**Resolución del reto “Guuglu”**

TheGrue - CTF Team

/home/jhonnthedickers/hacking/writeups/this.docs

20/02/2024

# **Nick de los autores***:* Astharot15

Localidad: Madrid, Madrid (España)

Temas: CTF, Hack0n, Web

Contacto: jhonnthedickers@gmail.com

# **Índice**

[**Índice 2**](#_jndyhq1cnps4)

[**Enunciado del Reto 2**](#_4d34og8)

[**Resolución 3**](#_2s8eyo1)

[Extrayendo el archivo: 3](#_26in1rg)

[Encontrar archivo oculto: 3](#_e8wtsnpoaso5)

[**Flag: 4**](#_iei8aqfmk384)

# 

# 

# 

# 

# **Enunciado del Reto**

He creado una página web como Google. Por ahora está en vías de desarrollo por lo que cada usuario solo puede ver sus posts.

*Palabras clave:* Web, Google, login, information disclosure.

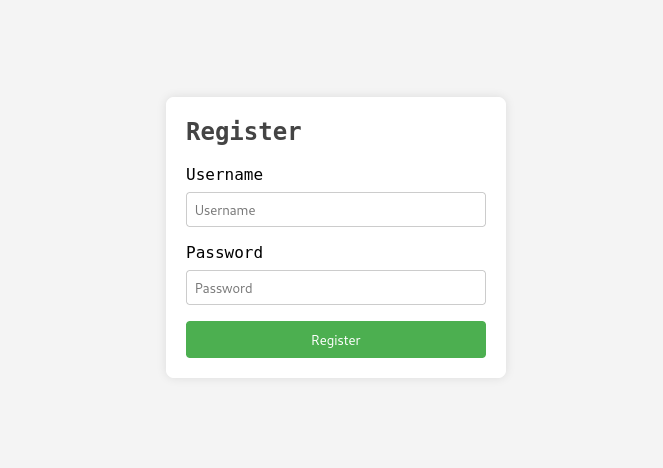
# **Resolución**

## 

## **Leyendo el código:**

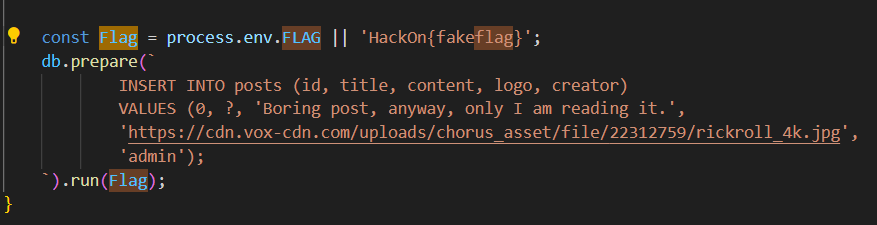
Nos dan la carpeta dónde se encuentra el reto, por lo que es un reto de white box ya que podemos ver el funcionamiento interno de la aplicación.

Al comienzo nos pide loggearnos con un usuario que creamos.



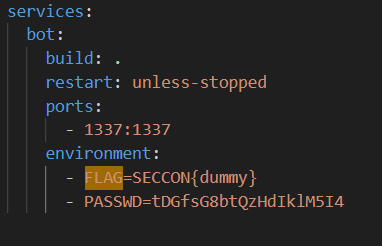
Vamos a ahorrarnos todo el rabbit hole de la página web ya que el reto, o está mal configurado, ya que no se usa la url de un bot con el que cuenta, o tiene callejones sin salida por todos lados.

Viendo el código encontramos la flag en las publicaciones del administrador.



Entonces sabemos que tenemos que loggearnos como administrador o engañar a la aplicación web para que crea que somos administrador.

Al hacer la búsqueda y filtrar por flag encontramos algo interesante.



¿No será no? La contraseña del administrador en el archivo que nos dan en el reto.

Efectivamente lo es, buscamos entre sus posts y obtenemos la flag.

### **Flag:** HackOn{\*\*\*\*\*\*\*\*}

La flag no se dá gratis, un beso y te la paso