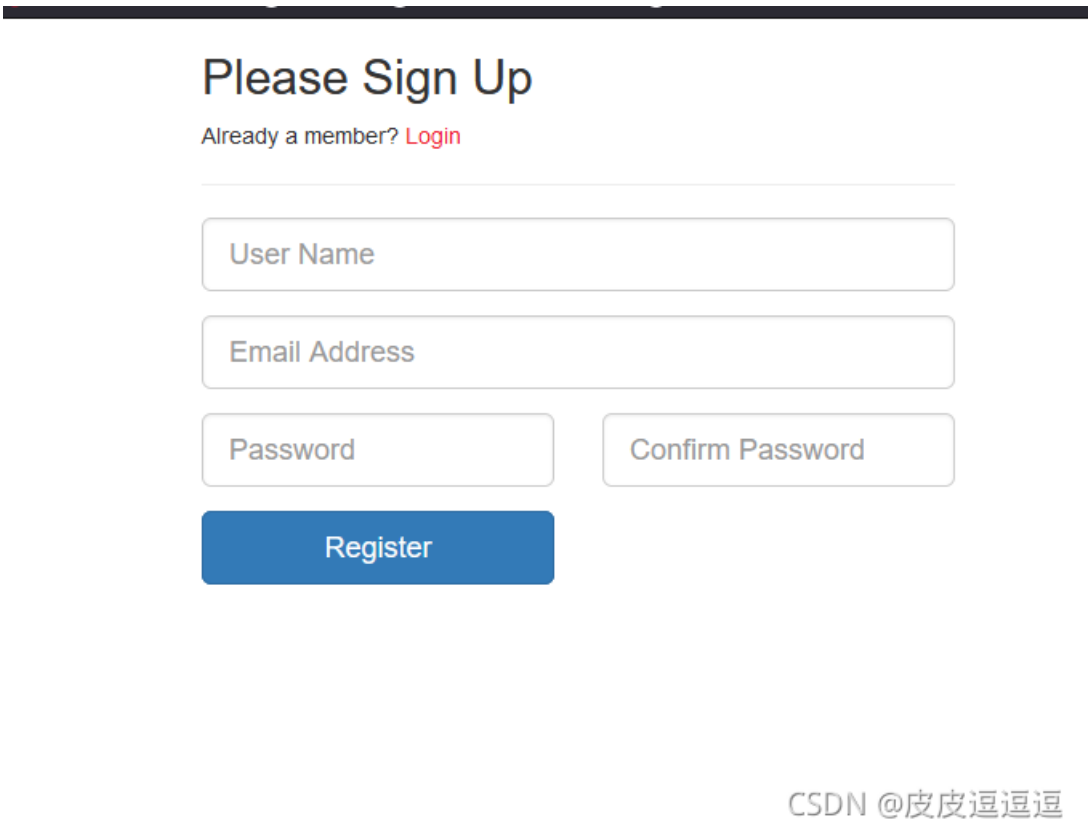
攻防世界-upload

原创

皮皮逗逗逗 于 2021-09-24 11:04:47 发布 334 收藏 1
分类专栏： #ctf 文章标签： html css

进入场景映入眼帘

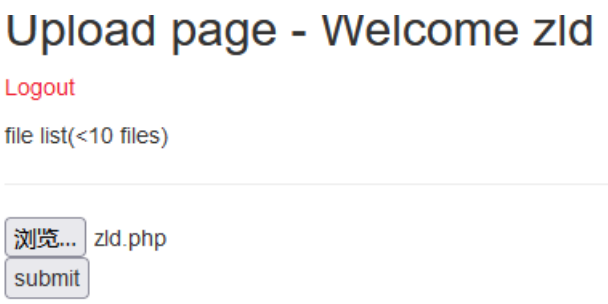


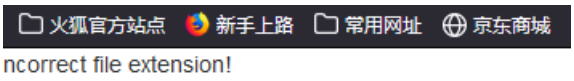
需要注册账号

注册好之后,登录跳转页面

突破点应该就在这里了

我们先上传一个php文件





ncorrect file extension!

