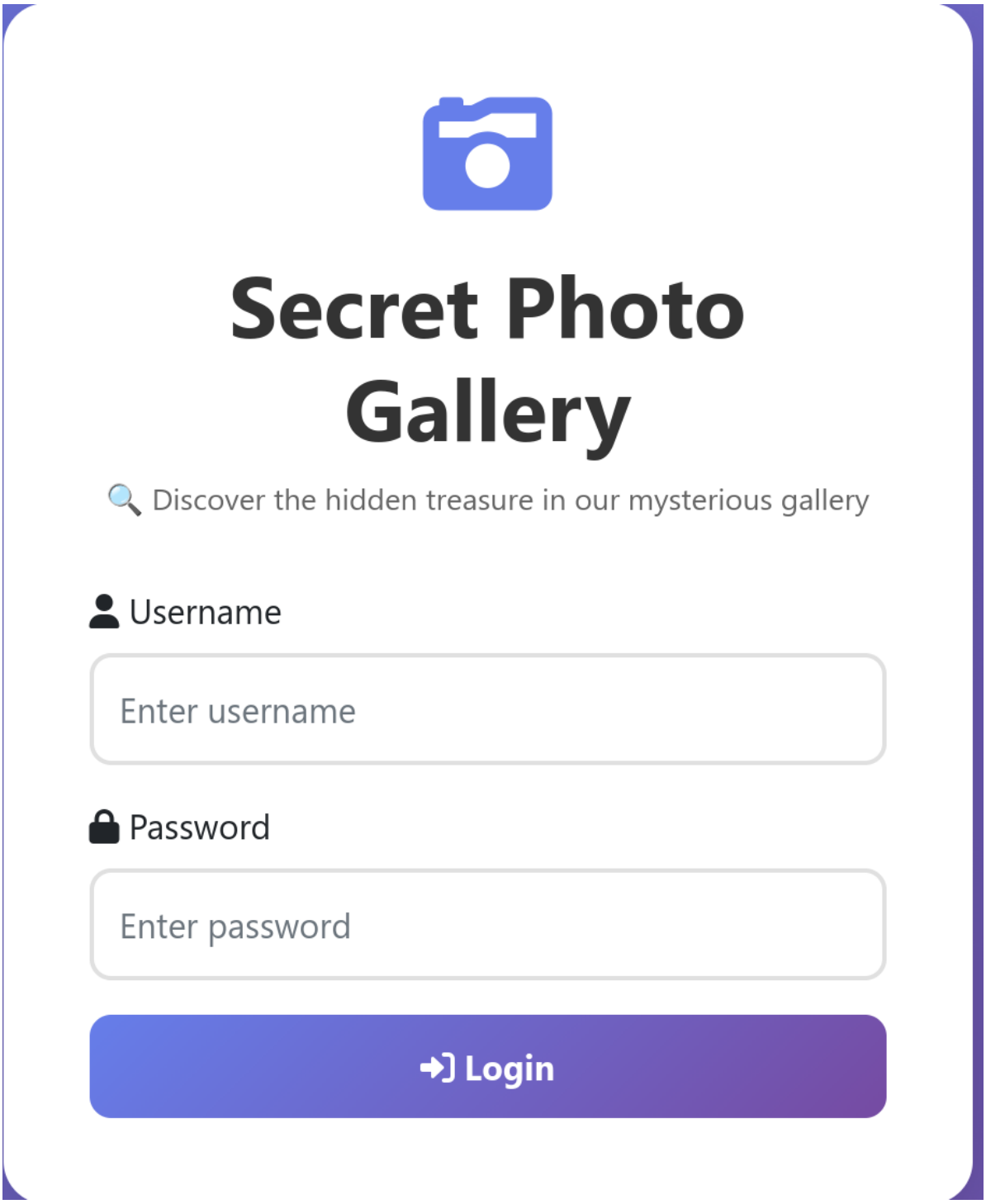
