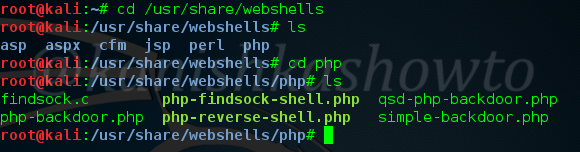
Upload shell and hack a website:Part 2-web shells in kali linux

Good morning everybody. In[Part 1 of this series](https://hackercool.com/2016/06/upload-shell-and-hack-a-website-part-1/), we saw how one of the most popular shells can be used to hack a website. However popularity has its own disadvantages, at the least in the field of cyber security. The C99 php shell is very well known among the antivirus. Any common antivirus will easily detect it as malware. Although it is unlikely that web servers will be installed with antivirus, still it is good to stay one step ahead. So today we will see some of the least popular but still effective web shells.

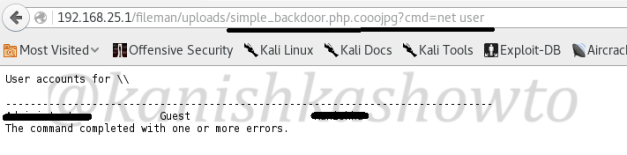
As you all know, Kali Linux is one of the best pentesting distros available. It would be very disappointing if it didn’t have web shells in its arsenal. Open a terminal and navigate to the directory “/usr/share/webshells” as shown below. As you can see, web shells are classified according to the language of the website we are trying to hack. Today we will see about PHP shells. So go into that directory and do an “ls”. You can see the shells below.

[](https://i0.wp.com/hackercool.com/wp-content/uploads/2016/06/webshells1.png?ssl=1)

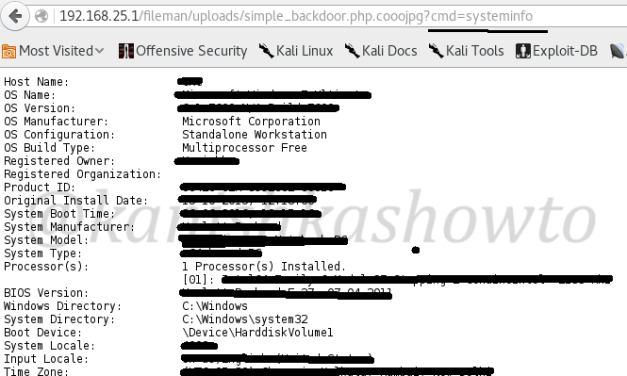
Now let us see their features by uploading each one them into web server we want to hack. See [how to upload the shells.](https://hackercool.com/2016/06/rfi-hacking-for-beginners-part-1/)

1. simple-backdoor.php

As the name clearly tells, the functioning of this shell is very simple. It is used to execute some commands on the target web server. Let us go to the shell’s link after uploading and execute the “net user” command as shown below. As already used in Part 1, this command gives us all the users present on the Window’s system.

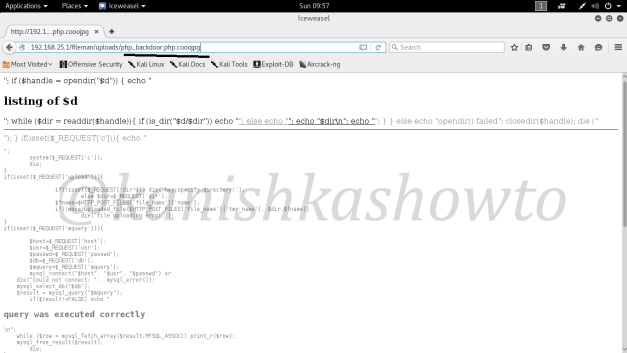
[](https://i0.wp.com/hackercool.com/wp-content/uploads/2016/06/webshells2.png?ssl=1)

Similarly let us execute another powerful command “systeminfo” to get the web server’s whole information as shown below. Sorry about the censor.

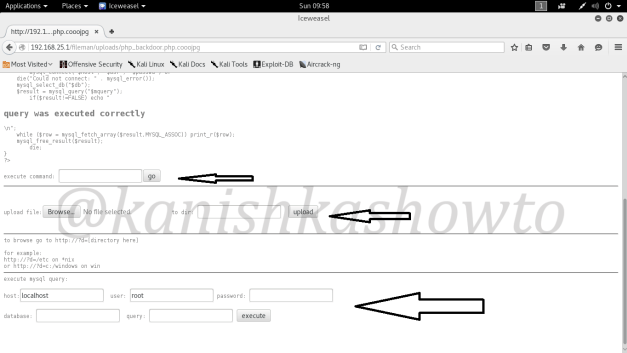
[](https://i2.wp.com/hackercool.com/wp-content/uploads/2016/06/webshells3.png?ssl=1)

php-backdoor.php

The php-backdoor, as the name implies  is file upload shell just used to add more backdoors. It helps us in the case where we can’t easily upload any additional files we want.

