<HTML>

<HEAD><TITLE>Login Page</TITLE></HEAD>

<BODY>

<CENTER>

<FORM method="POST" action="http://yourserver/cgi-bin/login.py">

<paragraph> Enter your login name: <input type="text" name="login">

<paragraph> Enter your password: <input type=password name="password">

<paragraph> <input type="submit" value="Connect">

</FORM>

</CENTER>

<HR>

</form>

</BODY>

</HTML>

login.py:

#!/usr/local/bin/python

import cgi

def header(title):

print "Content-type: text/html\n"

print "<HTML>\n<HEAD>\n<TITLE>%s</TITLE>\n</HEAD>\n<BODY>\n" % (title)

def footer():

print "</BODY></HTML>"

form = cgi.FieldStorage()

password = "python"

if not form:

header("Login Response")

elif form.has\_key("login") and form["login"].value != "" and form.has\_key("password") and form["password"].value == password:

header("Connected ..." )

print "<center><hr><H3>Welcome back," , form["login"].value, ".</H3><hr></center>"

print r"""<form><input type="hidden" name="session" value="%s"></form>""" % (form["login"].value)

print "<H3><a href=browse.html>Click here to start browsing</a></H3>"

else:

header("No success!")

print "<H3>Please go back and enter a valid login.</H3>"

footer()

I would like to make this login form vulnerable to RCE (remote code execution), is this possible with the function eval() or exec().

I am looking for functions that introduce a vulnerability within the login form. Are there whole classes/modules that contain dangerous functionally? Also would it be possible to make this login form vulnerable to remote code execution?

PRE - Knowledge

Understanding the code:-

Creating the HTML file using the post method to hide the data from the URL as it cannot be cached or saved in history on request.

login.py

This file used to import the “CGI” module. In this script must contain 2 sections of number headers and the type of data of the client respectively. CGI class has the method FieldStorage() that is used to index like a Python dictionary which supports all the dictionary methods. One benefits of them empty strings are not included and do not appear in the dictionary.   
form = cgi.FieldStorage()

Here we are declaring the form dictionary using FieldStorage() method.

THE logic line to login is:-

elif form.has\_key("login") and form["login"].value != "" and form.has\_key("password") and form["password"].value == password

It checks if the form has key login and login key should not have empty string as value, and it goes same for password if the form has key password and its value matched should be equal to password.

Answer and explanation

Remote Code Execution is actually the method and technique used by the hackers to access the information of the other’s computer.   
  
1) Yes, we can use eval() function to achieve this method which will help in reading the expression as a string and then the method is executed on it.

Basically, eval() is used to hide the potential information of the code. The eval() takes two extra arguments to allow you to do this: eval(expression[, globals[, locals]]). To do a complete lockdown.

2) Pretty much everything that we use a module to process file system it turns data in the executable code. As there will be many exploits even eval() can be a big red flag to vulnerable.