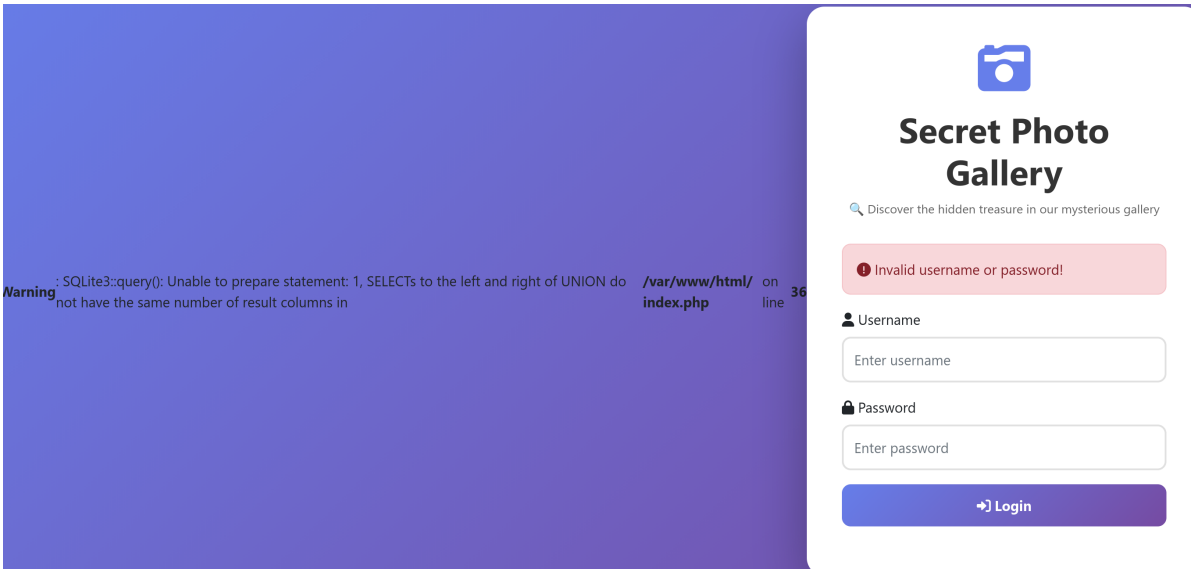
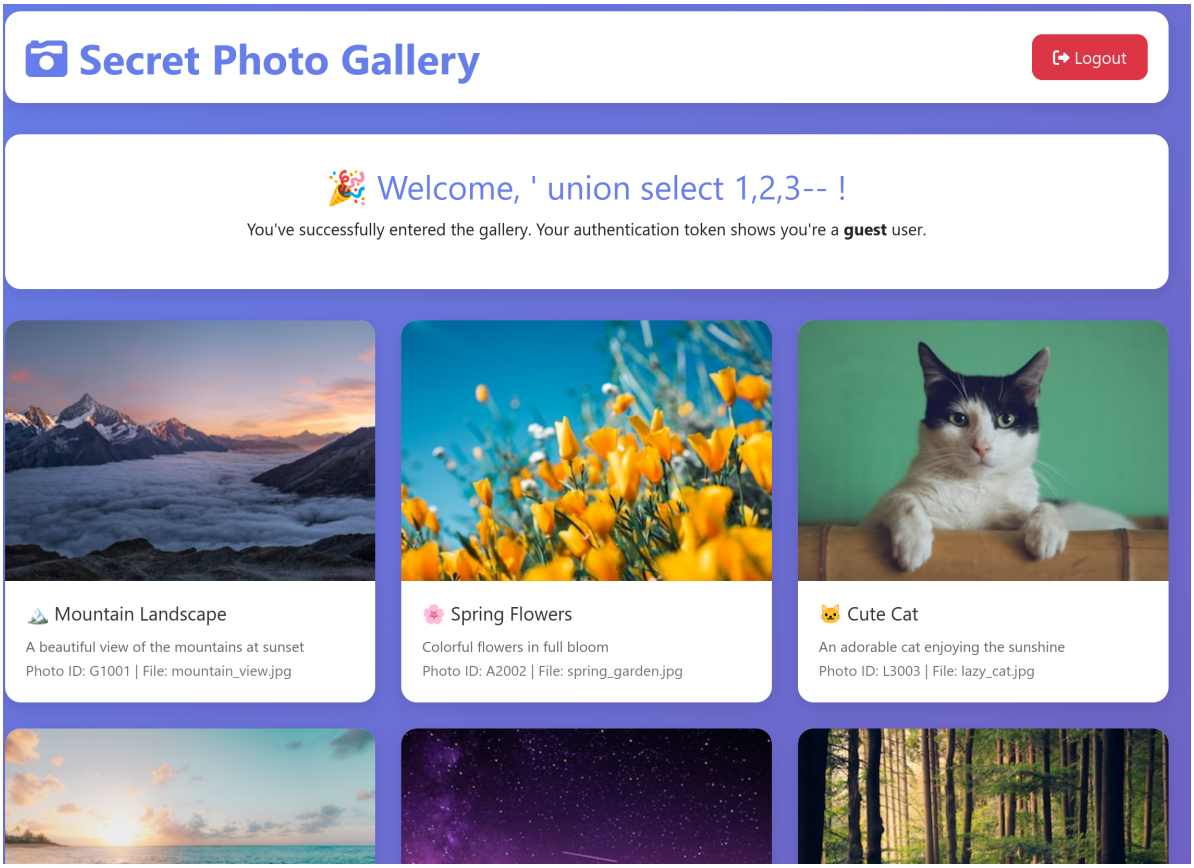
