

i春秋“百度杯”CTF比赛 十月场 Gift

原创

[「已注销」](#) 于 2018-10-24 13:22:39 发布 2052 收藏

分类专栏: [春秋](#) 文章标签: [gift](#) [ctf](#) [百度杯](#)

友链: <https://cutt.ly/7777aaaa>

本文链接: https://blog.csdn.net/include_heqile/article/details/83342576

版权



[春秋](#) 专栏收录该内容

19 篇文章 0 订阅

订阅专栏

欢迎扫码关注微信公众号

回复关键字【资料】获取各种学习资料



微信搜一搜

Q 我吃你家米了

https://blog.csdn.net/include_heqile/

<https://www.ichunqiu.com/battalion?t=1&r=0>

进入题目链接，是一张黑人问号图片：



直接使用 [burp suite](#) 抓包送到 [Repeater](#) 模块，检查发送和相应报文的 [HTTP](#) 头部字段，并未发现可疑字段，图片是 [base64](#) 编码，点击 [href](#) 链接，依然还是刚的页面，尝试更改请求方法，将 [GET](#) 更改为 [POST](#)，响应如下：

Forbidden (403)

CSRF verification failed. Request aborted.

You may notice this message because this site requires a CSRF token when

You are seeing this message because this site requires a CSRF cookie when submitting forms. This cookie is required for security reasons, to ensure that your browser is not being hijacked by third parties.

If you have configured your browser to disable cookies, please re-enable them, at least for this site, or for 'same-origin' requests.

More information is available with `DEBUG=True`.

如果了解过 Django 的话应该很容易看出来这是 Django 的报错页面，这一点可以从红色箭头指向的地方看出来，下面是一张 Django 的初始界面，对比一下：

django

[View release notes for Django 2.1](#)



The install worked successfully! Congratulations!

You are seeing this page because `DEBUG=True` is in your settings file and you have not configured any URLs.

 **Django Documentation**
Topics, references, & how-to's

 **Tutorial: A Polling App**
Get started with Django

 **Django Community**
Connect, get help, or contribute

下面的工作就是去搜索往年的与 Django 有关的 write up，找到一篇：

<https://bbs.ichunqiu.com/thread-14365-1-1.html>

???

然后我就去看了一下他的 github 页面，找到了对应的文件，并下载了下来，提示说密码是他的生日，那我们直接制作字典并爆破即可

字典制作代码：

```
#include <stdio.h>

#include <stdio.h>

int main()
{
    int year = 0, month = 0, day = 0;
    for(year=1990; year<=2018; year++)
        for(month=1; month<=12; month++)
            for(day=1; day<=31; day++)
                printf("%d%02d%02d\n", year, month, day);
    return 0;
}
```

```
$ gcc getPasswd.c -o getPasswd
https://blog.csdn.net/include_heqile
$ ./getPasswd > password.txt
```

爆破脚本代码:

```
#!/bin/bash

cat ./password.txt | while read LINE
do
    #将标准错误和标准输出都重定向至文件123中
    unzip -P "$LINE" gift.zip > 123 2>&1
    grep -q "bad" ./123
    if [ $? -eq "0" ]; then
        rm -rf S*
        continue
    else
        grep -q "incorrect" ./123
        if [ $? -eq "0" ]; then
            echo "wrong password"
            continue
        else
            echo $LINE
            break
        fi
    fi
done
```

当我们给 `unzip` 提供错误的密码有时也能将文件解密，但是会提示:

```
Archive:  gift.zip
extracting: SECRET_KEY.KEY          bad CRC 0e4c3140 (should be 0c451838)
(may instead be incorrect password) https://blog.csdn.net/include_heqile
```

因此我们先检查输出中是否存在字符串 `bad` (因为 `incorrect` 在两种情况中都会出现, `bad` 只会出现在这种情况中)

最后执行 `getPasswd.sh`, 成功获得压缩包密码:

