登录

DedeCMS前台鸡助Getshell漏洞

phpoop / 2018-01-22 15:13:00 / 浏览数 11842 安全技术 漏洞分析 顶(1) 踩(0)

0x00 介绍

织梦5.7会员中心，由于为了安全性问题，限制了注册会员在会员中心发布信息的时候上传图片，但是管理员登录会员中心发布信息的时候上传图片却不受影响。那该如何解

首先，具体的问题为，注册会员点击图片上传，预览选择好本地图后点击上传到服务器上，会出现如下所示结果：

图片上传失败，并无像正常上传图片后提交按钮跳转到相应的图像属性界面上，仅在当前窗口上弹出一个滚动条，上面的滚动条里面提示为"提示：需输入后台管理目录才能

现在知道具体原因后就容易解决问题了，直接搜索织梦网站程序文件夹下的全部包含"提示：需输入后台管理目录才能登陆"的文件，找到include\dialog\config.php文件。

```
//■■■■■■■■■
$cuserLogin = new userLogin();

if($cuserLogin->getUserID() <=0 )
{
   if(empty($adminDirHand))
   {
       ShowMsg("<b>■■■■■■■■■■■■■■■■■■</b><br /><form>■■■■■■■■■■■■<input type='hidden' name='gotopage' value='".urlencode($
       exit();
   }
   $adminDirHand = HtmlReplace($adminDirHand, 1);
   $gurl = "../../{$adminDirHand}/login.php?gotopage=".urlencode($dedeNowurl);
   echo "<script language='javascript'>location='$gurl';</script>";
   exit();
}
```

所以说dedecms5.7要上传图片的话，必须按照上面做，我们这里是按照这个规则，认为管理员开启了会员上传图片的权限，低于5.7的只要开启会员中心即可日传

扎心哦~~~~

0x01 准备工作

1,安装新版cms

地址：http://updatenew.dedecms.com/base-v57/package/DedeCMS-V5.7-UTF8-SP2.tar.gz

2, 打开dede会员功能

3,注册一个新用户

4,审核一下此用户

嗯~~~~这样一个基本的站点就完成了。我们也可以进行测试了

0x01 利用过程

1,先添加一个图片马

上图这个是经过处理的图片马，需要处理的图片马是因为（绕过文件后缀名检测以后，php-GD对图片的渲染和处理会导致webshell代码错位失效，所以需要特殊的图片马

2,

0x02 图片马制作

■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■

这里确实不要多说什么，因为绕过文件后缀名检测以后，php-GD对图片的渲染和处理会导致webshell代码错位失效，所以我们需要进行绕过。

绕过php-GD对图片的渲染和处理导致webshell代码错位失效(此处参考索马里海盗方法)

图片会经过php-GD处理，会导致webshell语句错位失效，如何在处理后仍然保留shell语句呢？

在正常图片中插入shell并无视GD图像库的处理，常规方法有两种
1.对比两张经过php-gd库转换过的gif图片，如果其中存在相同之处，这就证明这部分图片数据不会经过转换。然后我可以注入代码到这部分图片文件中，最终实现远程代码
2.利用php-gd算法上的问题进行绕过

这里我们选择第二种，使用脚本进行处理图片并绕过
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、执行图片处理脚本脚本进行处理 php jpg_payload.php x.jpg
3、如果没出错的话，新生成的文件再次经过gd库处理后，仍然能保留webshell代码语句

提示：
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
注：上面的字全部是抄的，先说明一下不然给人按在地上骂就不好了
制作过程：

0x03 漏洞原理

漏洞地址：http://127.0.0.1/DedeCMS-V5.7-UTF8-SP2/uploads/include/dialog/select_images_post.php

漏洞文件：select_images_post.php

0x04 漏洞修复

前面有提到过，没有？没看到？说的不清不楚？等官方更新版本咯。

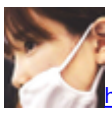
■■■http://mp.weixin.qq.com/s/IZn_xnO2tyUWmx9dronYUQ

上一篇：安全事件关联规则讨论 下一篇：Misc 总结 ----流量分析 ...
1. 7 条回复


sqvds 2018-01-22 18:49:53

搜了一下9月份好像有人发了这个洞说是和你一起审的。。

0 回复Ta


hades 2018-01-22 22:22:06

@sqvds 这个只是作为漏洞分析发出来技术探讨，难道漏洞分析的时候你们都要去找谁发现的额？？
试着想想为什么两篇文章的开头是一样的，而下面的内容不是一样的？？？