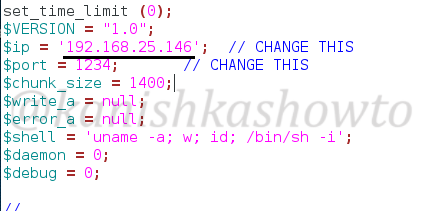
[](https://i0.wp.com/hackercool.com/wp-content/uploads/2016/06/webshells4.png?ssl=1)

I works akin to file upload function in our Part 1. As you can see below, it has upload form and a function to execute commands. We can also connect to the database.

[](https://i0.wp.com/hackercool.com/wp-content/uploads/2016/06/webshells5.png?ssl=1)

php-reverse-shell.php

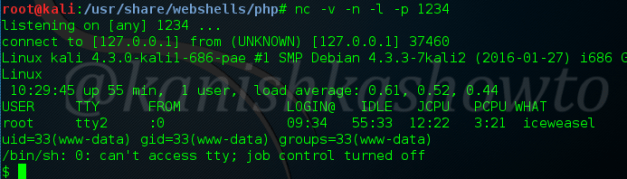
Every shell doesn’t require us to visit the web server. In fact we can make the webserver visit us. Enter the php-reverse-shell. As its name says, it makes a reverse connection to our attacker system. In order for this shell to make a reverse connection, it needs an IP address. So before uploading this shell we need to change the IP address in the script to our IP address ( Kali Linux ) as shown below. Save it and close it.

[](https://i0.wp.com/hackercool.com/wp-content/uploads/2016/06/webshells6.png?ssl=1)

Next, let us start a netcat listener in one of the terminal. If you are new to netcat the command “nc -v -n -l -p 1234” tells netcat to listen verbosely on port 1234. Remember the port number should be same as we specified above.

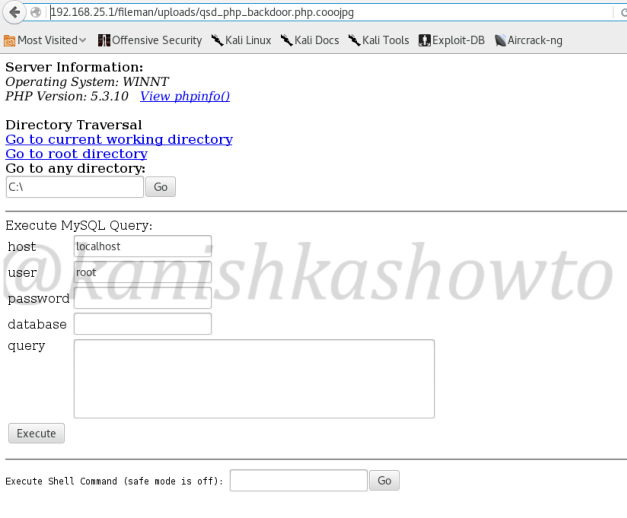
[](https://i2.wp.com/hackercool.com/wp-content/uploads/2016/06/webshells7.png?ssl=1)

Now when we upload the shell, On kali linux we will get a terminal as shown below. Hit “ls” to see the contents of the directory.

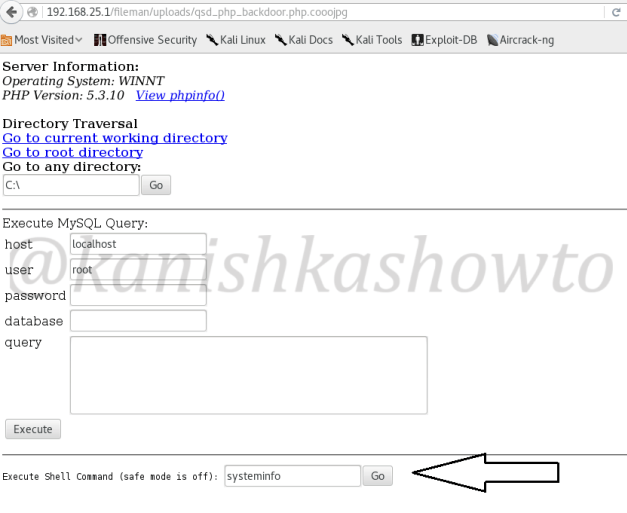
[](https://i2.wp.com/hackercool.com/wp-content/uploads/2016/06/webshells8.png?ssl=1)

qsd-php-backdoor.php

The qsd-php-backdoor is compatible with both Linux and Windows web servers. As we upload it, it will detect whether the web server is Windows or Linux and then acts accordingly. The screenshot is shown below. As you can see we can move to the root directory of web server and come back, execute shell commands and SQL queries.

[](https://i0.wp.com/hackercool.com/wp-content/uploads/2016/06/webshells9.png?ssl=1)

You already know what happens when we execute “systeminfo” command as shown below.

[](https://i0.wp.com/hackercool.com/wp-content/uploads/2016/06/webshells10.png?ssl=1)

That’s about web shells in Kali Linux. Hope it was helpful.