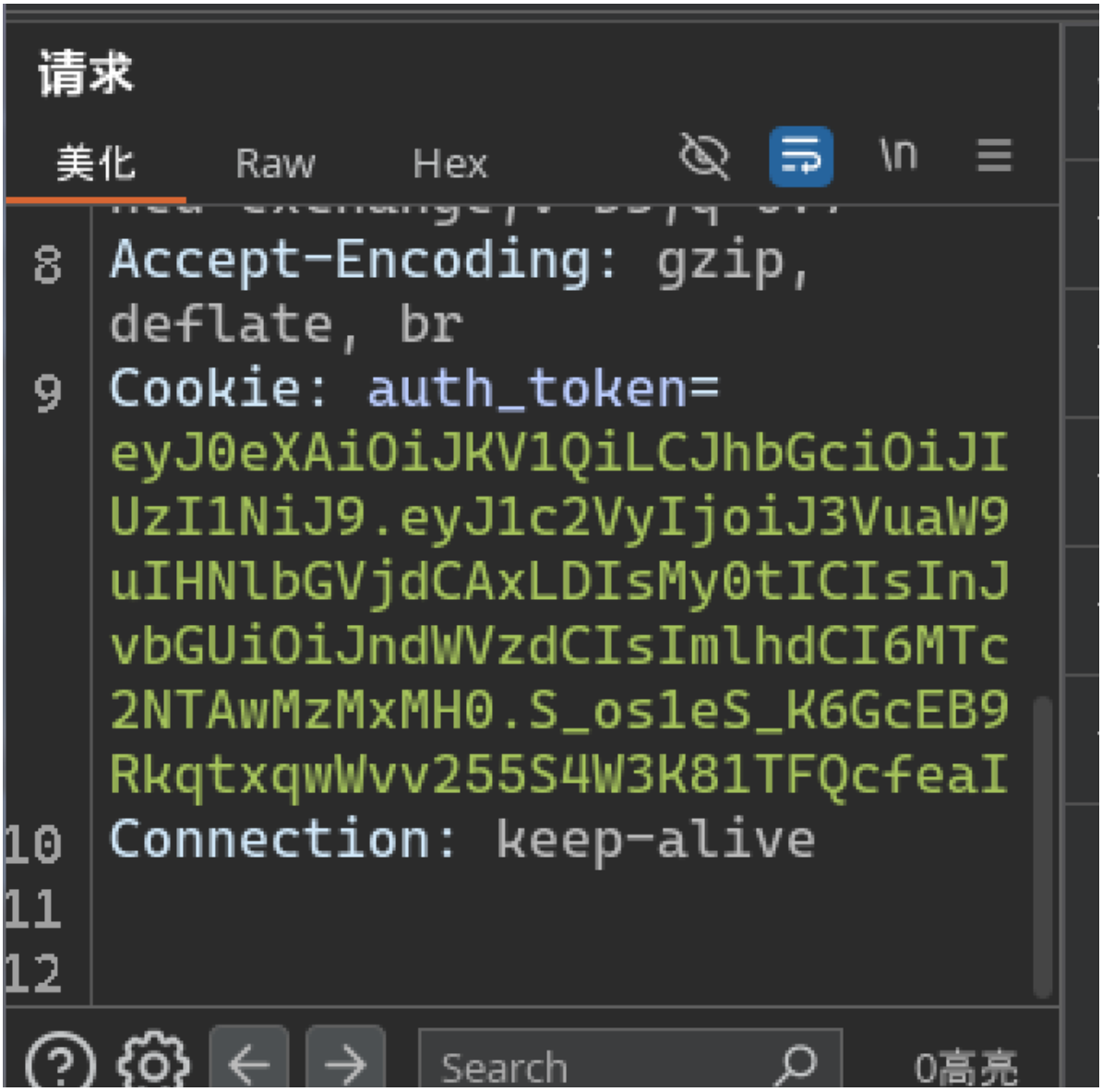


