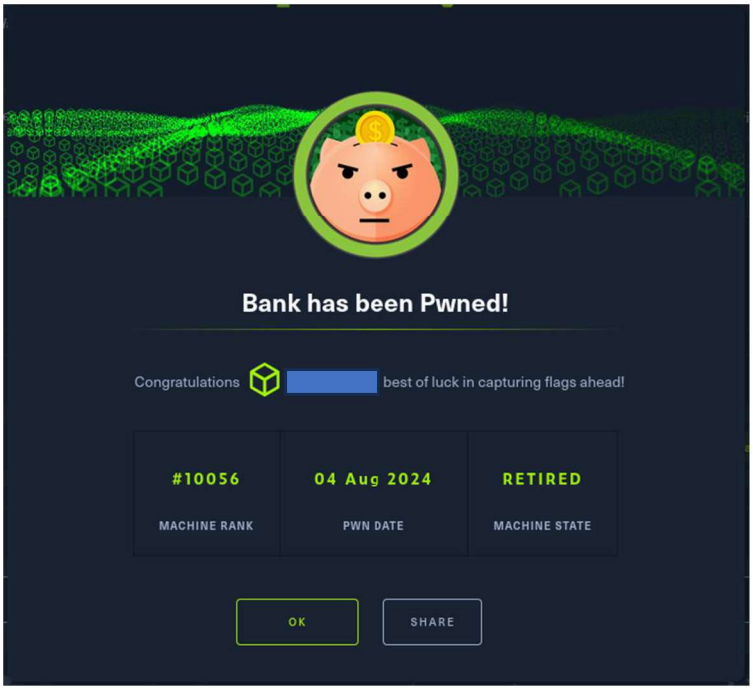
| Hack The Box - Bank | |
|---|---|
| **Sistema Operativo:** | **Linux** |
| **Dificultad**: | **Easy** |
| **Release:** | **16/06/2017** |
| | |
| **Técnicas utilizadas** | |
| ● Identifying vulnerable services<br>● Exploiting SUID files | |

En este write-up, se detalla el proceso de resolución de la máquina "Bank" de Hack The Box. La resolución de este reto implicó realizar un ataque de transferencia de zona DNS, seguido de la identificación de directorios ocultos mediante técnicas de fuerza bruta. Posteriormente, se descubrieron credenciales válidas que permitieron el acceso a la aplicación web, donde se aprovechó una vulnerabilidad en la funcionalidad de carga de archivos para ejecutar código remoto. Finalmente, se llevó a cabo una escalada de privilegios mediante la explotación de archivos con el bit SUID activado, culminando en el acceso al sistema como usuario root.



## Enumeración

La dirección IP de la máquina víctima es 10.129.251.182. Por tanto, envié 5 trazas ICMP para verificar que existe conectividad entre las dos máquinas.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ ping -c 5 10.129.251.182 -R
PING 10.129.251.182 (10.129.251.182) 56(124) bytes of data.
64 bytes from 10.129.251.182: icmp_seq=1 ttl=63 time=51.9 ms
RR:     10.10.16.25
        10.129.0.1
        10.129.251.182
        10.129.251.182
        10.10.16.1
        10.10.16.25

64 bytes from 10.129.251.182: icmp_seq=2 ttl=63 time=53.0 ms    (same route)
64 bytes from 10.129.251.182: icmp_seq=3 ttl=63 time=53.1 ms    (same route)
64 bytes from 10.129.251.182: icmp_seq=4 ttl=63 time=53.4 ms    (same route)
64 bytes from 10.129.251.182: icmp_seq=5 ttl=63 time=52.7 ms    (same route)

--- 10.129.251.182 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 51.945/52.826/53.427/0.498 ms
```

Una vez que identificada la dirección IP de la máquina objetivo, utilicé el comando **nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn 10.129.251.182 -oN scanner_bank** para descubrir los puertos abiertos y sus versiones:

- **(-p-)**: realiza un escaneo de todos los puertos abiertos.
- **(-sS)**: utilizado para realizar un escaneo TCP SYN, siendo este tipo de escaneo el más común y rápido, además de ser relativamente sigiloso ya que no llega a completar las conexiones TCP. Habitualmente se conoce esta técnica como sondeo de medio abierto (half open). Este sondeo consiste en enviar un paquete SYN, si recibe un paquete SYN/ACK indica que el puerto está abierto, en caso contrario, si recibe un paquete RST (reset), indica que el puerto está cerrado y si no recibe respuesta, se marca como filtrado.
