

Forum:[Hack Forums](#)

Thread: [Remote Command Execution](#)

SaintJimmy - April 24, 2020, 9:02 pm

What is Remote Command Execution?

In some times we call it remote code execution or OS command execution. Any way what's going on here is same. We run a shell command through a web application functionality. First of all we have to understand how is possible to execute a Linux command in a web application. In PHP we have some functions to do this. Like `system()`, `exec()` etc.

`System()` - what this function does is get the command as a parameter and execute it on the Linux server and print the output.

```
Code <?php
$cmd = 'uname -a' ;
system($cmd);
?>
```

`exec()` - This function also execute the given parameter as a Linux command. But one thing about this function is it'll don't print out the output. If we want to get output we need to use `echo` command with this function. Like this one.

```
Code <?php
$cmd= 'whoami';
exec($cmd);
?>
Code <?php
$cmd=$_GET['cmd'];
echo exec($cmd);
?>
```

Example:

Think about the following web application. Example HTML code for this output:

```
Code <html>
<body>
<form action="ping.php" method="Get">
Host:<br>
<input type="text" name="target" >
<br>

<input type="submit" value="Submit">
</form>
</body>
</html>
```

We know that it simply fetch the host name from user as an input and sent it via a get request to back-end script for further handling. Now the question is how back end PHP script handle this input and show the result data to the user?

```
Code <?php
$host = $_get[target];
system(ping $host -v);
?>
```

What this does is it'll take the data which is send by GET method and save that data to a variable called host. Then it gives that host to system function as the argument.

Example Execution:

Now, What if I enter <http://www.google.com> as the input? Output is:

```
Code system(ping http://www.google.com -v);
```

What if we enter 'whoami' (whoami is a Linux command which will give you the user name) as the input? Will our second command is executed? No. While both ping and whoami are linux commands we can't do this that way. If we want to combine two linux command we can do it this way.

```
Code date && whoami
```

Now I enter this as input. <http://www.google.com> && whoami, our query becomes:

```
Code system(ping http://www.google.com && whoami -v);
```

Still not working? There is no argument called -v for the whoami command. We can try this instead:

```
Code system(ping http://www.google.com && whoami & -v);
```

That's it.