1.根据提示考sql注入，payload：’union select 1 -- 报错，是由于与前面的select的列数不同，换payload：‘union select 1,2,3 -- 成功登录

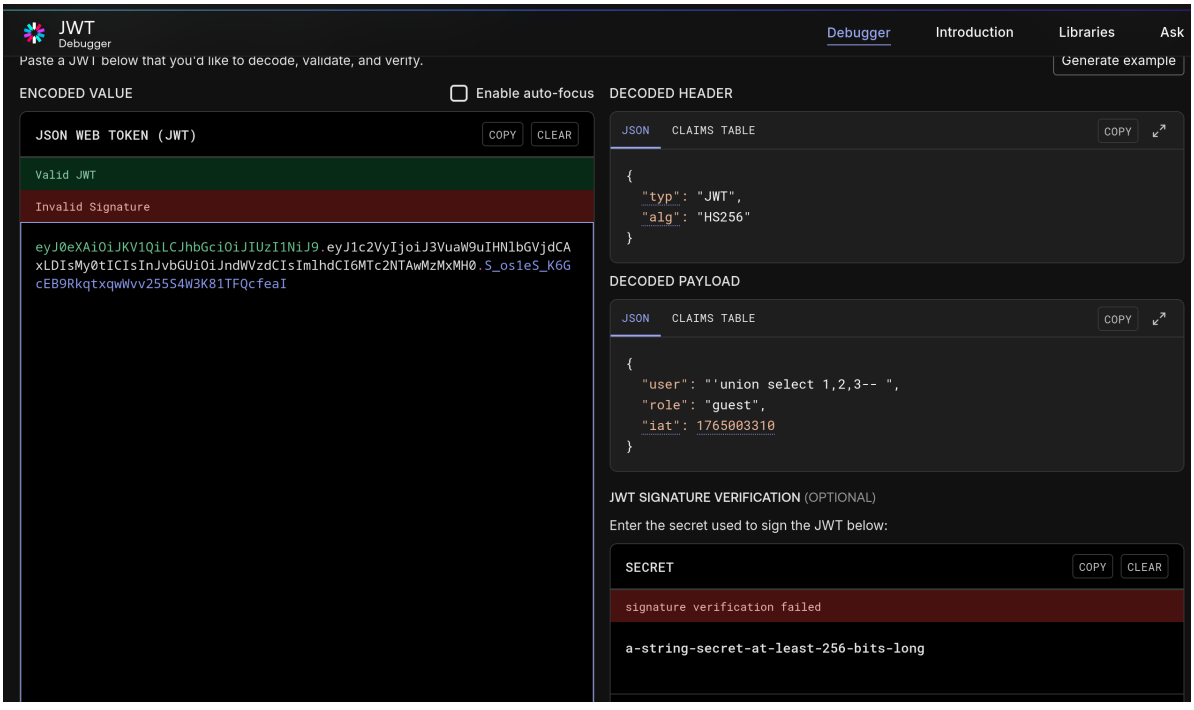




