i春秋 “百度杯”CTF比赛 九月场 SQLi writeup

J-1547 于 2020-01-12 16:21:06 发布 331 收藏

分类专栏： 笔记

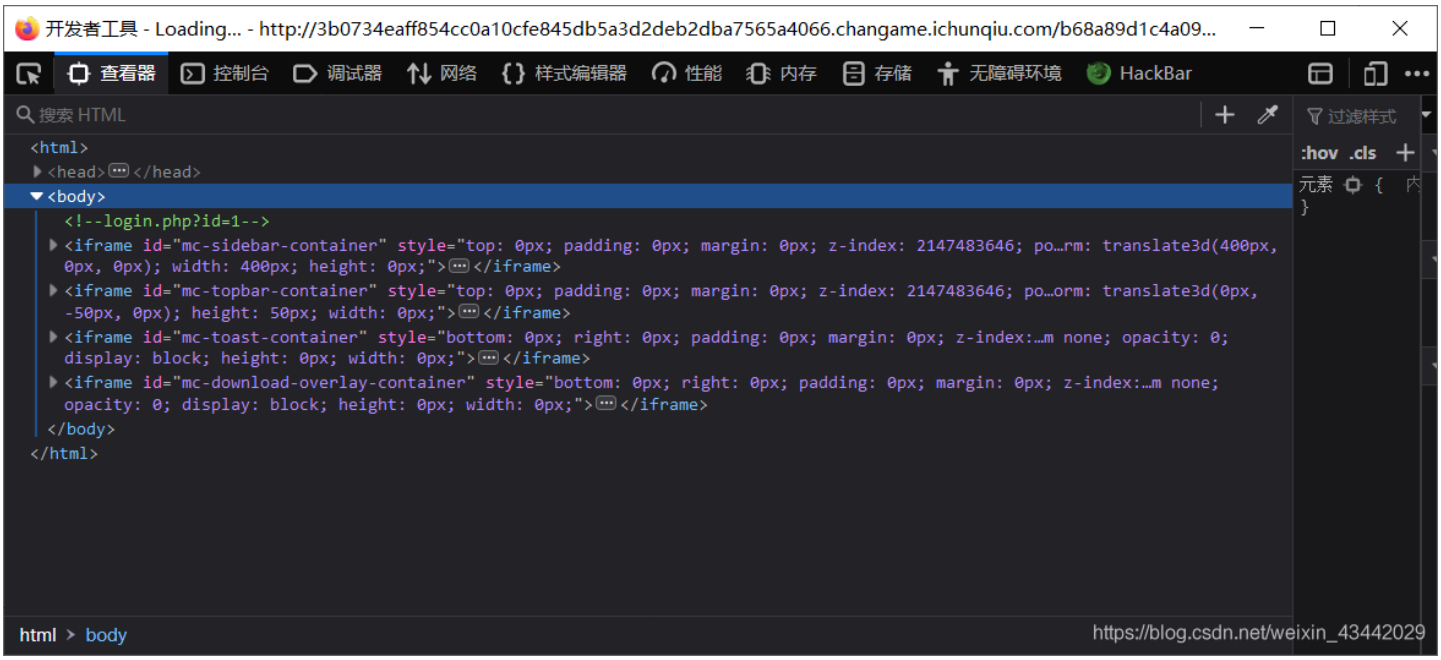
笔记 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

