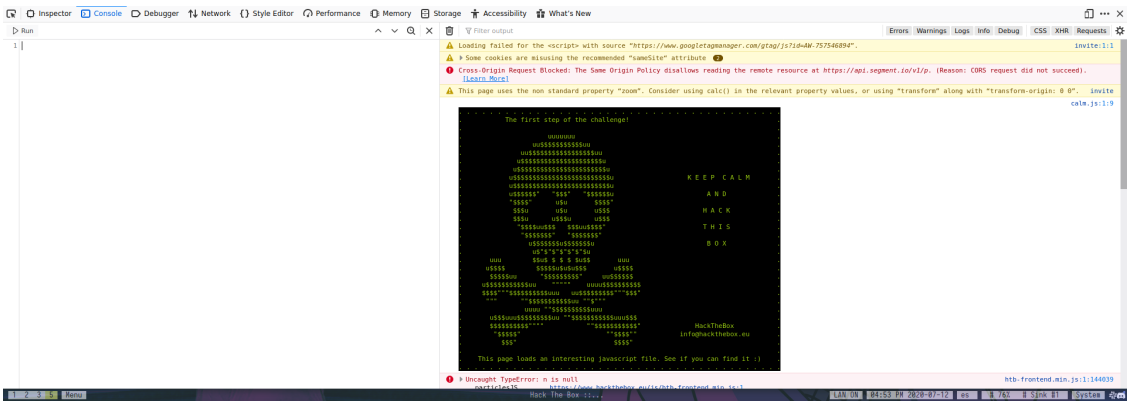

Figura 2: El primer intento consiste en ver si la consola entrega alguna información interesante. Sin embargo, somos bienvenidos con un mensaje de buscar algun archivo interesante dentro de los scripts descargados.

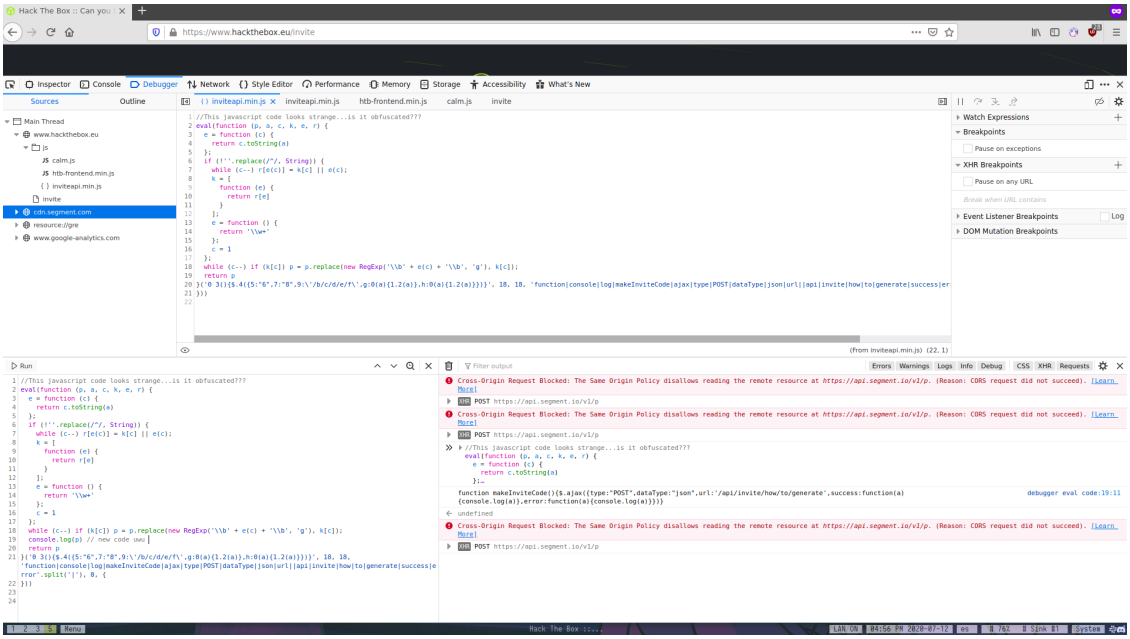

Figura 3: El archivo encontrado (extremadamente obvio por cierto) pertenece a un código obfuscado. Ahora, esta ejecución per-se no es real. Cuando un código es obfuscado para luego ser ejecutado suele tener un proceso de carga en etapas posteriores, sin embargo este código nunca es ejecutado. Por tanto procedemos a ejecutar el código y ver su salida (aunque normalmente esto no se hace ya que si no sabes con seguridad que hace, es posible que estés cayendo en un honeypot si no tienes el entorno aislado).