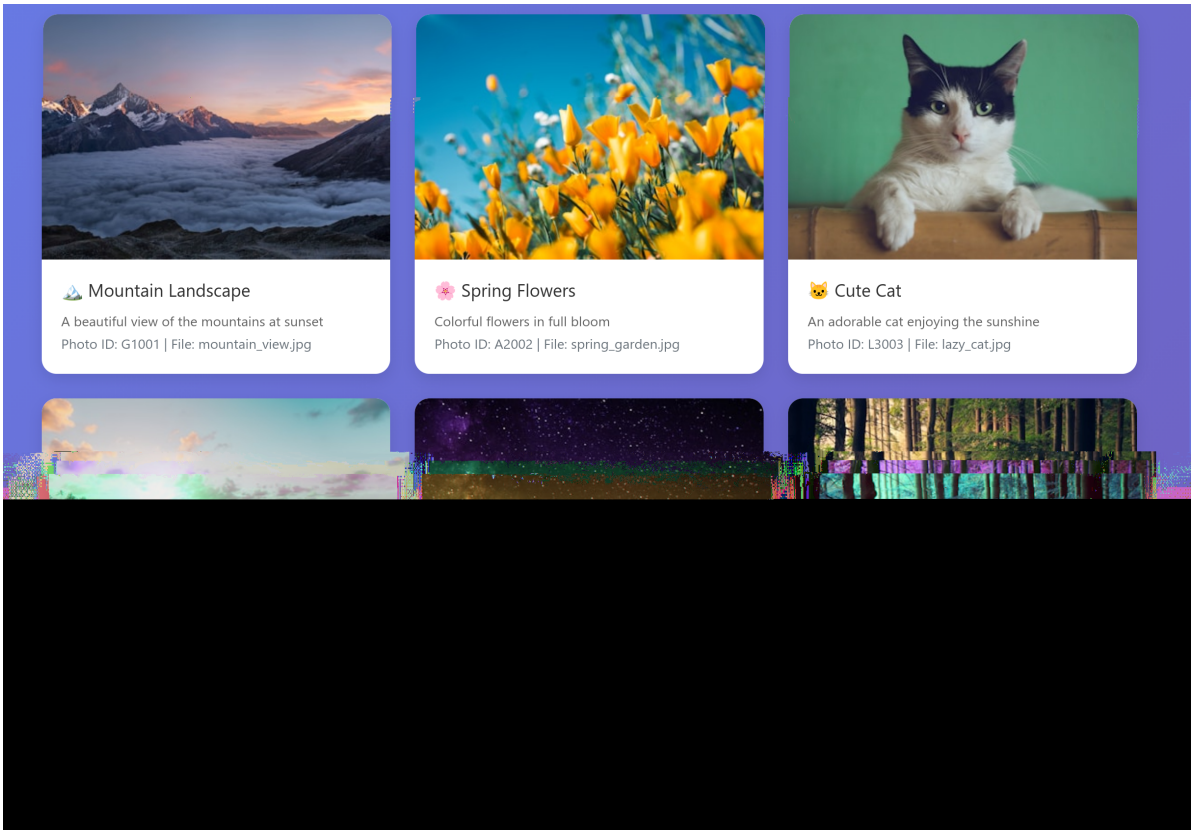
2.但是提示我是guest用户，用bp抓包发现token



3.将token赋值到jwt.io网站上发现还没有密钥

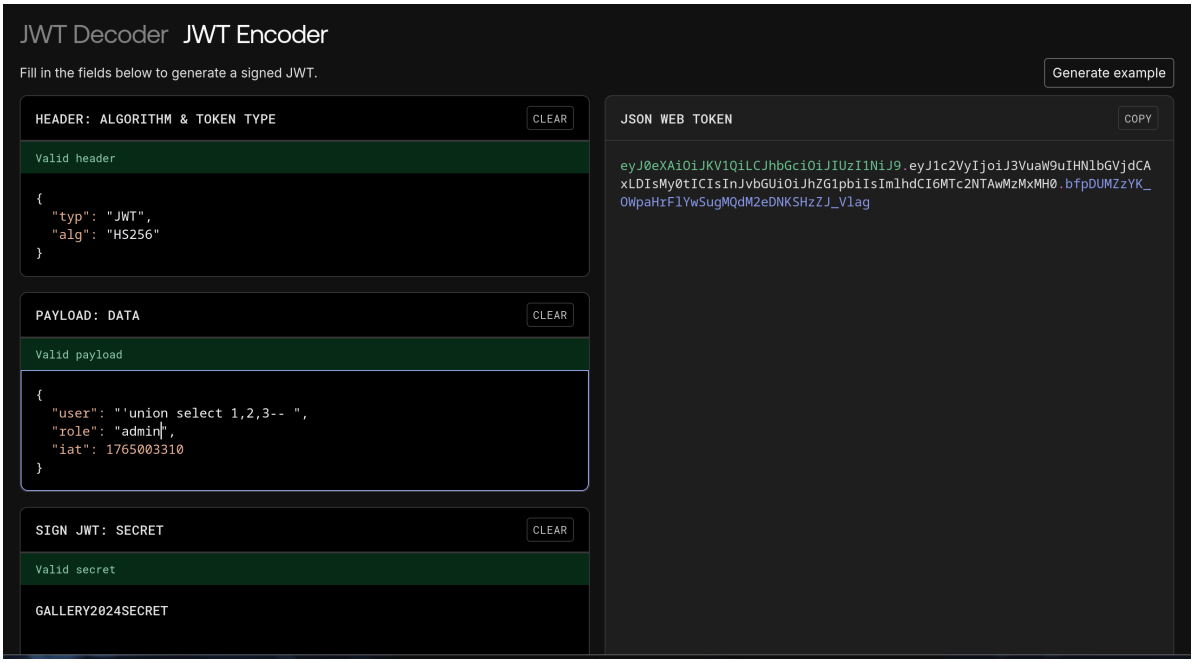


