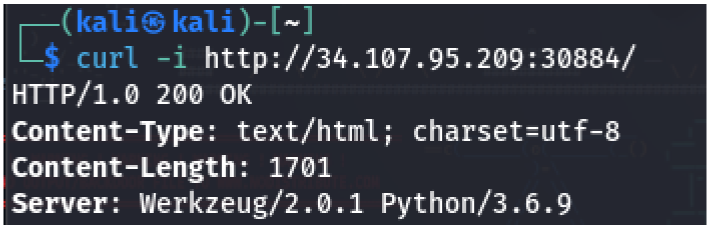
From the title of the chall, it’s hinted at some sort of **SSRF** vulnerability. After a bit of testing it turns out the server application is vulnerable to **LFI** via file:///, since we are able to type file:///etc/passwd as an url and the website displays the contents. That way, we find out the existence of /home/ctf

The 2nd part of the chall involved me banging my head trying to find the flag to no avail. At some point, I decided maybe there’s something I’m missing so I tried a curl –i:



```
┌──(kali㉿kali)-[~]
└─$ curl -i http://34.107.95.209:30884/
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 1701
Server: Werkzeug/2.0.1 Python/3.6.9
```

Yep, that’s what I was missing. All along, I was assuming the website was generated using nginx or apache2 or something like that, not python/flask. By looking at **file:///home/ctf/app.py** we can see the source code of the website.

The code is simple: we get the flag is the Host of our request is **company.tld**. After a quick curl the challenge is completed.

Made with love by: AndreiCat