Create status.html, df.php, and ls.php in your webserver's /var/www/html directory with the contents shown below. See if you can put something in the text box that causes the server to execute a command of your choosing. Hint: You might want to search for how to run two or more commands at once from the Linux terminal.

Contents of status.html

<html>

<title> Status, with command injection flaw </title>

<body>

<h4> Quick 'n Dirty Server Status<h4>

<a href="/df.php">Check Disk Utilization</a>

<br><br>

<h4>File listing for a directory</h4>

<form action="ls.php" method="get">

Enter a file path, leave empty for current dir: <input name="text" type="text" />

<input type="submit" />

</form>

Contents of df.php

<?php

// Send df command to shell\_exec

$output = shell\_exec('df');

echo "<pre>$output</pre>";

?>

<a href="/status.html">Return</a>

Contents of ls.php

<?php

// check to see if textbox is empty

if (isset($\_GET['text'])) {

$cmd = $\_GET['text'];

} else {

$cmd = '.';

}

$cmd = "ls -l ".$cmd;

$output = shell\_exec($cmd);

echo "<pre>$output</pre>";

?>

<a href="/status.html">Return</a>