4.观察每个图片的ID，发现除了第一个字母都是有顺序的

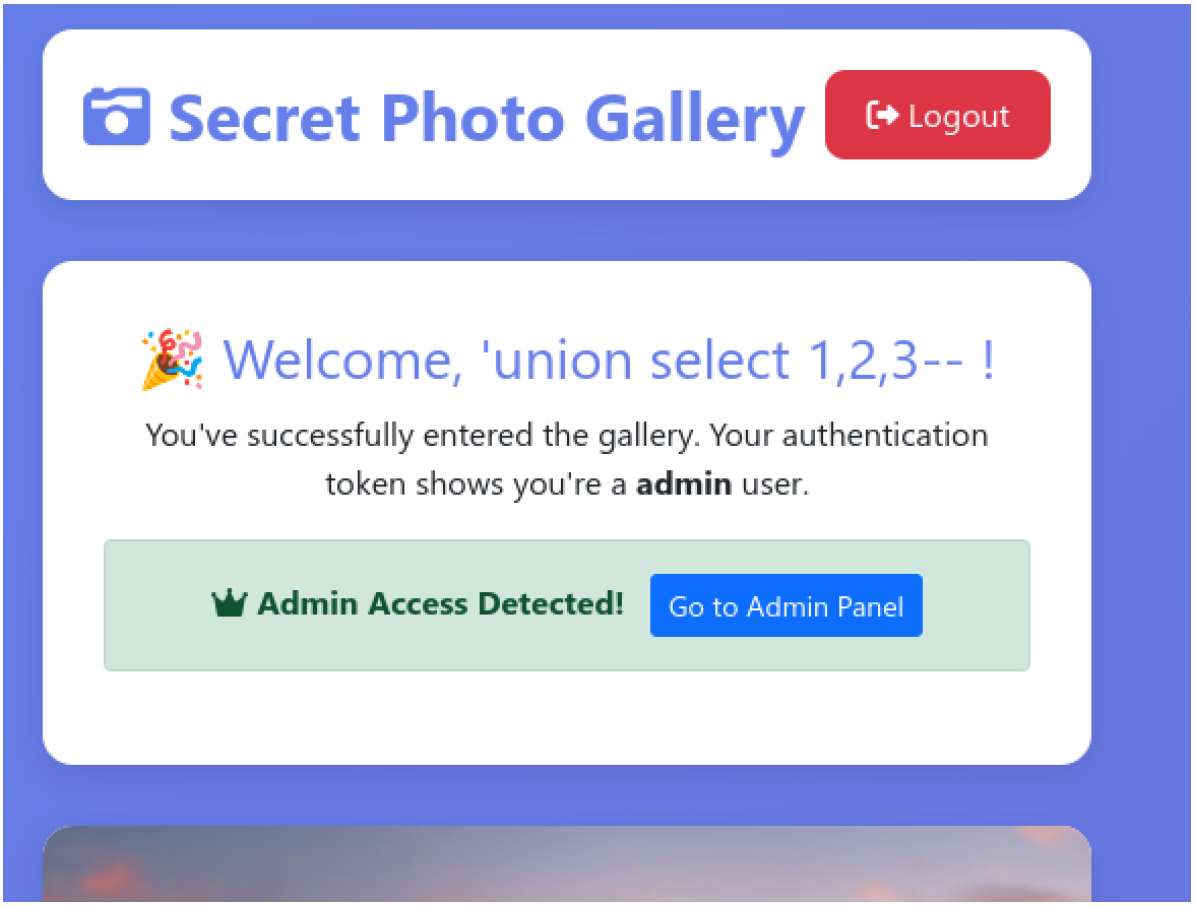


5.把每张图片的ID的第一个字符搜集起来果然是一句话