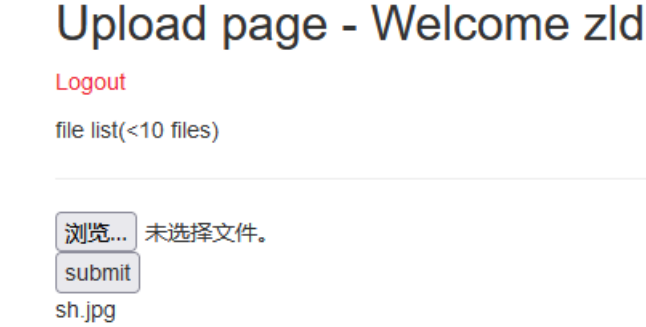
显示不正确的文件扩展名,被拦了

用burp抓包改信息

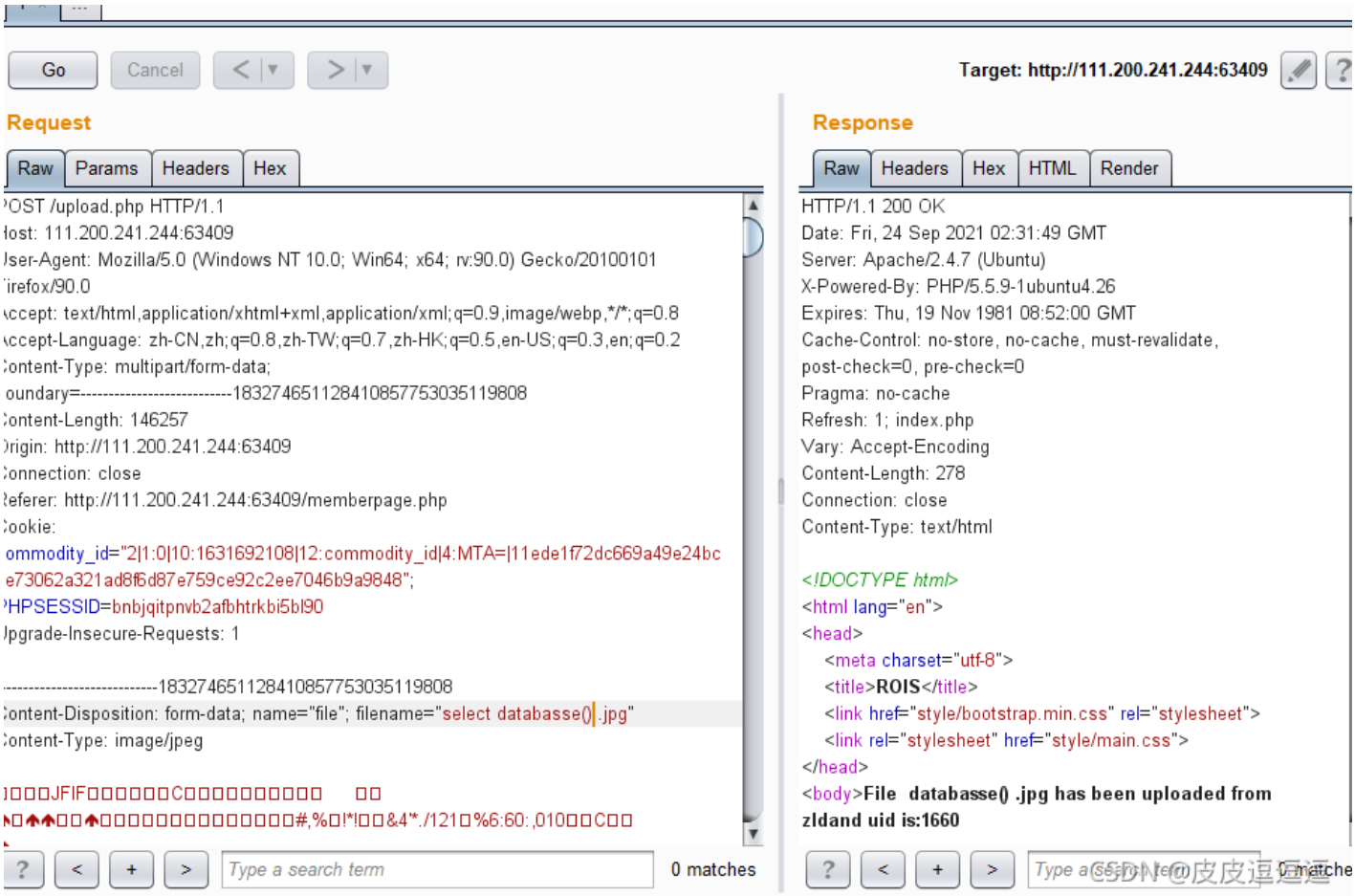
成功上传 但是没有上传路径 只能上传不能利用

思考(题目给的是upload,给的引导思路 就是上传文件拿flag)