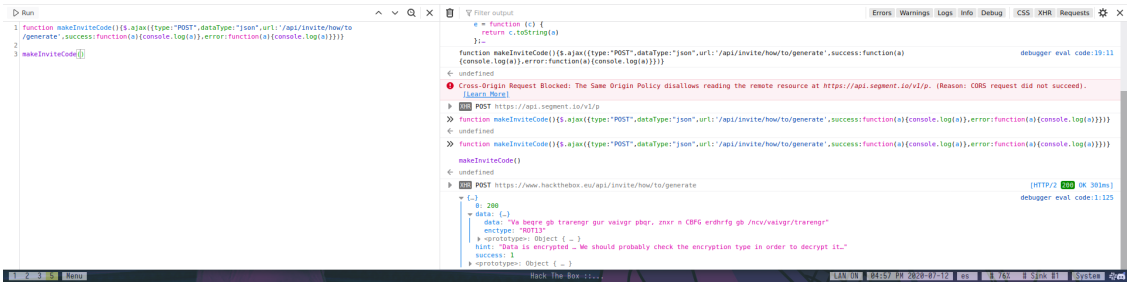

Figura 4: El resultado de el código obfuscado es una llamada a la api del sitio, la cual devuelve un contenido encriptado (oh si, súper encriptado), el cual indica claramente que es ROT13.

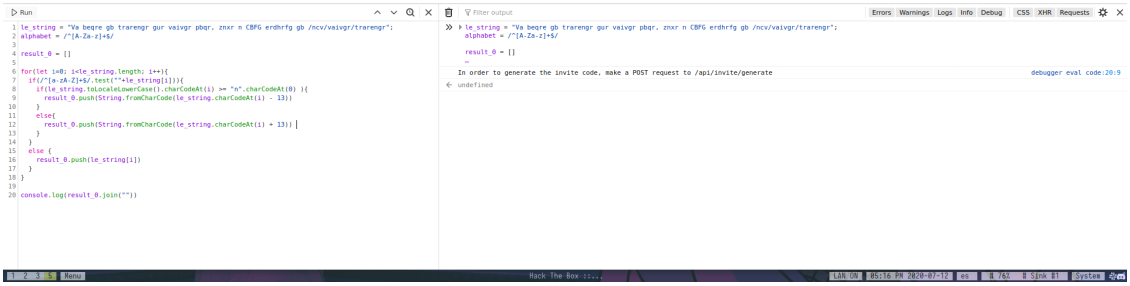

Figura 5: Al revertir ROT13 tenemos un mensaje donde nos dicen que tenemos que ejecutar una llamada POST a otra dirección para tener nuestro invite-code.