0x00

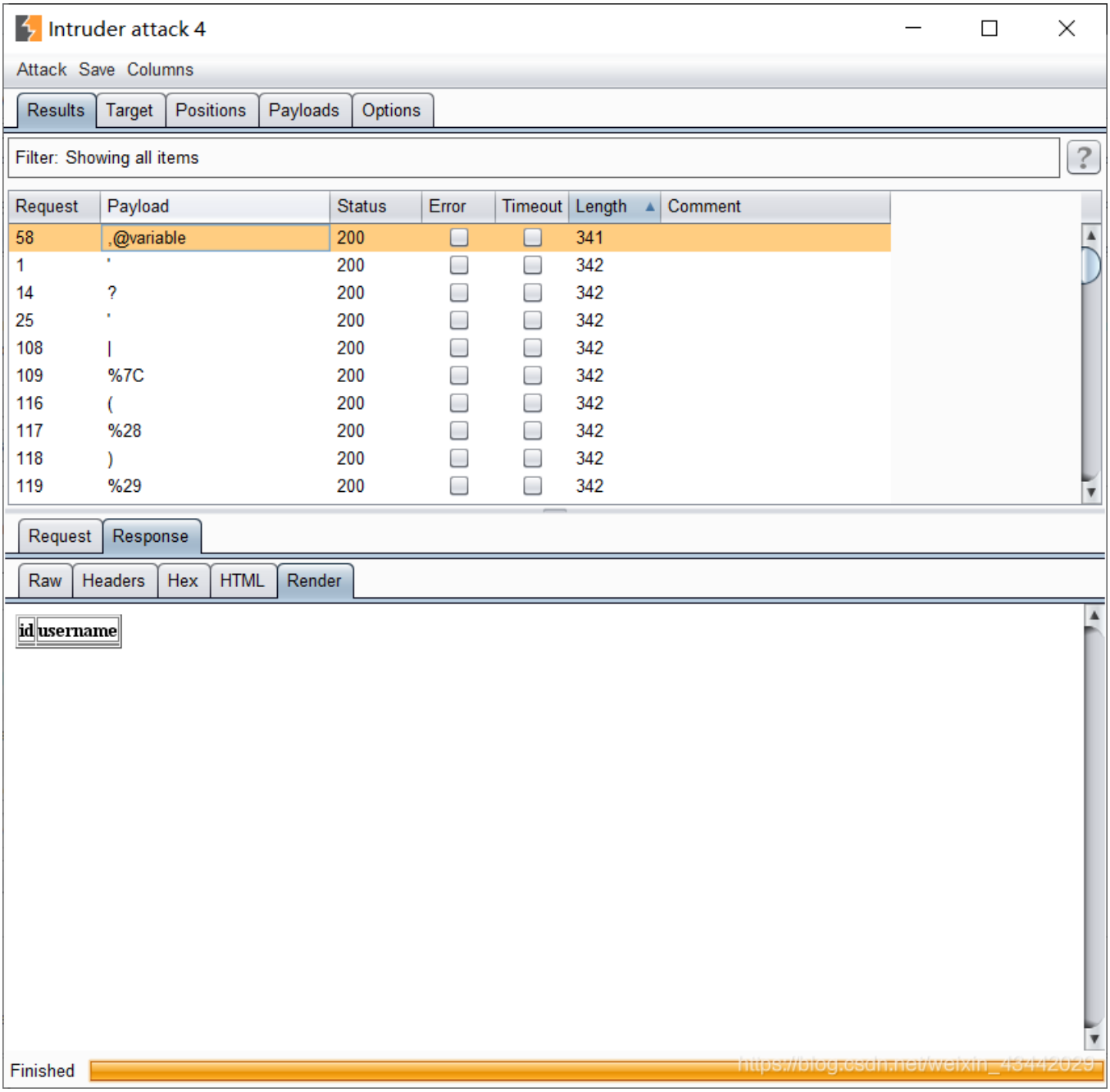
打开题目链接后是一个空白页面，老规矩，去源代码找线索，于是就发现了提示login.php?id=1。



由题目可以知道这一题是SQL注入有关，那url的参数id应该就是注入点了。不过我试了好几次都没有特殊的回显，后来在网上搜到一些提示说真正的页面是l0gin.php。不得不说出题人和解出来的人脑洞是真的大。（不过之后做了一些其他题目后才发现这次比赛的出题人很喜欢这样的命名方式，可能是这样想出来的吧）

0x01

访问l0gin.php后发现是典型的sql注入的回显界面。于是我先用burpsuite跑sqli fuzzing字典，发现后台对逗号以后的输入做了截断处理。



于是就上网找无逗号注入的方法，发现可以用join 来替代逗号。

举个例子：

普通的sql注入语句：

```
union select group_concat(table_name) from information_schema.tables where table_schema=database(),user()
```

