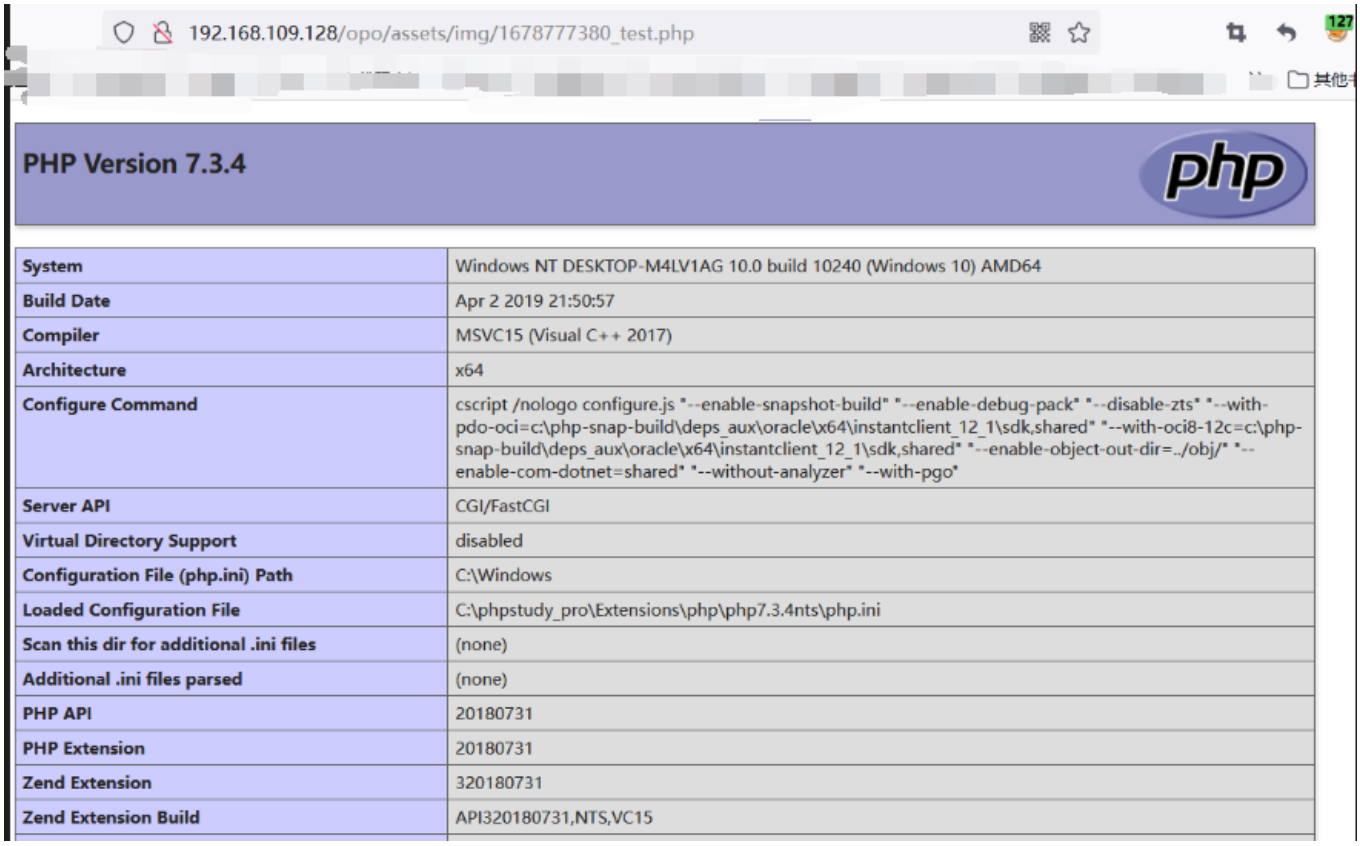
The online pizza ordering system has a file upload (RCE) vulnerability

```
Online pizza ordering system exists file upload (RCE)
vulnerability, vulnerability exists in save_menu() function, can
upload any format of the file, and execute any code, the function
of the file name timestamp confusion, but can be predicted, can be
used by malicious users to upload any file execution code, access
to the server.
```



System	Windows NT DESKTOP-M4LV1AG 10.0 build 10240 (Windows 10) AMD64
Build Date	Apr 2 2019 21:50:57
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--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	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\phpstudy_pro\Extensions\php\php7.3.4nts\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,NTS,VC15

```php
if($action == "save_menu"){
    $save = $crud->save_menu();
    if($save)
        echo $save;
}
```


function save_menu(){
extract(&array: $_POST);
$data = " name = '$name' ";
$data .= ", price = '$price' ";
$data .= ", category_id = '$category_id' ";
$data .= ", description = '$description' ";
if(isset($status) && $status == 'on')
$data .= ", status = 1 ";
else
$data .= ", status = 0 ";
if($_FILES['img']['tmp_name'] != ''){
$fname = strtotime(date(format: 'y-m-d H:i')).'_'.$_FILES['
$move = move_uploaded_file($_FILES['img']['tmp_name'],'../
$data .= ", img_path = '$fname' ";
}