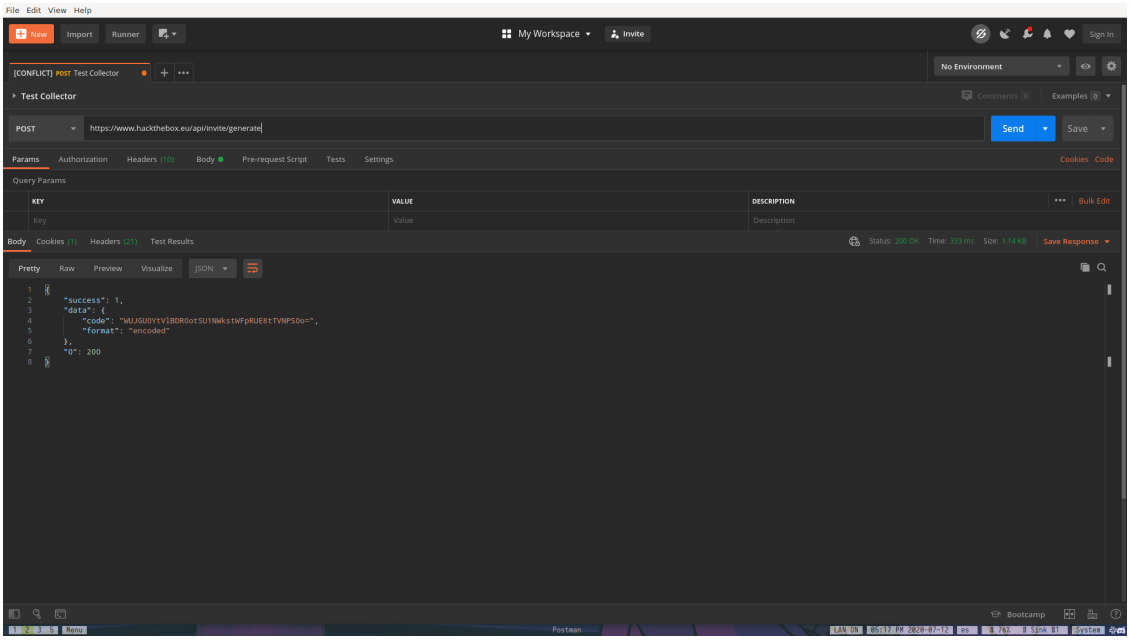

Figura 6: Ejecutamos la llamada pero resulta que el resultado viene codificado como base64 (delatado por la parte final).

Figura 7: Revertimos el codificado y tenemos algo que parece... Un invite code -aunque en realidad mas parece una serial de Windows XP -.