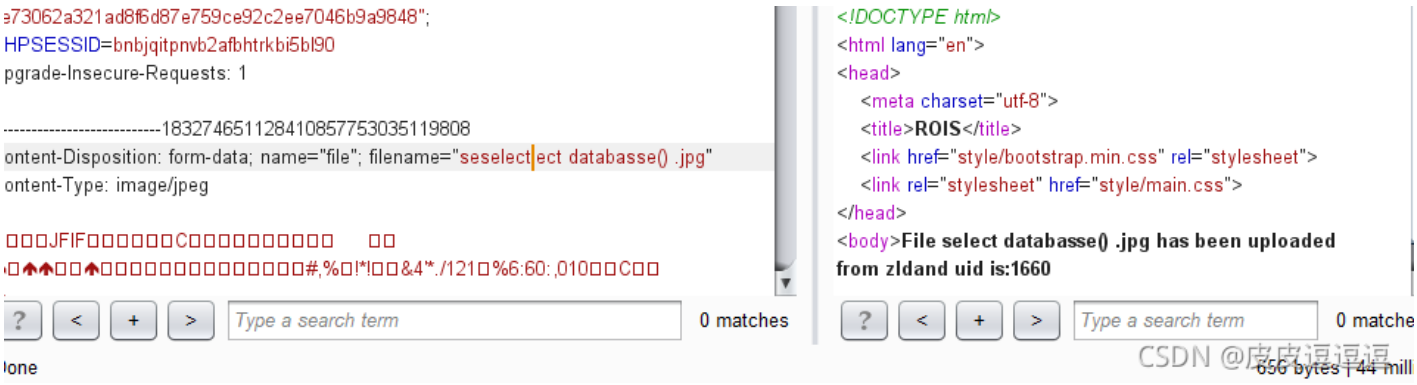
我试着上传jpg,png格式的图片文件



有文件名回显,这说明文件已经被传到了数据库中,游览器又从数据库中读取了上传的文件,那么这个过程久有可能触发sql注入,那么将文件名中加入sql语句,尝试burp抓包修改



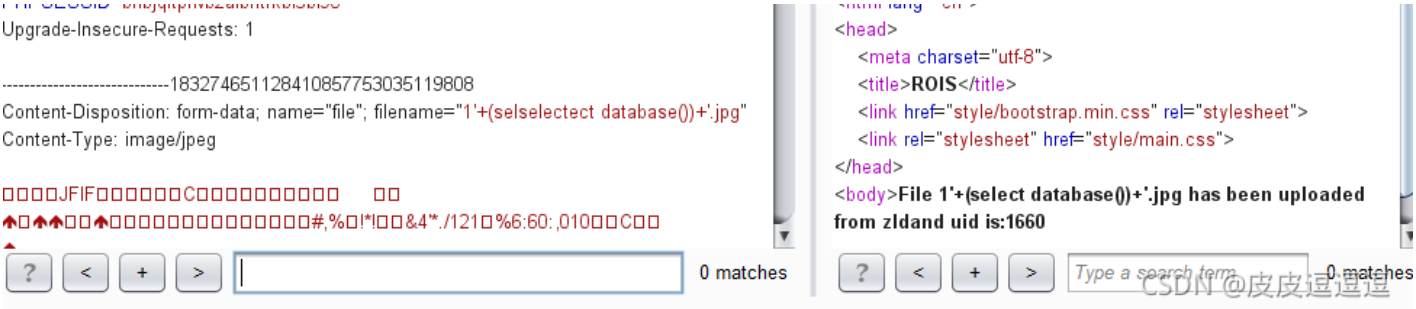
可以看出select被过滤了,之后的尝试 from也被过滤了,那么尝试双写绕过



双写绕过成功

由此可以得出结论肯能存在sql注入.

尝试去验证sql注入的存在



浏览... 未选择文件。
submit
sh.jpg
databasse() .jpg
select databasse() .jpg
1
sh.jpg

sql语句是执行了,但无法输出执行结果.(可能数据被过滤掉了)

那么尝试将查询结果改为16进制输出

输出7765626(7765625 + 1) 用16进制解码字符串为web.

这里有个坑，插入数据库文件名中如果包括SQL语句，在返回信息时，服务器将对字母进行截断（某些特殊字符也会截断或过滤） 尝试用10进制表示 conv函数(src,from_base,to_base) src是要转换的数据, from_base是原进制, to_base是目标进制.

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

构造payload '+(selselectect conv(hex(database()),16,10))+'.jpg

用了科学计数法(估计是数字太长了,这里就需要截断获取数据了

构造payload：'+(selselectect conv(substr(hex(database()),1,12),16,10))+ '.jpg (经过测试发现长度最大为12,超过12 就会返回科学计数法表示)

通过解码得到web_up

取下一段'+(selselectect conv(substr(hex(database()),13,12),16,10))+ '.jpg

解码得load拼起来得web_load

有看库名,就开始爆表名,再之后是字段名

不再一一赘述 方法类似

最后得到flag

!!_@m_Th.e_F!lag