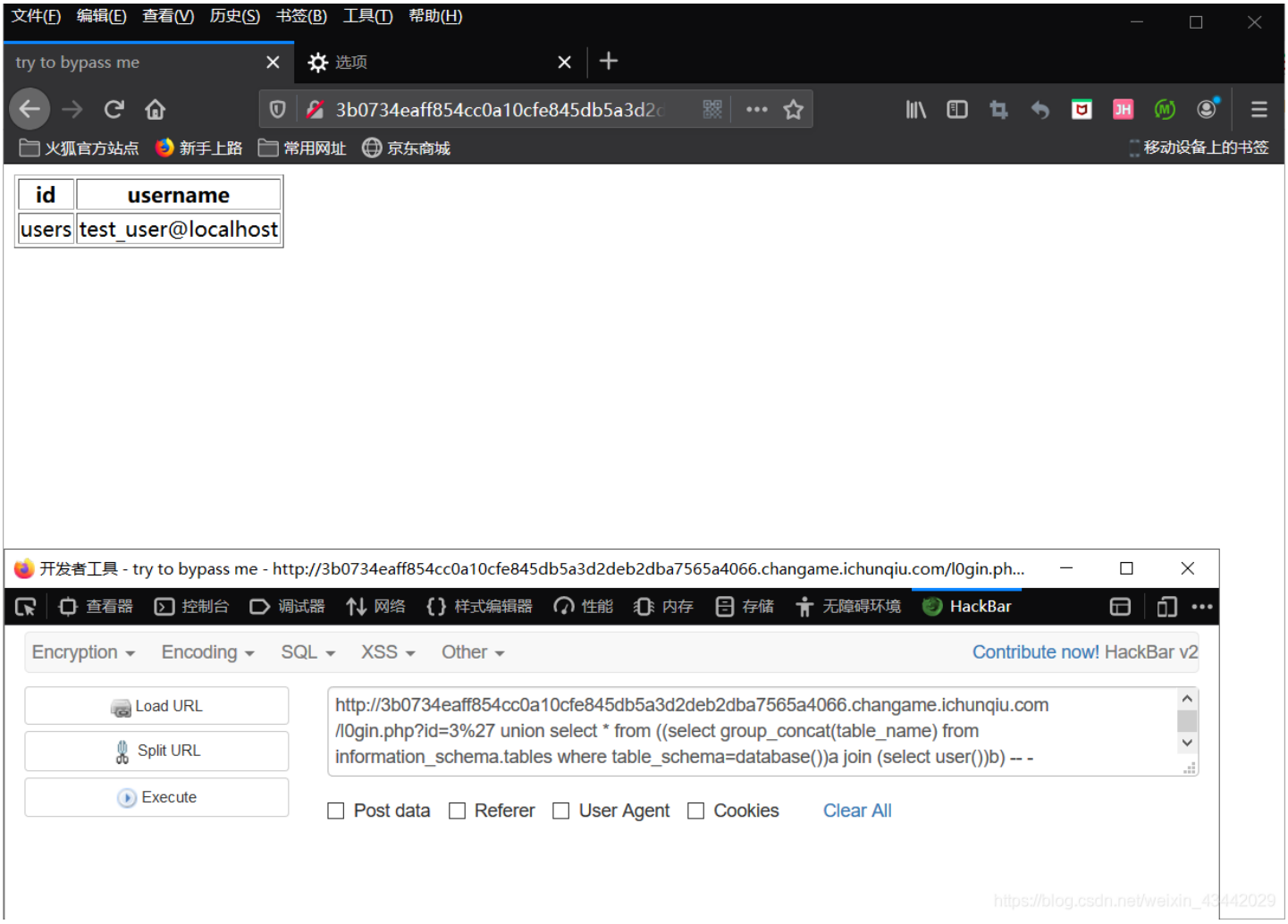
使用join的无逗号注入语句：

```
union select * from ((select group_concat(table_name) from information_schema.tables where table_schema=database())a join (select user())b)
```