0 回复Ta


sqvds 2018-01-22 23:49:11

@hades 抱歉，我只是随便说说，无所谓你们谁发现的，你太敏感了

0 回复Ta


hades 2018-01-23 00:02:07

@sqvds 漏洞发现者比较敏感 呵呵哒 我没什么的 哇哈哈

0 回复Ta


hades 2018-01-23 09:33:48

@phpice 后台再次编辑有问题，先把你的回复用我的账号发，晚点给你恢复过来

我在16年的时候也以为是一个前台的漏洞，并提交给了先知，被驳回了，再后来我仔细测试后发现其实这是一个后台漏洞。
如果不仔细读代码确实很容易被误导。
你能在本地测试成功是因为你先登录了后台，此时已经存在了一个登录后台成功的session，然后再没用注销登录的情况下直接访问member目录，这个时候前台自动登录

```
//[redacted]
$cuserLogin = new userLogin();

if($cuserLogin->getUserID() <=0 )
{
   if(empty($adminDirHand))
   {
       ShowMsg("<b>[redacted]</b><br /><form>[redacted]<input type='hidden' name='gotopage' value='".urlencod
       exit();
   }
   $adminDirHand = HtmlReplace($adminDirHand, 1);
   $gurl = "../../{$adminDirHand}/login.php?gotopage=".urlencode($dedeNowurl);
   echo "<script language='javascript'>location='$gurl';</script>";
   exit();
}

class userLogin
{
   var $userName = '';
   var $userPwd = '';
   var $userID = '';
```

```
    var $adminDir = '';
    var $userType = '';
    var $userChannel = '';
    var $userPurview = '';
    var $keepUserIDTag = 'dede_admin_id';
    var $keepUserTypeTag = 'dede_admin_type';
    var $keepUserChannelTag = 'dede_admin_channel';
    var $keepUserNameTag = 'dede_admin_name';
    var $keepUserPurviewTag = 'dede_admin_purview';
    var $keepAdminStyleTag = 'dede_admin_style';
    var $adminStyle = 'dedecms';

    //php5■■■■
    function __construct($admindir='')
    {
        global $admin_path;
        if(isset($_SESSION[$this->keepUserIDTag]))
        {
            $this->userID = $_SESSION[$this->keepUserIDTag];
            $this->userType = $_SESSION[$this->keepUserTypeTag];
            $this->userChannel = $_SESSION[$this->keepUserChannelTag];
            $this->userName = $_SESSION[$this->keepUserNameTag];
            $this->userPurview = $_SESSION[$this->keepUserPurviewTag];
            $this->adminStyle = $_SESSION[$this->keepAdminStyleTag];
        }

        if($admindir!='')
        {
            $this->adminDir = $admindir;
        }
        else
        {
            $this->adminDir = $admin_path;
        }
    }
    /*
    ........
    */
    function getUserID()
    {
        if($this->userID != '')
        {
            return $this->userID;
        }
        else
        {
            return -1;
        }
    }
```

通过代码可以发现 $this->userid必须不能等于空，$this->userid就是$_SESSION[$this->keepUserIDTag]
也就是$_SESSION['dede_admin_id'];
我们看看$_SESSION['dede_admin_id']是在什么情况下会被赋值

```
function keepUser()
    {
        if($this->userID != '' && $this->userType != '')
        {
            global $admincachefile,$adminstyle;
            if(empty($adminstyle)) $adminstyle = 'dedecms';

            @session_register($this->keepUserIDTag);
            $_SESSION[$this->keepUserIDTag] = $this->userID;

            @session_register($this->keepUserTypeTag);
            $_SESSION[$this->keepUserTypeTag] = $this->userType;

            @session_register($this->keepUserChannelTag);
            $_SESSION[$this->keepUserChannelTag] = $this->userChannel;
```

```
            @session_register($this->keepUserNameTag);
            $_SESSION[$this->keepUserNameTag] = $this->userName;

            @session_register($this->keepUserPurviewTag);
            $_SESSION[$this->keepUserPurviewTag] = $this->userPurview;

            @session_register($this->keepAdminStyleTag);
            $_SESSION[$this->keepAdminStyleTag] = $adminstyle;

            PutCookie('DedeUserID', $this->userID, 3600 * 24, '/');
            PutCookie('DedeLoginTime', time(), 3600 * 24, '/');

            $this->ReWriteAdminChannel();

            return 1;
        }
        else
        {
            return -1;
        }
    }
```

在看看keepUser 是什么时候被调用的。

```
//■■■■
$admindirs = explode('/',str_replace("\\",'/',dirname(__FILE__)));
$admindir = $admindirs[count($admindirs)-1];
if($dopost=='login')
{
    $validate = empty($validate) ? '' : strtolower(trim($validate));
    $svali = strtolower(GetCkVdValue());
    if(($validate=='' || $validate != $svali) && preg_match("/6/",$safe_gdopen)){
        ResetVdValue();
        ShowMsg('■■■■■■!','login.php',0,1000);
        exit;
    } else {
        $cuserLogin = new userLogin($admindir);
        if(!empty($userid) && !empty($pwd))
        {
            $res = $cuserLogin->checkUser($userid,$pwd);

            //success
            if($res==1)
            {
                $cuserLogin->keepUser();
                if(!empty($gotopage))
                {
                    ShowMsg('■■■■■■■■■■■■■■■■■',$gotopage);
                    exit();
                }
                else
                {
                    ShowMsg('■■■■■■■■■■■■■■■■■","index.php");
                    exit();
                }
            }

            //error
            else if($res==-1)
            {
                ResetVdValue();
                ShowMsg('■■■■■■■■!','login.php',0,1000);
                exit;
            }
            else
            {
                ResetVdValue();
                ShowMsg('■■■■■■!','login.php',0,1000);
```

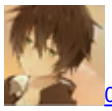
```
                exit;
            }
        }

        //password empty
        else
        {
            ResetVdValue();
            ShowMsg('■■■■■■■■■■■!','login.php',0,1000);
            exit;
        }
    }
}
```

只有在后台登录的时候被调用。前台压根就没办法对session进行操作，没有办法控制session就没有办法绕过这个if($cuserLogin->getUserID() <=0)判断，所以，这是一个假漏洞。

==========

抛开认证问题，就上传绕过来说，同目录下的select_soft_post.php文件更好绕过
把上传文件名改成1.htm.php?
文件类型只要有text就行

0 回复Ta


0r3ak 2018-01-23 11:15:16

@phpice 说得没错，这里很容易被误导，昨天我也纳闷，之前在复现"DeDecms
任意用户登录,管理员密码重置漏洞"的时候以为可以利用组合漏洞去getshell，不需要知道后台，后来测试的时候发现并没有用，还是提示登录后台，之前也发现了这个漏
再在前台上传是不行的了。

1 回复Ta


root 2018-01-23 18:17:22

貌似admin账号不允许前台登录。

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