- **(-sC)**: utiliza los scripts por defecto para descubrir información adicional y posibles vulnerabilidades. Esta opción es equivalente a **--script=default**. Es necesario tener en cuenta que algunos de estos scripts se consideran intrusivos ya que podría ser detectado por sistemas de detección de intrusiones, por lo que no se deben ejecutar en una red sin permiso.
- **(-sV)**: Activa la detección de versiones. Esto es muy útil para identificar posibles vectores de ataque si la versión de algún servicio disponible es vulnerable.
- **(--min-rate 5000)**: ajusta la velocidad de envío a 5000 paquetes por segundo.
- (**-Pn**): asume que la máquina a analizar está activa y omite la fase de descubrimiento de hosts.

```
┌──(root㉿kali)-[/home/administrador/Descargas]
└─# cat nmap/scanner_bank
# Nmap 7.94SVN scan initiated Sun Aug  4 18:15:14 2024 as: nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn -oN nmap/scanner_bank 10.129.251.182
Increasing send delay for 10.129.251.182 from 0 to 5 due to 2437 out of 8121 dropped probes since last increase.
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '^HTTP/1\.1 \d\d\d (?:[^\r\n]*\r\n(?!\r\n))*?.*\r\nServer: Virata-EmWeb
LaserJet ([\w._ -]+)   '
Nmap scan report for 10.129.251.182
Host is up, received user-set (0.088s latency).
Scanned at 2024-08-04 18:15:14 CEST for 31s
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 08:ee:d0:30:d5:45:e4:59:db:4d:54:a8:dc:5c:ef:15 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAMJ+YATka9wvs0FTz8iNWs6uCiLqSFhmBYoYAorFpozVGkCkU1aEJ7biybFTw/qzS9pbSsaYA+3LyUyvh3BSPGEt1BgGW/H29MuXjkznwVz60JqL4GqaJzYSL
AIBIBAhLmVd3Tz+o+6Oz39g4Um1le8d3DETINWk3myRvPw8hcnRwAFe1+14h3RX4fr+LKXoR/tYrI138PJyiyl+YtQWhZnJ7j8lqnKRU2YibtnUc44kP9FhUqeAcBNjj4qwG9GyQSWm/Q5CbOokgaaE
HgrZ2cLgKTIuneGS8lauXjC66NNMoUkJcMHpwRkYC0A86LDmhES6OuPsQwAjr1AtUZn97QjYu1d6WPfhTdsRYBuCotgKh2SBkzV1Bcz77Tnp56JA==
|   2048 b8:e0:15:48:2d:0d:f0:f1:73:33:b7:81:64:08:4a:91 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDc0rofjHtpSlqkDjjnkEiYcbUrMH0Q4a6PcxqsR3updDGBWu/RK7AGWRSjPn13uil/nl44XF/fkULy7FoXXskByLCHP8FS2gYJApQMvI9n81ERc
WpqDv+RWtbc2Wuc/FTeGSOt1LBTbtKcLwEehBG+Ym8o8iKTd+zfVudu7v1g3W2Aa3zLuTcePRKLUK3Q2D7k+5aJnWrekpiARQm3NmMkv1NuDLeW3amVBCv6DRJPBqEgSeGMGsnqkR8CKHO9/
|   256 a0:4c:94:d1:7b:6e:a8:fd:07:fe:11:eb:88:d5:16:65 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDH30xnPq1XEub/UFQ2KoHXh9LFKMNMkt60xYF3OrEp1Y5XQd0QyeLXwm6tIqWtb0rWda/ivDgmiE
|   256 2d:79:44:30:c8:bb:5e:8f:07:cf:5b:72:ef:a1:6d:67 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIA8MYjFyo+4OwYGTzeuyNd998y6cOx56mIuciim1cvKh
53/tcp open  domain  syn-ack ttl 63 ISC BIND 9.9.5-3ubuntu0.14 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.9.5-3ubuntu0.14-Ubuntu
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.7 ((Ubuntu))
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.7 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Aug  4 18:15:45 2024 -- 1 IP address (1 host up) scanned in 30.96 seconds
```

## Enumeración del puerto 53 (DNS)

Dado que el puerto 53 (DNS) estaba abierto, intenté realizar un ataque de transferencia de zona para identificar posibles subdominios.

