CVE-2019-8362复现

原理分析

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
                    $inquery = "
                   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');
                 ";
                    $dsql->ExecuteNoneQuery($inquery);
                    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:

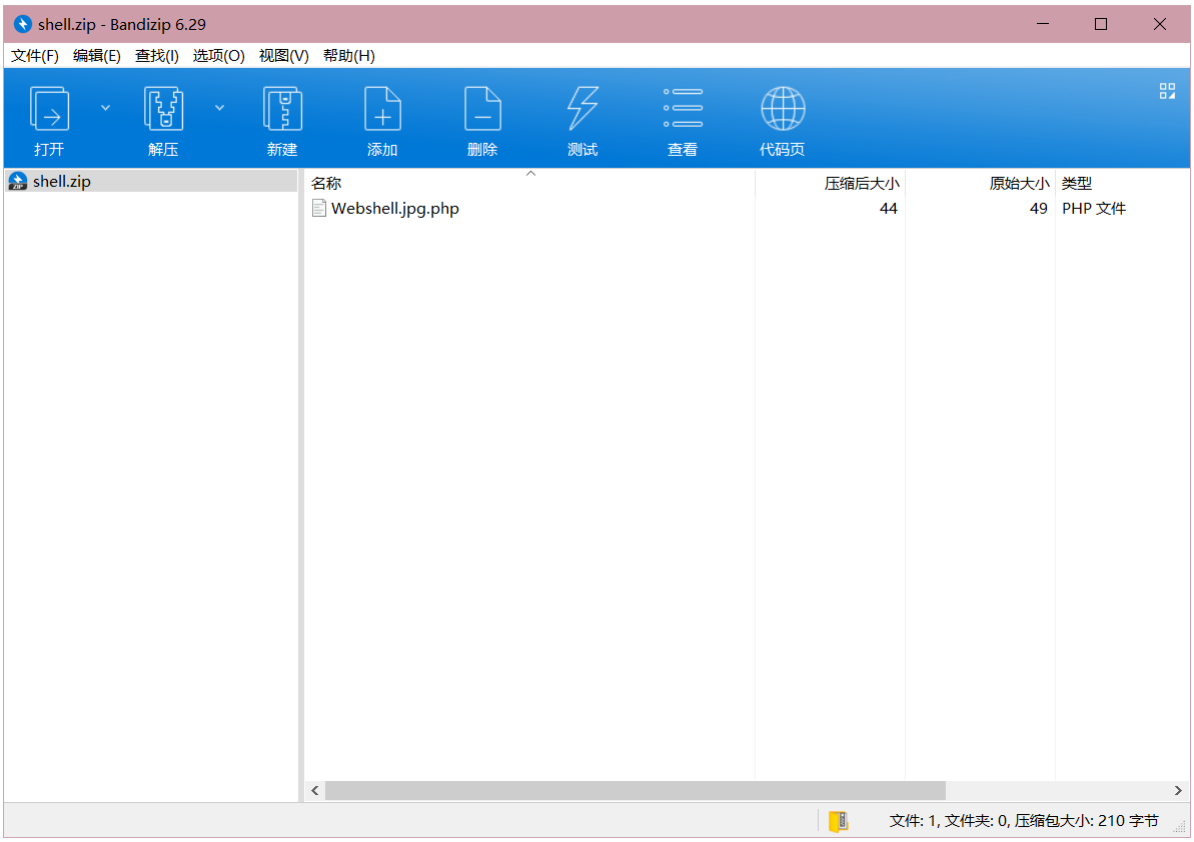
```
else if(preg_match("/\.(".$fileexp.")/i",$filename))
{
    $filearr[] = $truefile;
}
```