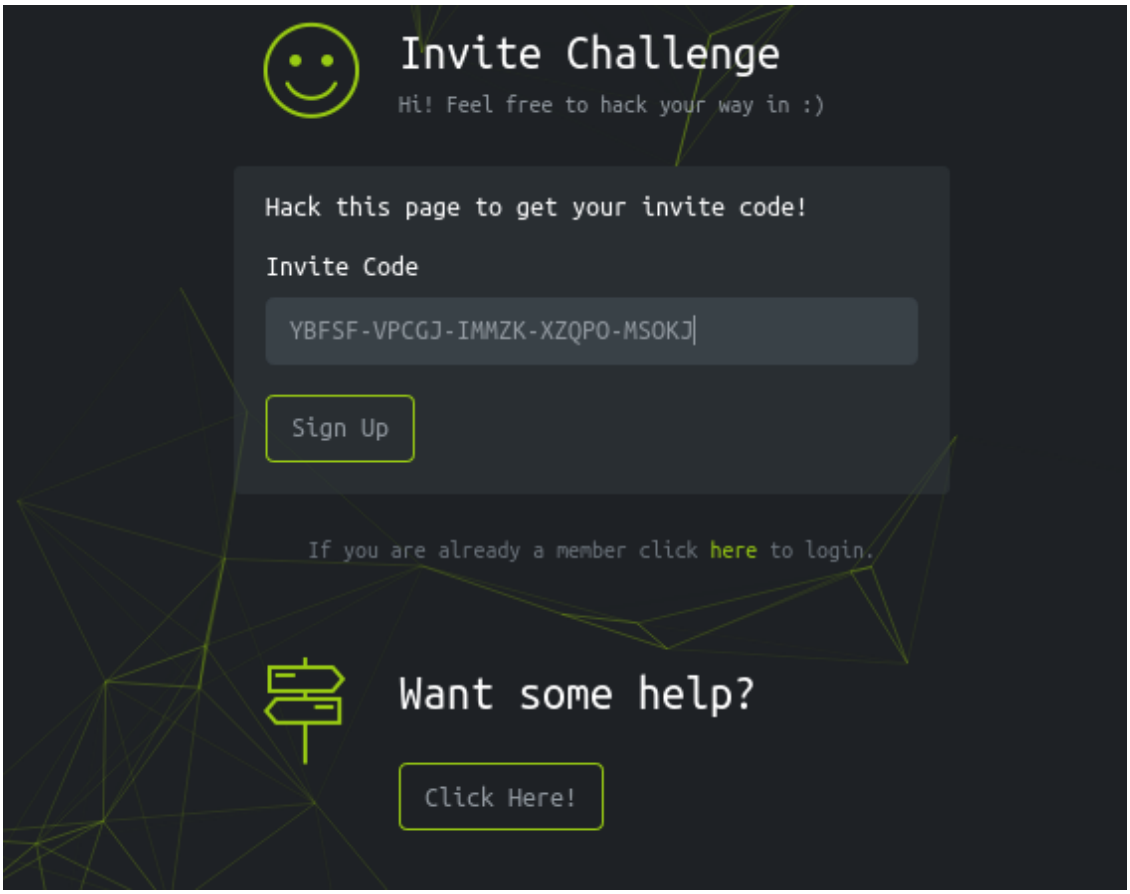

Figura 8: Pegamos el invite code...

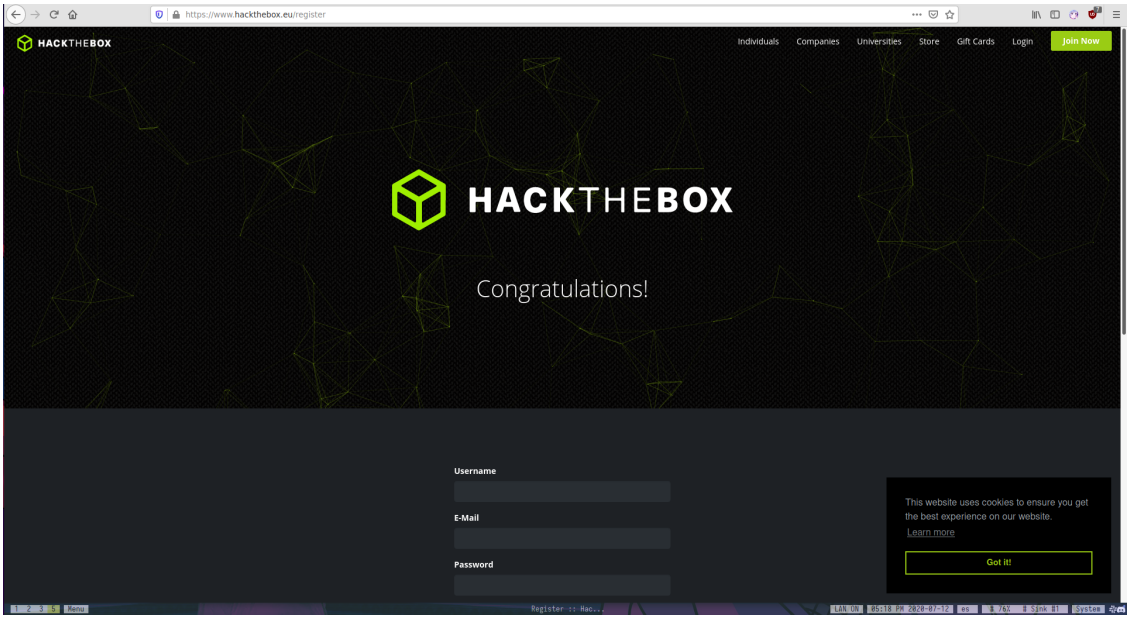

Figura 9: Y listo, fuimos aceptados para poder generar nuestra cuenta.