Una transferencia de zona es un proceso mediante el cual un servidor DNS transfiere una copia completa de su base de datos de zona a otro servidor DNS. Este proceso permite que los servidores secundarios mantengan una copia actualizada de la información DNS, asegurando que las consultas DNS puedan ser respondidas incluso si el servidor primario no está disponible. Existen dos tipos de transferencia de zona: completa (AXFR) e incremental (IXFR).

Un ataque de transferencia de zona ocurre cuando un atacante aprovecha este proceso para obtener información sensible de un servidor DNS. Este tipo de ataque se basa en la explotación del mecanismo de transferencia de zona, diseñado para replicar la información de la zona DNS entre servidores autorizados. El atacante comienza realizando una consulta DNS utilizando herramientas como dig, que permite interactuar con el servidor DNS y solicitar información específica. Para llevar a cabo el ataque, el atacante utiliza el parámetro AXFR, que es el comando estándar para solicitar una transferencia de zona completa.

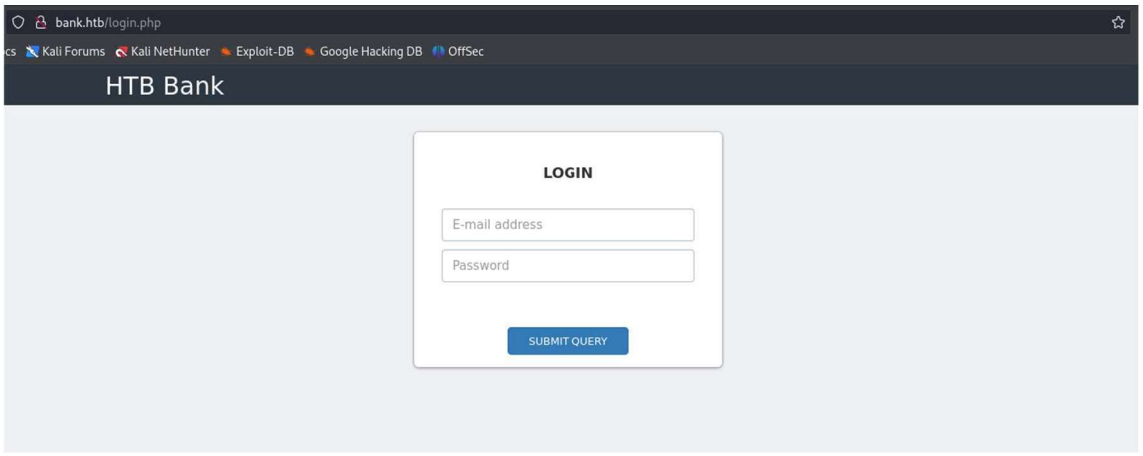
```
┌──(administrador㉿kali)-[~/Descargas]
└─$ dig @10.129.251.182 bank.htb axfr

; <<>> DiG 9.20.0-Debian <<>> @10.129.251.182 bank.htb axfr
; (1 server found)
;; global options: +cmd
bank.htb.               604800  IN      SOA     bank.htb. chris.bank.htb. 6 604800 86400 2419200 604800
bank.htb.               604800  IN      NS      ns.bank.htb.
bank.htb.               604800  IN      A       10.129.29.200
ns.bank.htb.            604800  IN      A       10.129.29.200
www.bank.htb.           604800  IN      CNAME   bank.htb.
bank.htb.               604800  IN      SOA     bank.htb. chris.bank.htb. 6 604800 86400 2419200 604800
;; Query time: 56 msec
;; SERVER: 10.129.251.182#53(10.129.251.182) (TCP)
;; WHEN: Sun Aug 04 18:25:07 CEST 2024
;; XFR size: 6 records (messages 1, bytes 171)
```

Considerando esta información, procedí a actualizar el archivo /etc/hosts para incluir la nueva entrada. Este proceso se conoce como **virtual hosting**, una técnica que permite a un servidor web alojar múltiples sitios web en la misma máquina física. Esto se logra mediante la asignación de nombres de dominio o direcciones IP específicas a cada sitio web, lo que permite al servidor identificar y enrutar las solicitudes de manera adecuada.

## Enumeración del puerto 80 (HTTP)

Al acceder a la página web disponible en el servidor, encontré una pantalla de inicio de sesión, pero no tenía las credenciales necesarias para acceder a la aplicación:




Con el objetivo de obtener más información, utilicé gobuster, una herramienta de fuerza bruta para la enumeración de directorios y archivos en sitios web, para listar los posibles directorios ocultos disponibles en este servidor, además de filtrar por archivos con extensiones txt, html y php.