这里只要文件名中包含".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。

漏洞复现

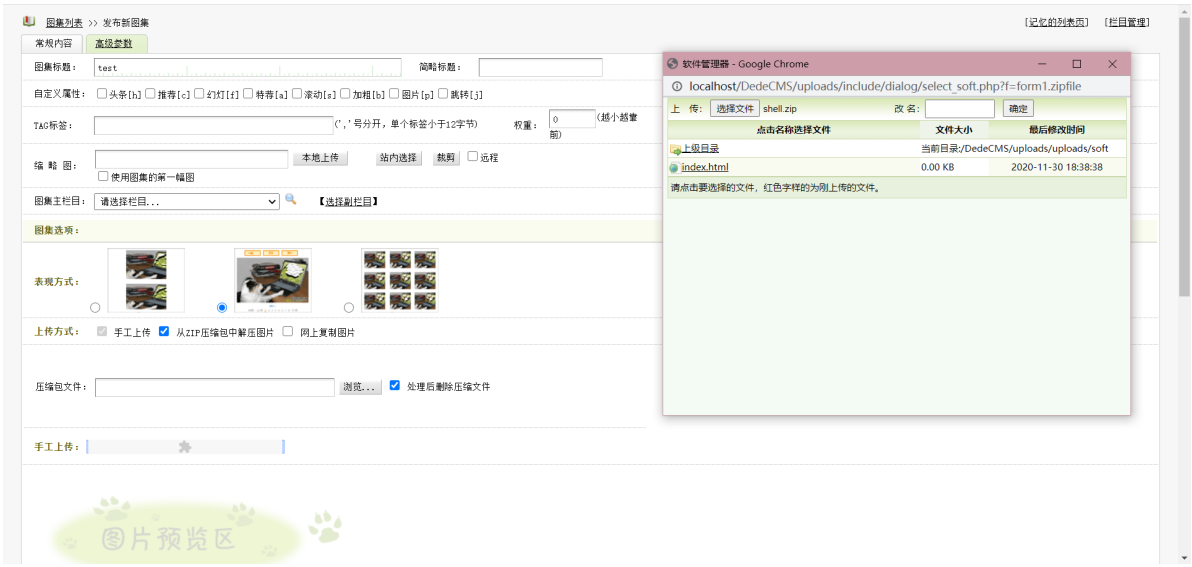
首先创建一个压缩包，并且在其中放入webshell.jpg.php，如图所示：

之后在http://localhost/DedeCMS/uploads/dede/album_add.php中新建图集，如图所示

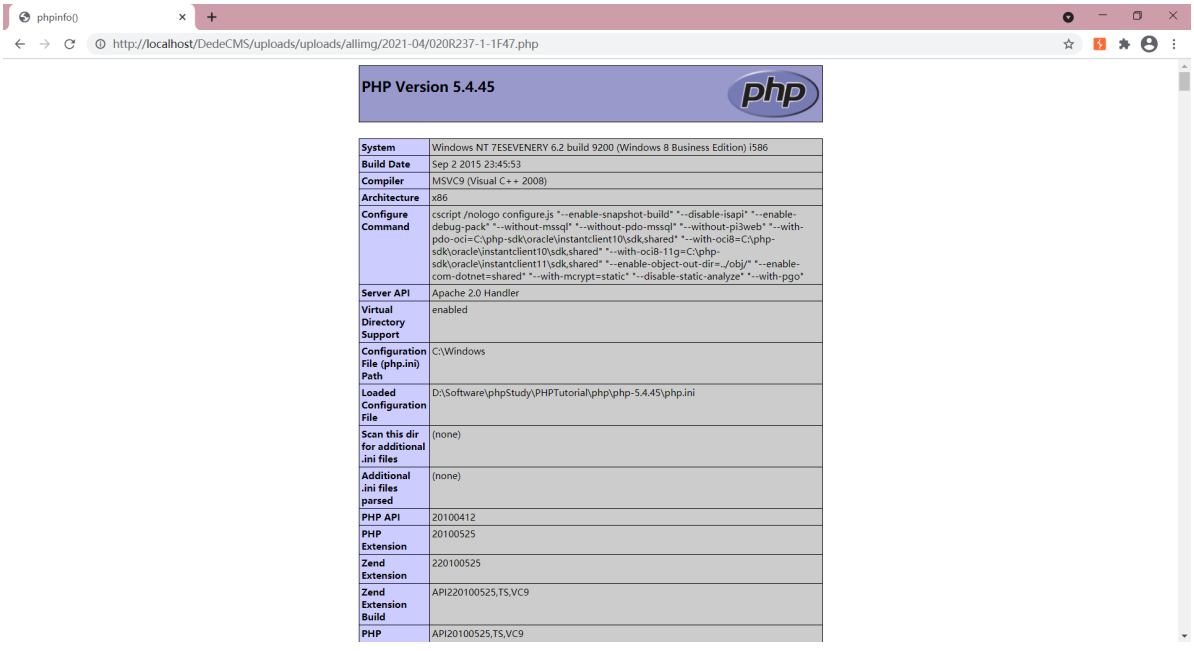


上传压缩包后选中即可，注意选择栏目：

之后查看图集



点击原始图片即可跳转到我们上传的webshell中



System	Windows NT 7ESEVENERY 6.2 build 9200 (Windows 8 Business Edition) i586
Build Date	Sep 2 2015 23:45:53
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	D:\Software\phpStudy\PHPTutorial\php\php-5.4.45\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525
Zend Extension Build	API220100525,TS,VC9
PHP	API20100525,TS,VC9