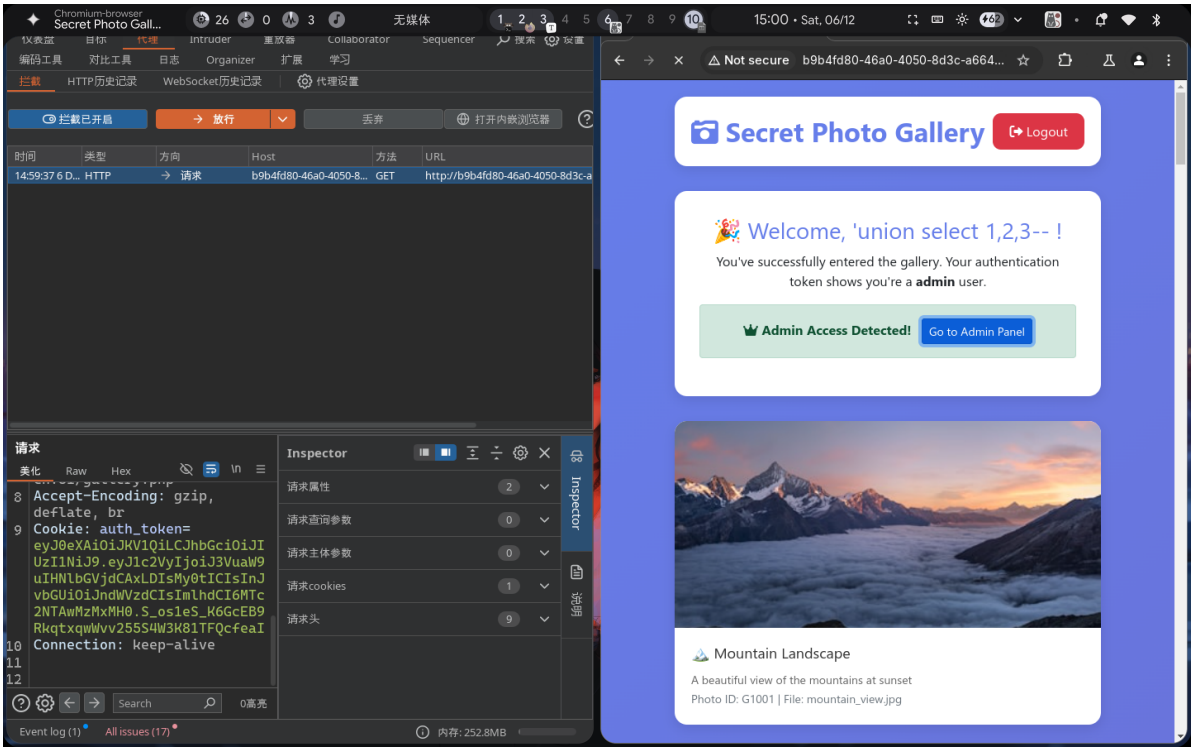
6.转到jwtencode模块，改role为admin



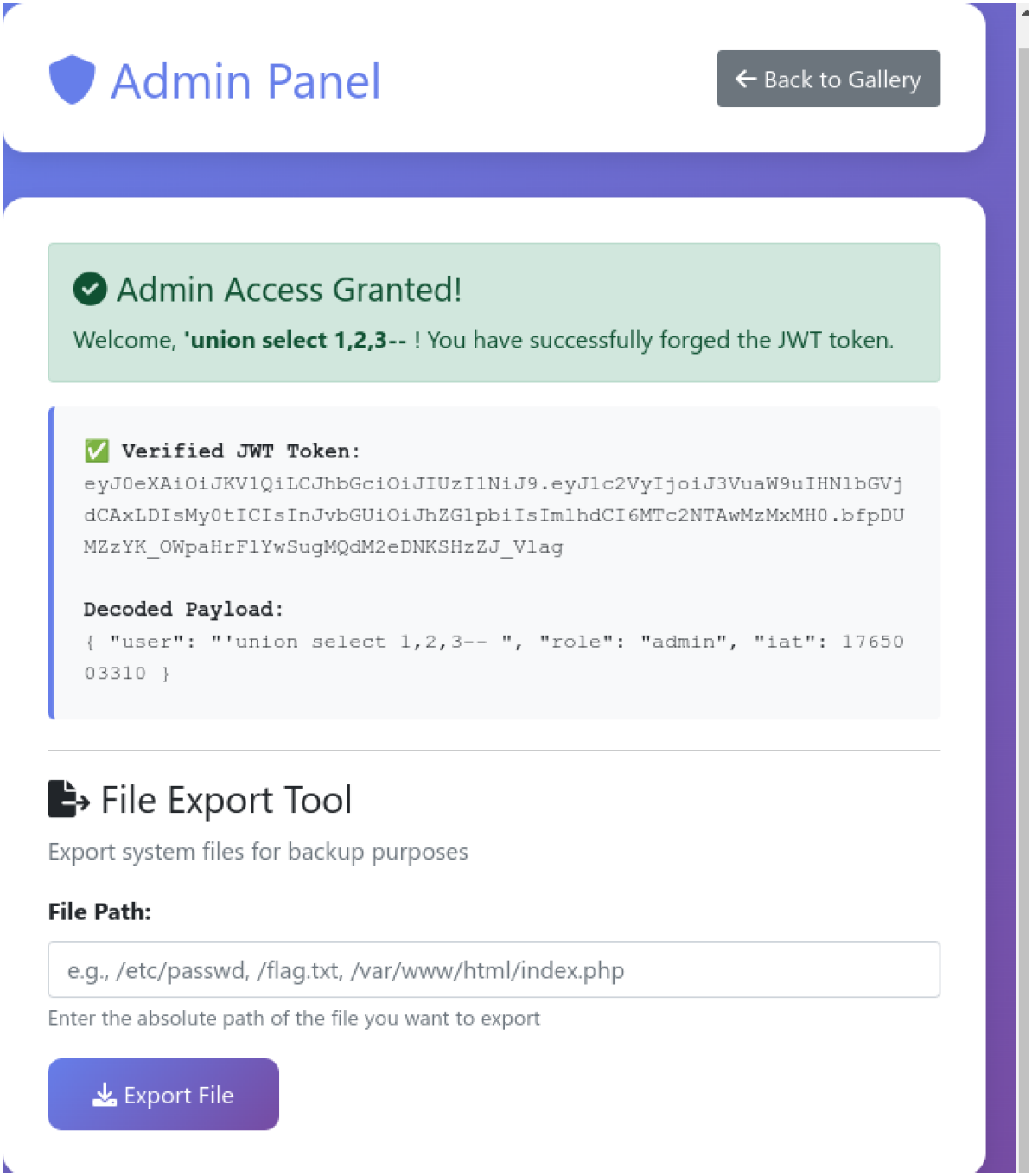
7将伪造的token赋值下来替换掉原来的token，成功成为admin user