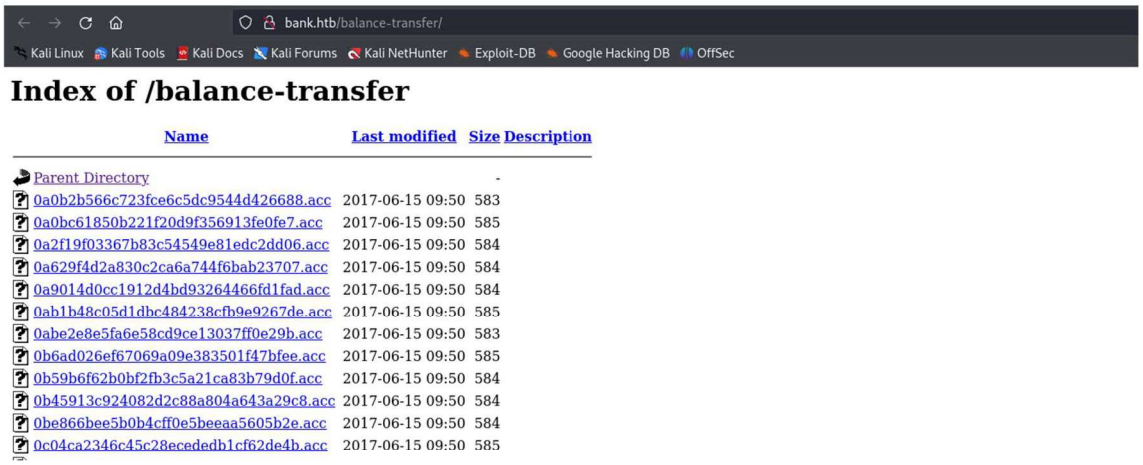
```
┌──(root㉿kali)-[/home/administrador/Descargas]
└─# gobuster dir -u http://bank.htb/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -b 403,404 -x php,txt,html --random-agent -t 200
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://bank.htb/
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   403,404
[+] User Agent:              Mozilla/5.0 (Windows; U; Windows NT 5.1 ; x64; en-US; rv:1.9.1b2pre) Gecko/20081026 Firefox/3.1b2pre
[+] Extensions:              php,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 302) [Size: 7322] [--> login.php]
/login.php            (Status: 200) [Size: 1974]
/uploads              (Status: 301) [Size: 305] [--> http://bank.htb/uploads/]
/assets               (Status: 301) [Size: 304] [--> http://bank.htb/assets/]
/logout.php           (Status: 302) [Size: 0] [--> index.php]
/inc                  (Status: 301) [Size: 301] [--> http://bank.htb/inc/]
/support.php          (Status: 302) [Size: 3291] [--> login.php]
/balance-transfer     (Status: 301) [Size: 314] [--> http://bank.htb/balance-transfer/]
Progress: 882240 / 882244 (100.00%)
===============================================================
Finished
===============================================================
```

El directory listing es una característica de los servidores web que permite la visualización de una lista de archivos y subdirectorios contenidos en un directorio específico del servidor. Esta funcionalidad se activa cuando no existe un archivo de índice predeterminado en el directorio solicitado. El directory listing puede ser una herramienta útil para administradores de sistemas, ya que permite verificar la estructura de archivos y directorios en el servidor. Sin embargo, también puede representar un riesgo de seguridad si no se configura adecuadamente, ya que puede exponer información sensible a usuarios no autorizados.

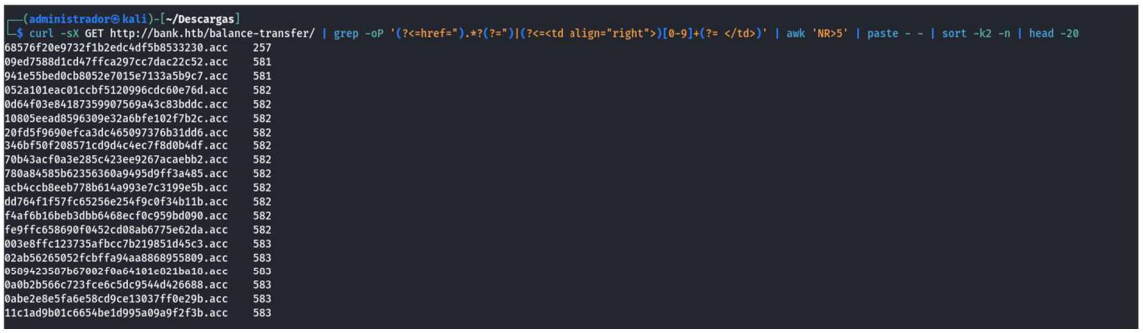
Por tanto, es recomendable desactivar el directory listing en la configuración del servidor web. Por ejemplo, en servidores Apache, se puede desactivar añadiendo Options -Indexes en el archivo .htaccess. En servidores Nginx, se puede lograr añadiendo autoindex off; en la configuración del servidor.