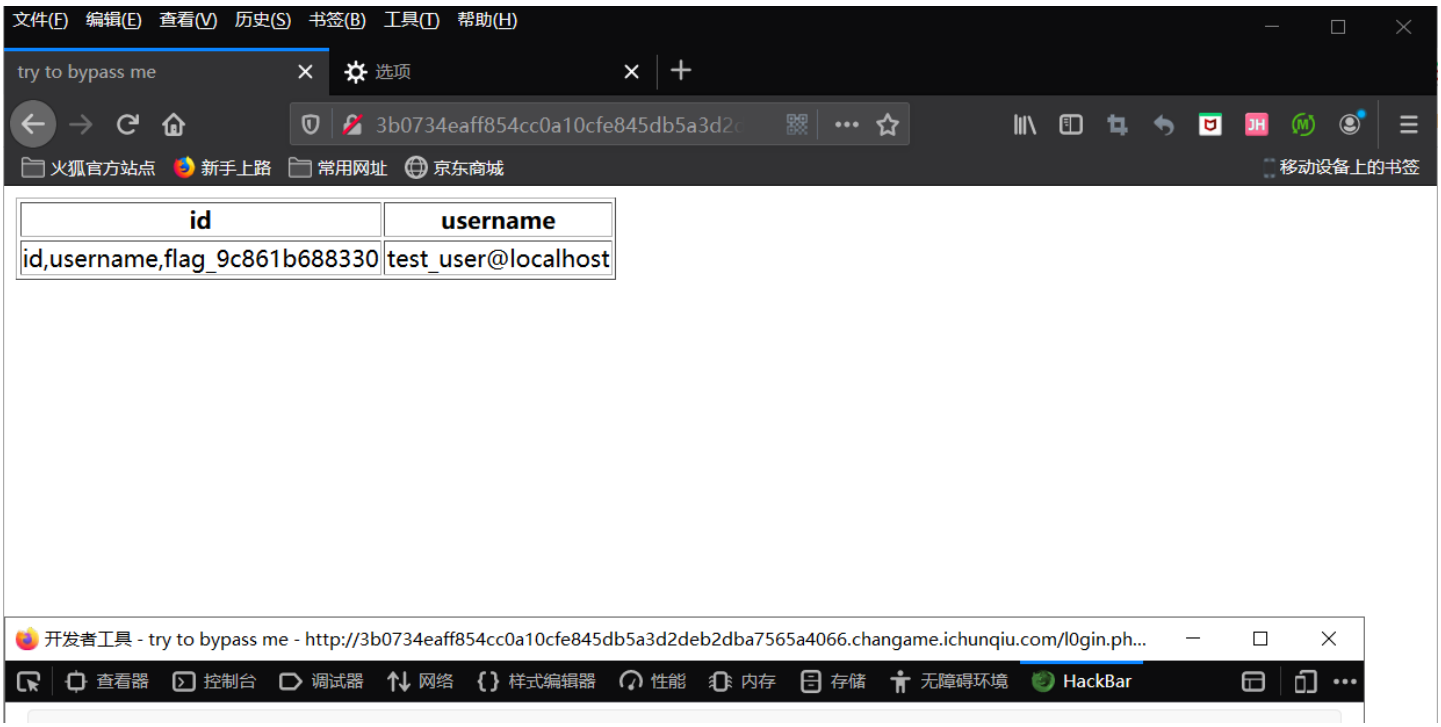
0x02

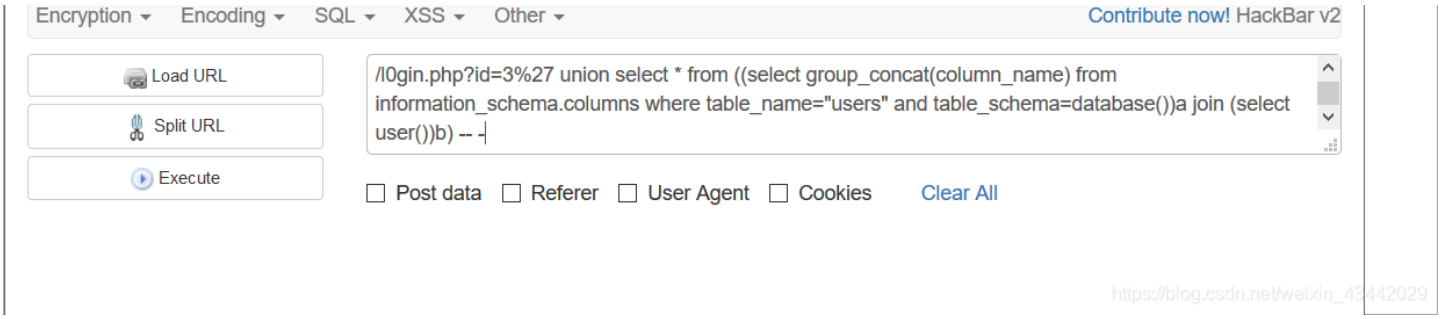
后续就是正常的sql注入流程了

爆表名

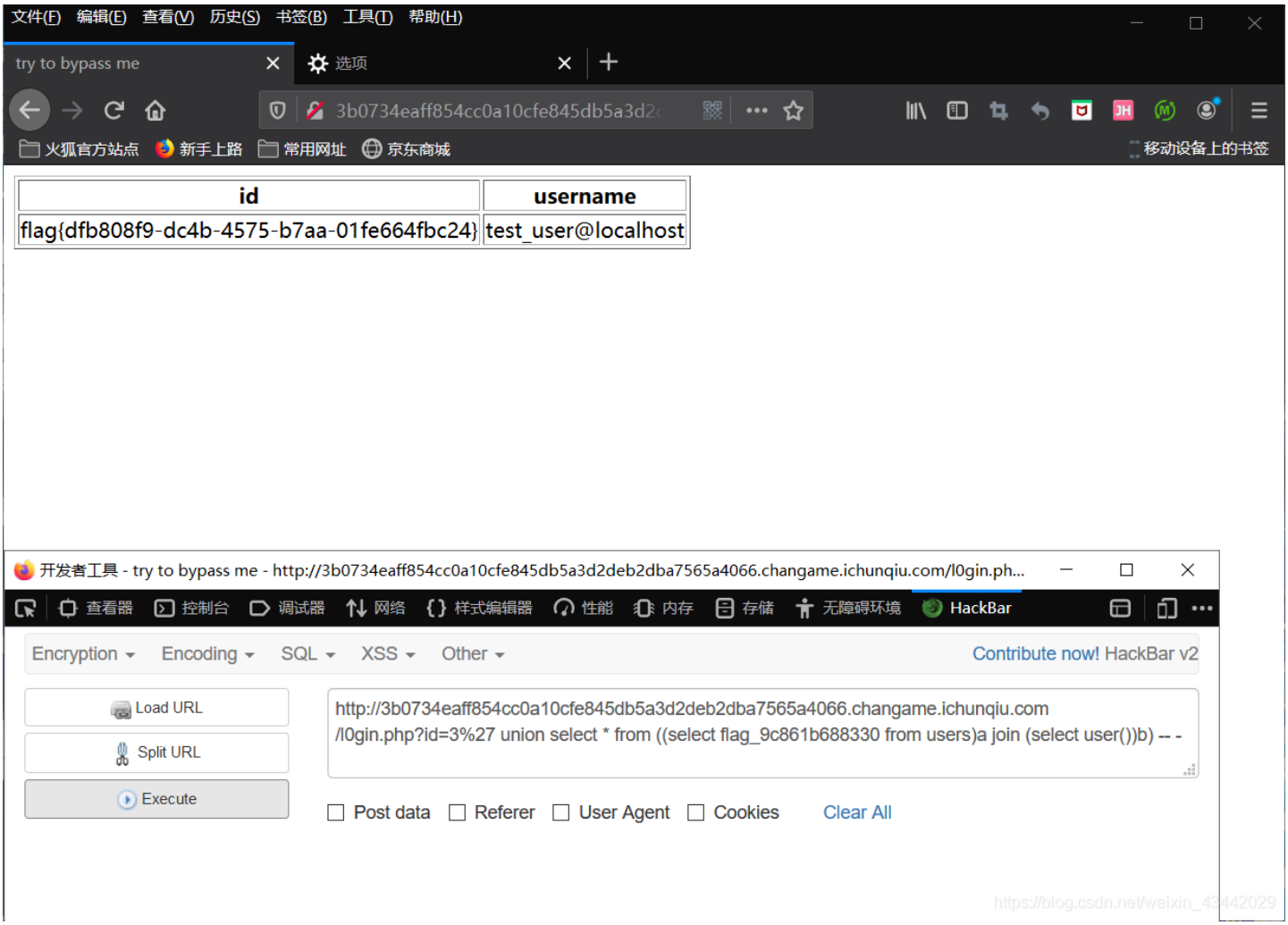


爆字段名





最后拿到flag



后话

这里还有一个坑：
最后的注释语句我一开始用的是“#”来注释，但是并没有正确的回显，后来又试了“-- ”，“--+”之类的注释，最后只有“-- -”有正确的回显。这一点我暂时还没有弄清楚。