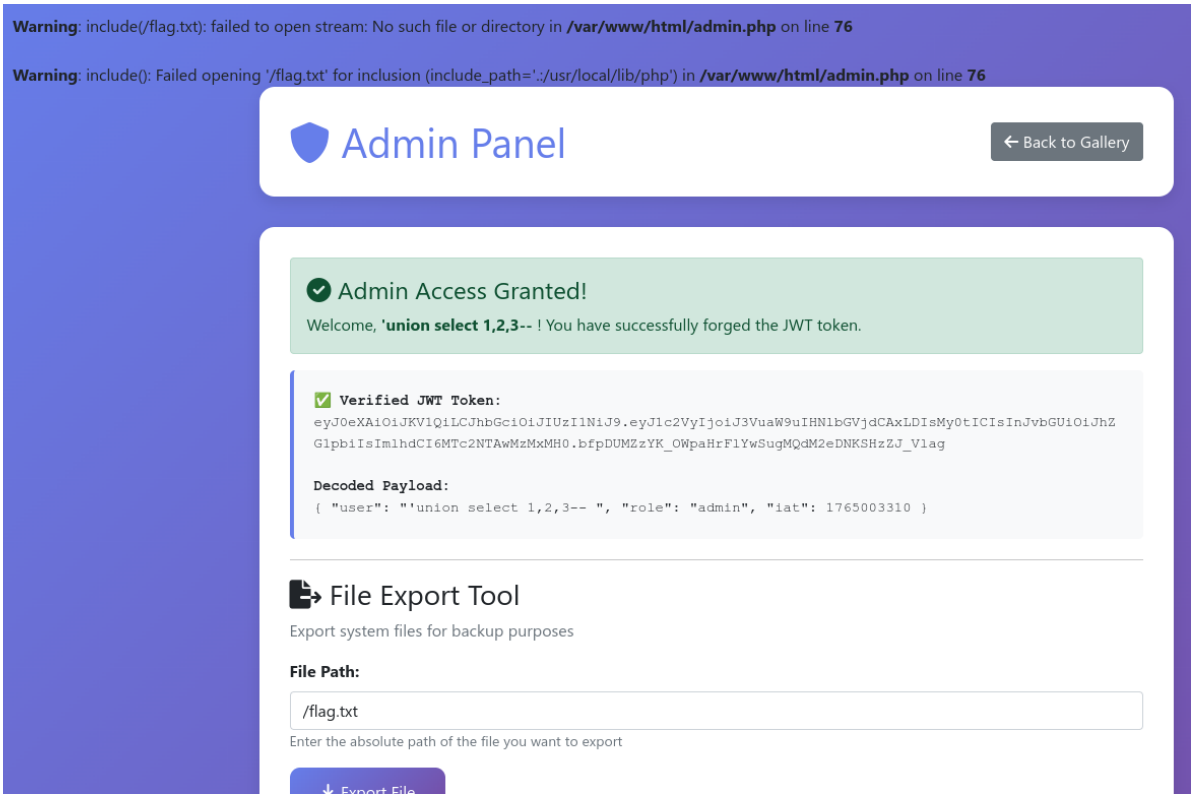
8.点击Go to Admin Panel ,再抓包，这要再替换一遍，放行



9.进入到Admin Panel在下面有一个Export file

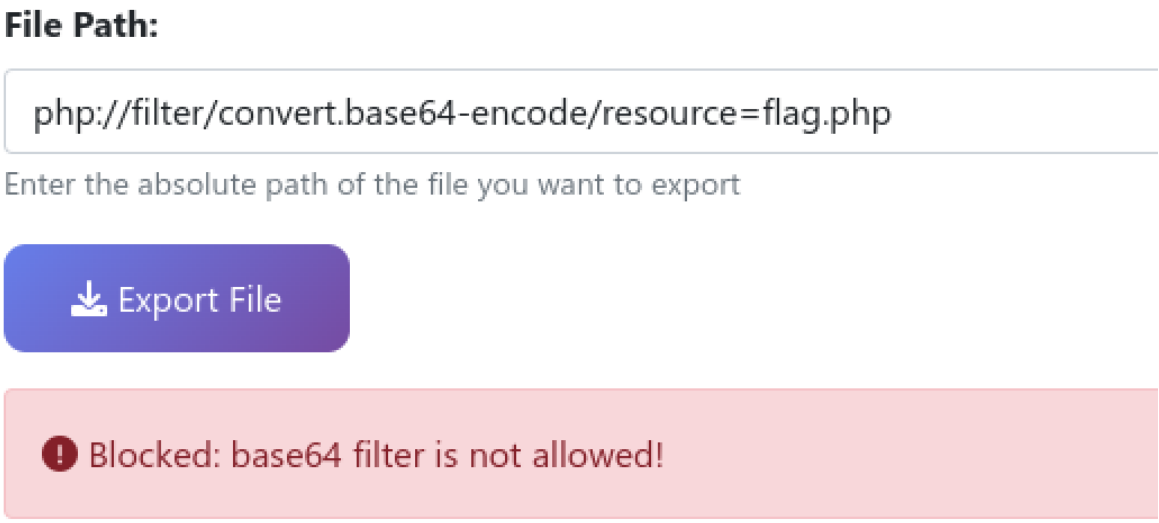


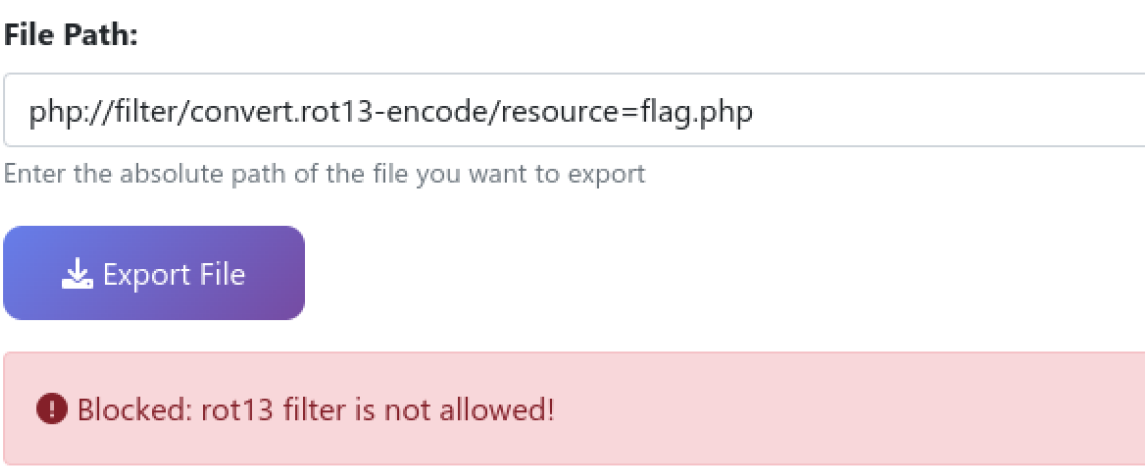
10.输入/flag.txt（Export file也要替换伪造的token），我以为要万事大吉了，结果



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





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