En este caso, fue posible listar los archivos disponibles en el directorio encontrado anteriormente con gobuster.

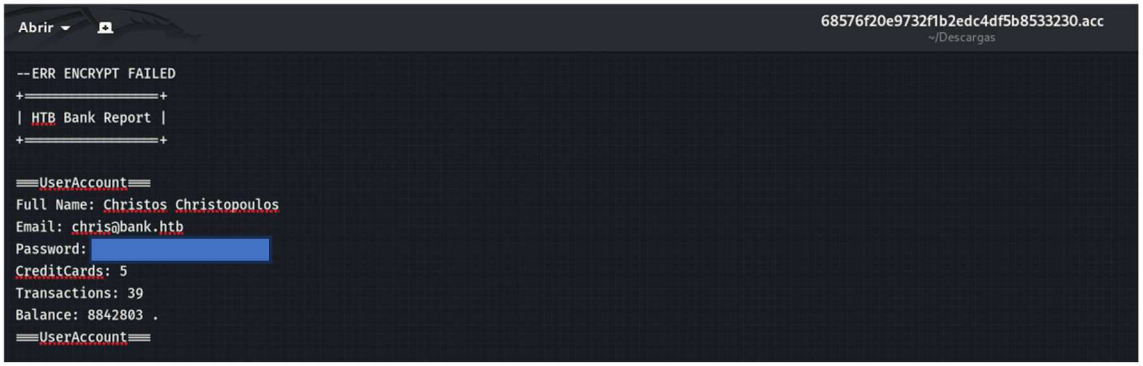
La extensión .acc se utiliza principalmente para archivos de datos de cuentas gráficas. Estos archivos son generados por el software Graphic Accounts de FKJ Software y contienen información financiera introducida por el usuario. Los archivos .acc permiten a los usuarios gestionar y planificar presupuestos personales, almacenando datos asociados a varias cuentas bancarias.



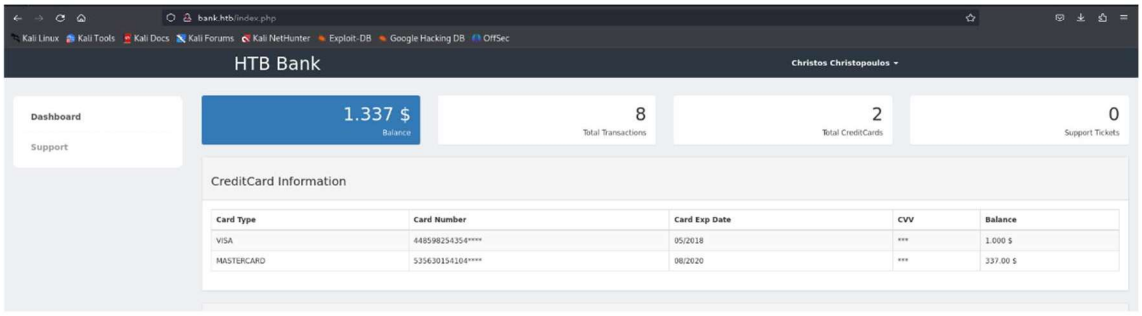

Curiosamente, al ordenar los datos encontrados anteriormente, de menor a mayor, encontré uno con un tamaño diferente al resto. Este archivo podría contener información útil.



