

# BUUCTF笔记

原创

[Ordsh1ne](#)  于 2021-07-25 13:43:04 发布  42  收藏

分类专栏: [笔记](#)

本文为明哥原创文章, 未经本文博主允许不得转载, 否则将追究法律责任

本文链接: <https://blog.csdn.net/curryzb/article/details/119047657>

版权



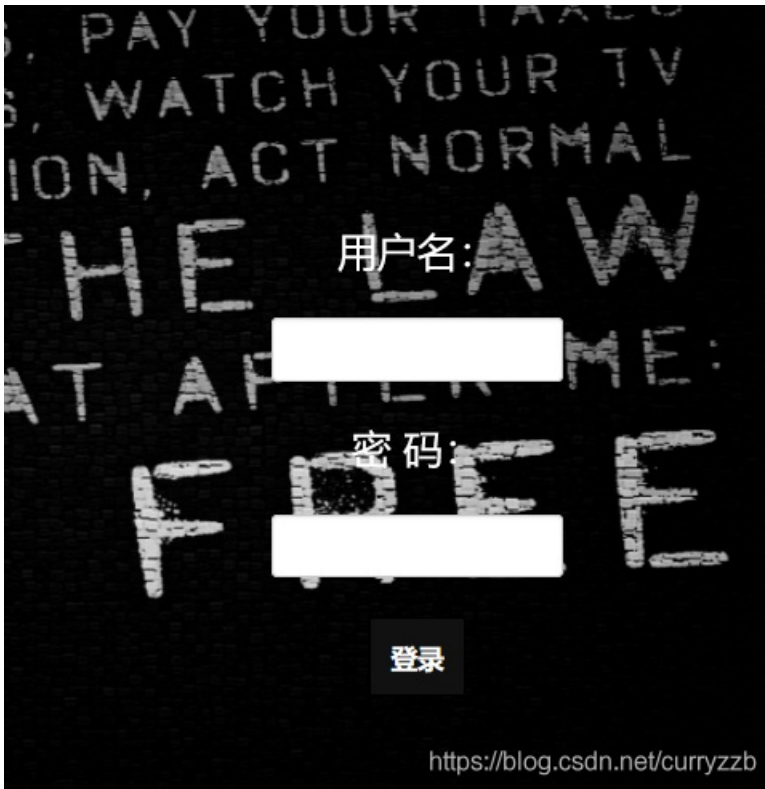
[笔记](#) 专栏收录该内容

9 篇文章 0 订阅

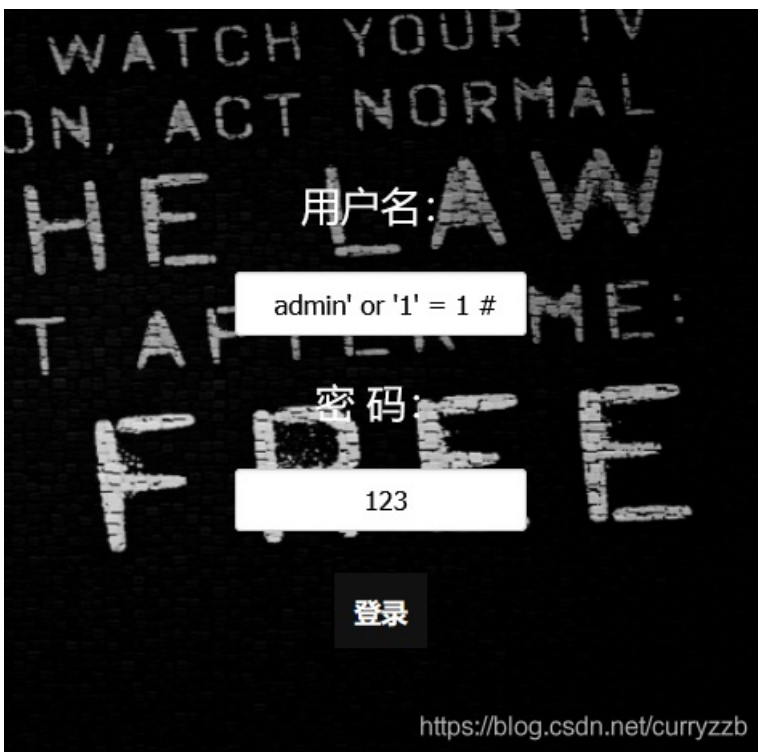
订阅专栏

## EasySQL

明显的SQL注入题

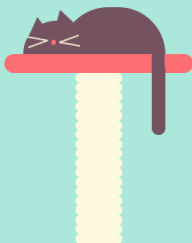


直接尝试万能密码



获得flag

[极客大挑战 2019]Havefun 1



Syclover @ cl4y

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

查看前端代码

```
<!DOCTYPE HTML>
<html> 滚动
  <head> ... </head>
  <body> flex 溢出
    <div class="main"> ... </div>
    <!--$cat=$_GET['cat']; echo $cat; if($cat=='dog'){ echo 'Syc{cat_cat_cat_cat}'; }-->
    <div style="position: absolute;bottom: 0;width: 99%;"> ... </div>
  </body>
</html>
```

可以看出，get提交参数给cat赋值，当cat的值为dog，就会得到flag

构造url

```
node4.buuoj.cn/?cat=dog
```

得到flag

[SUCTF 2019]EasySQL 1（未完）

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传

---

Give me your flag, I will tell you if the flag is right.

提交查询

直接上万能密码进行尝试, ' or 1=1 # , 提示Nonono. order by也不行, 看来对注入语句有验证, 联合注入应该是不行, 并且也没有报错信息

尝试输入个1, 回显 Array ( [0] => 1 )

再次尝试字母a, 没有回显

但是页面会进行相应的变化, 证明注入漏洞肯定是有

联合, 报错, 都不行, 又尝试盲注, 还是nonononono。。。

找找大佬的WP,

行, 又尝试盲注, 还是nonononono。。。

- [找找大佬的WP,](#)