

漏洞位于dede/album_edit.php或dede/album_add.php中:

```
/*-----  
function _getformzip()  
从ZIP文件中获取新图片  
-----*/  
  
if($formzip==1)  
{  
    include_once(DEDEINC."/zip.class.php");  
    include_once(DEDEADMIN."/file_class.php");  
    $zipfile = $cfg_basedir.str_replace($cfg_mainsite,'',$zipfile);  
    $tmpzipdir = DEDEDATA.'/ziptmp/'.cn_substr(md5(ExecTime()),16);  
    $ntime = time();  
    if(file_exists($zipfile))  
    {  
  
        @mkdir($tmpzipdir,$GLOBALS['cfg_dir_purview']);  
        @chmod($tmpzipdir,$GLOBALS['cfg_dir_purview']);  
        $z = new zip();  
        $z->ExtractAll($zipfile,$tmpzipdir);  
        $fm = new FileManagement();  
        $imgs = array();  
        $fm->GetMatchFiles($tmpzipdir,"jpg|png|gif",$imgs);  
        $i = 0;  
        foreach($imgs as $imgold)  
        {  
            $i++;  
            $savepath = $cfg_image_dir."/".MyDate("Y-m",$ntime);  
            CreateDir($savepath);  
            $iurl =  
$savepath."/".MyDate("d",$ntime).dd2char(MyDate("His",$ntime).'-'.$adminid."-  
{i}").mt_rand(1000,9999));  
            $iurl = $iurl.substr($imgold,-4,4);  
            $imgfile = $cfg_basedir.$iurl;  
            copy($imgold,$imgfile);  
            unlink($imgold);  
            if(is_file($imgfile))  
            {  
                $litpicname = $pagestyle > 2 ?  
GetImageMapDD($iurl,$cfg_ddimg_width) : $iurl;  
                $info = '';  
                $imginfos = GetImageSize($imgfile,$info);  
                $imgurls .= "{dede:img ddimg='$litpicname' text=''  
width='".$imginfos[0]."' height='".$imginfos[1]."' } $iurl {/dede:img}\r\n";  
  
                //把图片信息保存到媒体文档管理档案中  
                $inquiry = "  
INSERT INTO  
#@__uploads(title,url,mediatype,width,height,playtime,filesize,uptime,mid)  
VALUES  
('{title}','{iurl}','1','".$imginfos[0]."',".$imginfos[1]."',0','".filesize(  
$imgfile)."',".$ntime."', $adminid)";  
                $dsq1->ExecuteNoneQuery($inquiry);  
            }  
        }  
    }  
}
```

```

        if(!$hasone && $ddisfirst==1
        && $litpic==" " && !empty($litpicname))
        {
            if( file_exists($cfg_basedir.$litpicname) )
            {
                $litpic = $litpicname;
                $hasone = true;
            }
        }
    }
    if($delzip==1)
    {
        unlink($zipfile);
    }
    $fm->RmdirFiles($tmpzipdir);
}
}

```

此段代码的功能是从zip文件中获取图片，GetMatchFiles函数获取符合规则的图片(由传入参数知道是png,jpg,gif)，跟进GetMatchFiles函数：

```

function GetMatchFiles($indir, $fileexp, &$filearr)
{
    $dh = dir($indir);
    while($filename = $dh->read())
    {
        $truefile = $indir.'/'.$filename;
        if($filename == "." || $filename == "..")
        {
            continue;
        }
        else if(is_dir($truefile))
        {
            $this->GetMatchFiles($truefile, $fileexp, $filearr);
        }
        else if(preg_match("/\.(\".$fileexp.\")/i",$filename))
        {
            $filearr[] = $truefile;
        }
    }
    $dh->close();
}

```

问题就出在：

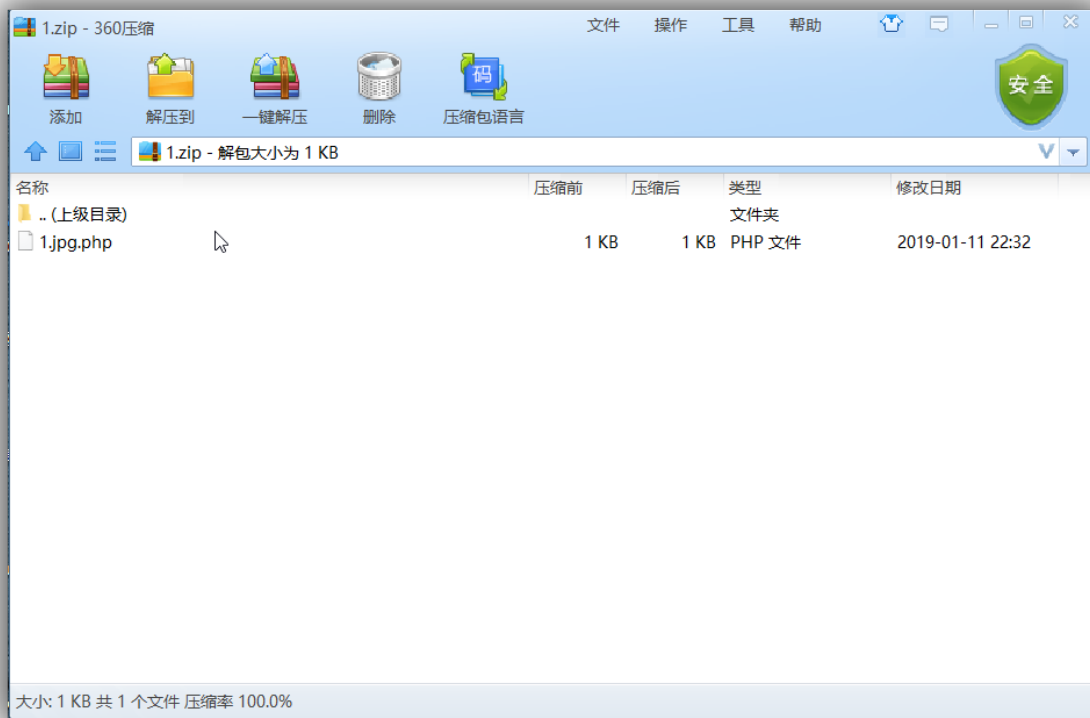
```

else if(preg_match("/\.(\".$fileexp.\")/i",$filename))
{
    $filearr[] = $truefile;
}

```

只要文件名中包含".jpg"、".png"、".gif"即可被上传。因此可以在zip文件中创建包含这几个字符串的php文件然后上传。

创建一个zip文件，其中包含一个php文件名称为“1.jpg.php”




然后访问dede/album_edit.php，选择“从ZIP压缩包中解压文件”，然后上传准备好的zip文件。



然后查看图集即可访问上传的php文件

10.10.10.132/dedecms/uploads/allimg/2019-02/16224017-1-11331.php

🔍 火狐官方网站 📺 新手上路 📄 常用网址

PHP Version 5.2.17

System	Windows NT A-7474D33154F24 5.2 build 3790
Build Date	Jan 6 2011 17:26:08
Configure Command	cmd /c nolog configure.js --enable-snapshot-build --enable-debug-pack --with-snapshot-template=d:\php-sdk\snap_5_2\vc6\86\template --with-php-build=d:\php-sdk\snap_5_2\vc6\86\php_build --with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk\shared --with-oci8=D:\php-sdk\oracle\instantclient10\sdk\shared --without-pi3web
Server API	Apache 2.4 Handler - Apache Lounge
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	C:\phpStudy\php\php-5.2.17\php.ini
Scan this dir for additional .ini files	(none)
additional .ini files parsed	(none)