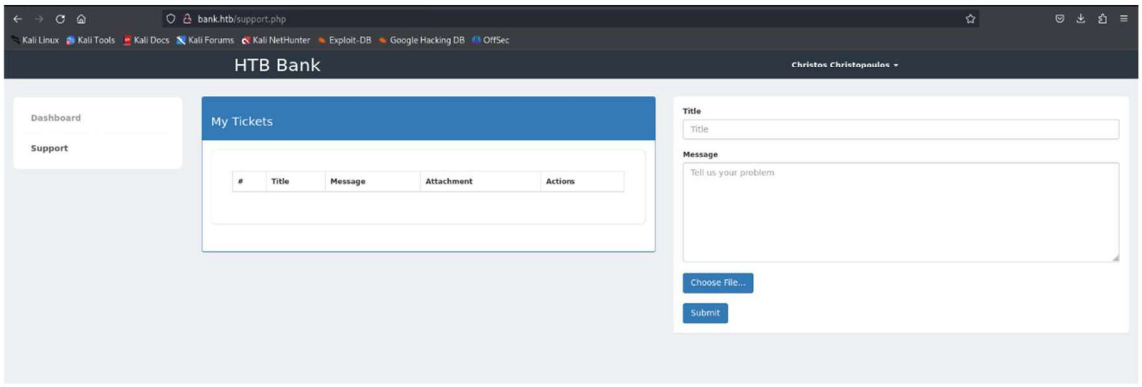

Al acceder al archivo encontrado anteriormente, encontré una posible contraseña, así como un nombre de usuario.



Estas credenciales resultaron ser válidas y pude iniciar sesión en la aplicación disponible.

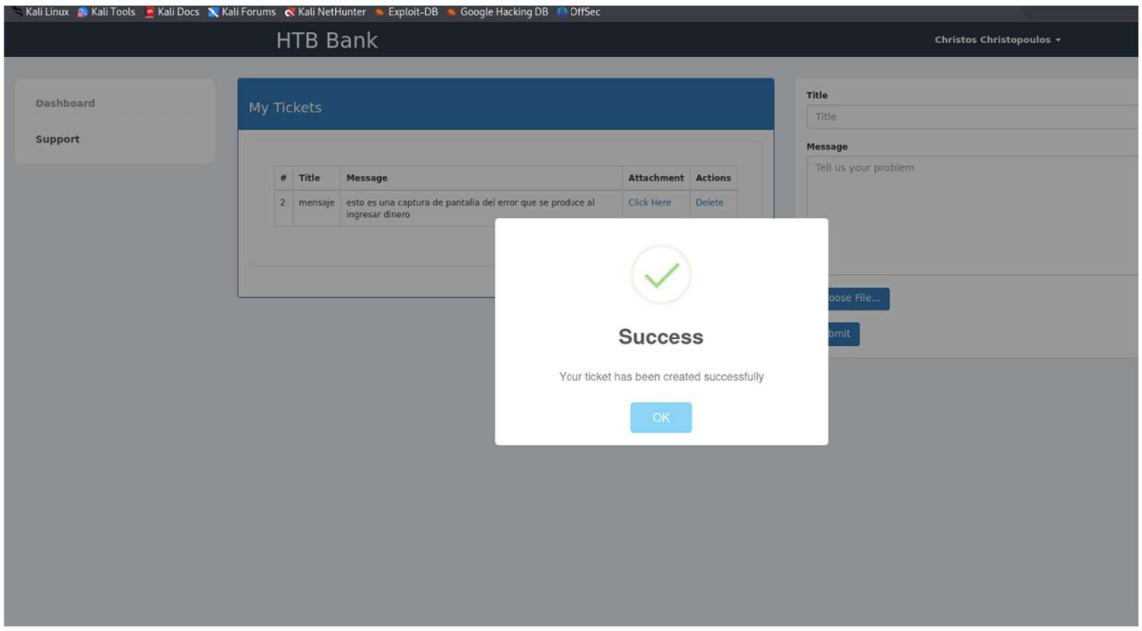



Investigando esta página web, descubrí que esta aplicación permitía subir un archivo al servidor, pero no sabía si era posible ejecutar código PHP, ni si había alguna extensión que pudiera usar para dicho objetivo.

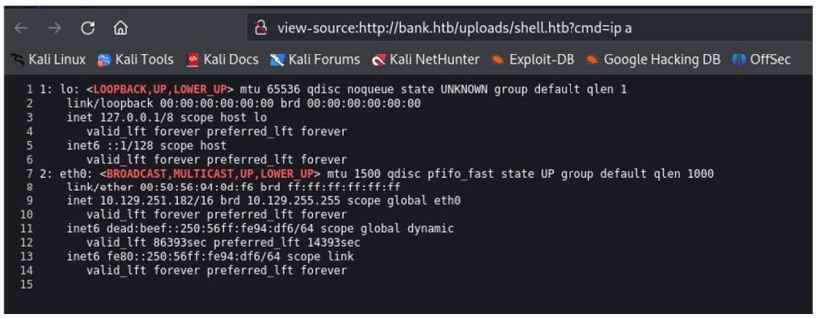



Por tanto, decidí leer el código fuente de la aplicación con el objetivo de encontrar alguna pista que me permitiera averiguar la extensión válida que podría subir al servidor. En este caso, el servidor permite ejecutar código PHP en archivos con extensión .htb.