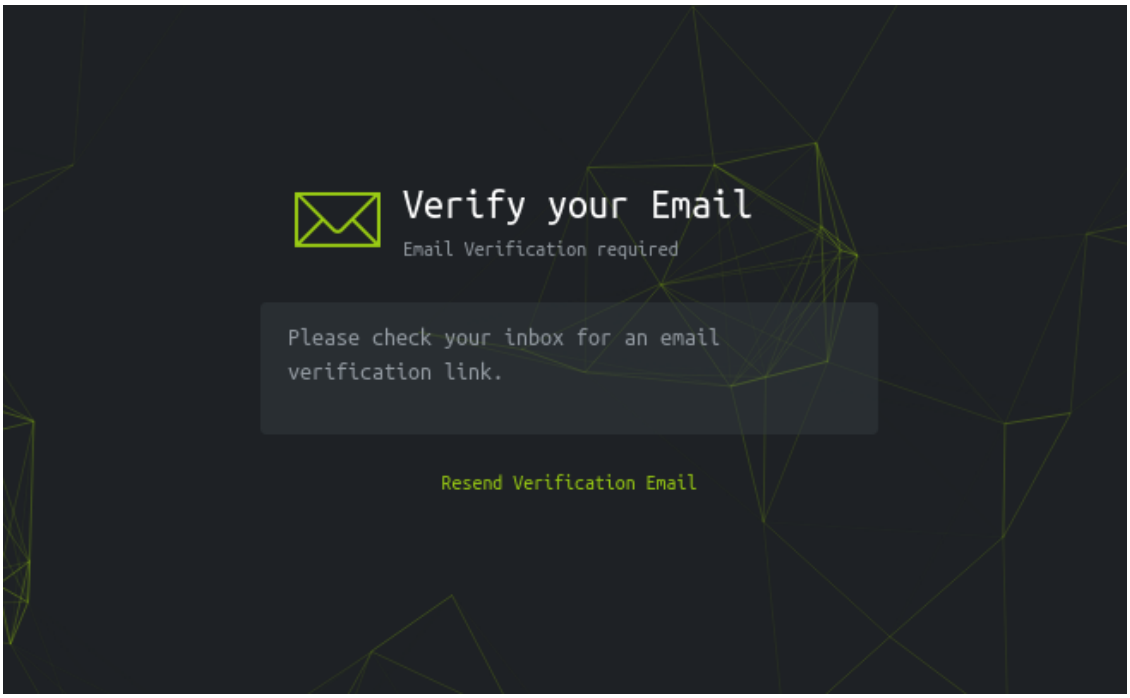

Figura 10: Revisamos el correo de confirmación...

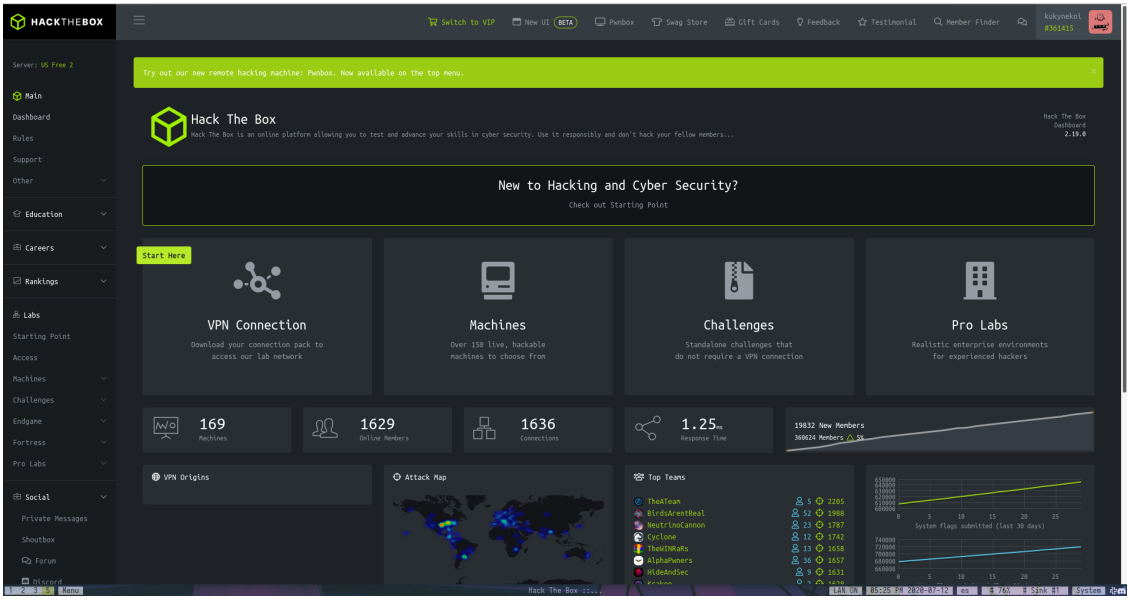

Figura 11: Y listo, logramos registrar nuestra cuenta en el sitio.

Referencias

[1] Mi repositorio *GitHub Repository*. https://github.com/KukyNekoi/UTAL/tree/master/ComputerScience