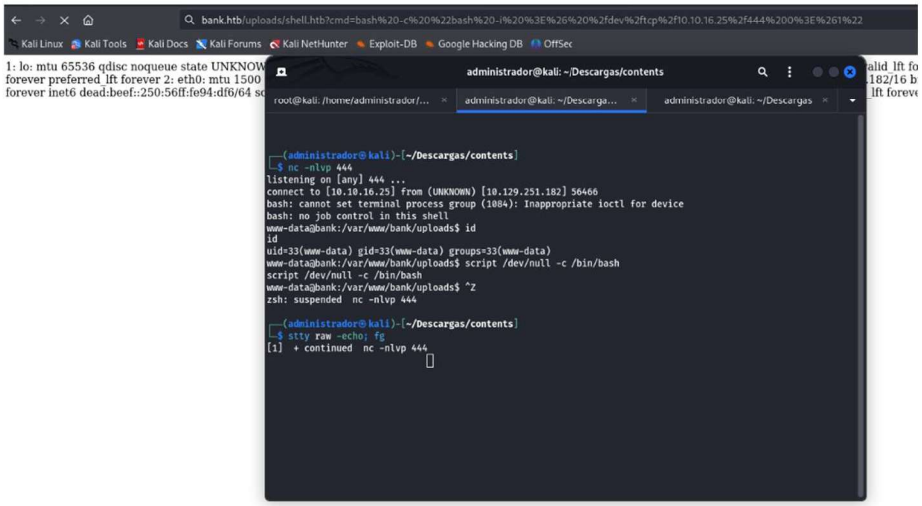
Teniendo en cuenta lo anterior, subí el archivo de forma exitosa usando la extensión descubierta.




Por tanto, sólo quedaba comprobar que era posible ejecutar comandos en la máquina víctima.

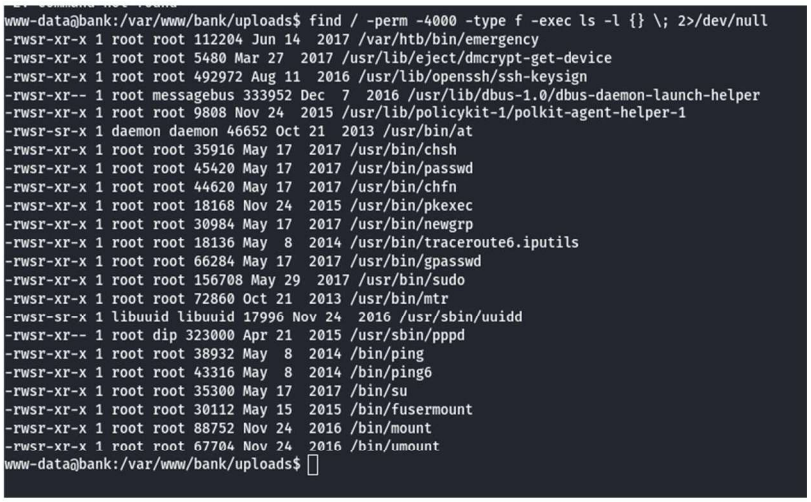



Sabiendo que podía ejecutar comandos remotos en la máquina objetivo, decidí entablar una conexión inversa con la máquina objetivo.



## Escalada de privilegios

Más tarde, comencé a buscar archivos con el bit SUID activado, ya que estos archivos pueden ejecutarse con privilegios elevados. Los archivos con el bit SUID (Set User ID) activado permiten que los usuarios ejecuten el archivo con los permisos del propietario del archivo, en lugar de con los permisos del usuario que lo ejecuta. Esto es crucial para la escalada de privilegios, ya que puede permitir a un atacante ejecutar comandos con permisos de root si el archivo SUID es propiedad del usuario root.




Finalmente, accedí al sistema como usuario root.


## Bibliografía


https://www.reviversoft.com/es/file-extensions/acc