

72crm v9任意文件上传漏洞CVE-2022-37181 (<https://www.zilyun.com/38621.html>)

漏洞描述

在受影响的版本中，上传logo功能未检测上传文件的类型，具有管理员权限的用户可以通过该功能上传任意文件，攻击者可通过上传恶意文件从而控制服务器。

影响版本

72crm v9

漏洞分析

applicationadmincontrollerSystem.php line 51 后续发现没有设置validate，直接进行了move操作，导致可以上传任意文件 后续move函数（set filename） 第352行： 后续函数 生成以php为后缀的基于时间的文件名， 然后以此文件名move_uploaded_file（thinkphpliblibrarythinkFile.php第369行）

```
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         $resImg = $fileModel->updateByField($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 }
```

Linux实验室
www.linuxlab.com

```
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) : '';
```

```
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 }
```

```
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                         $savename = date('Ymd') . DS . md5(microtime( get_as_float: true));
397                         break;
398                     default:
399                         if (in_array($this->rule, hash_algos())) {
400                             $hash = $this->hash($this->rule);
401                             $savename = substr($hash, start: 0, length: 2) . DS . substr($hash, start: 2);
402                         } elseif (is_callable($this->rule)) {
403                             $savename = call_user_func($this->rule);
404                         } else {
405                             $savename = date('Ymd') . DS . md5(uniqid(md5(microtime( get_as_float: true)), more_entropy: true));
406                             // $savename = date('Ymd') . DS . md5(microtime(true));
407                         }
408                 }
409             }
410         } elseif ('' === $savename || false === $savename) {
411             $savename = $this->getInfo( name: 'name');
412         }
413
414         if (!strpos($savename, needle: '.')) {
415             $savename .= '.' . pathinfo($this->getInfo( name: 'name'), options: PATHINFO_EXTENSION);
416         }
417     }
```

Linux实验室
www.linuxlz.com

```
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     }
```

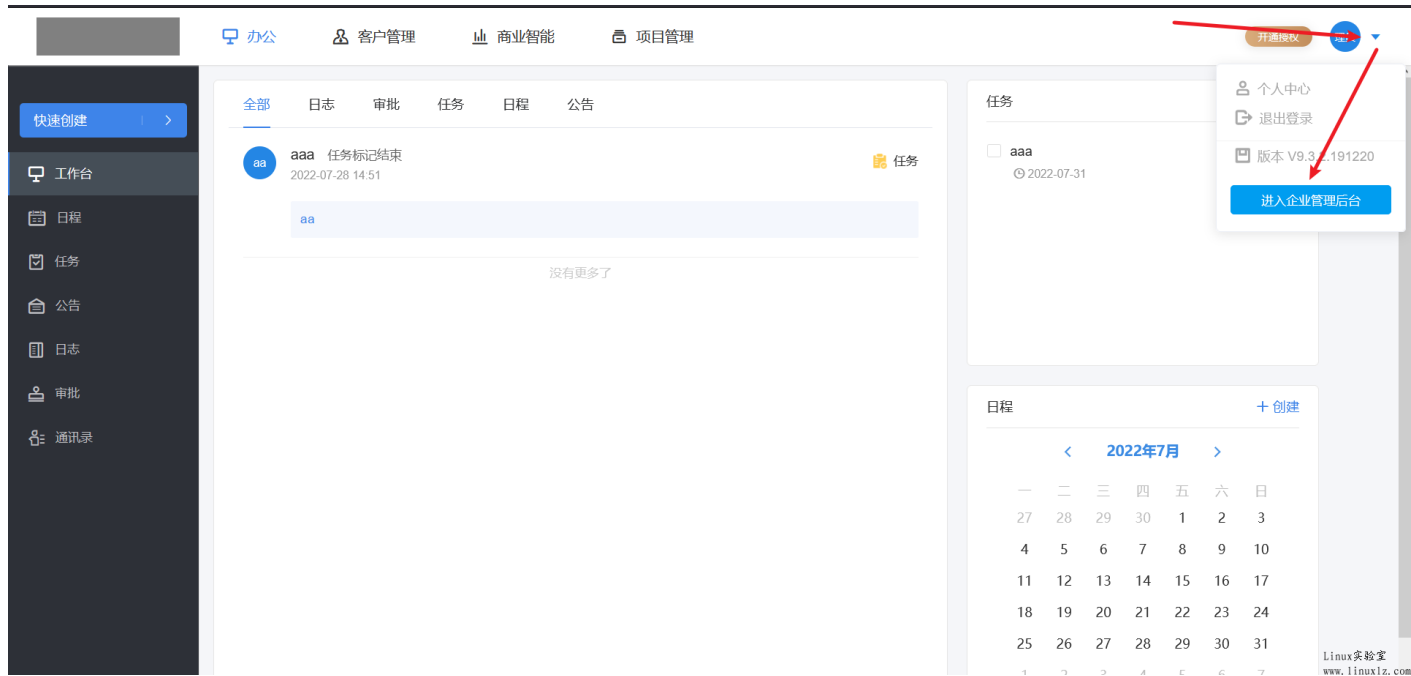
Linux实验室
www.linuxlz.com

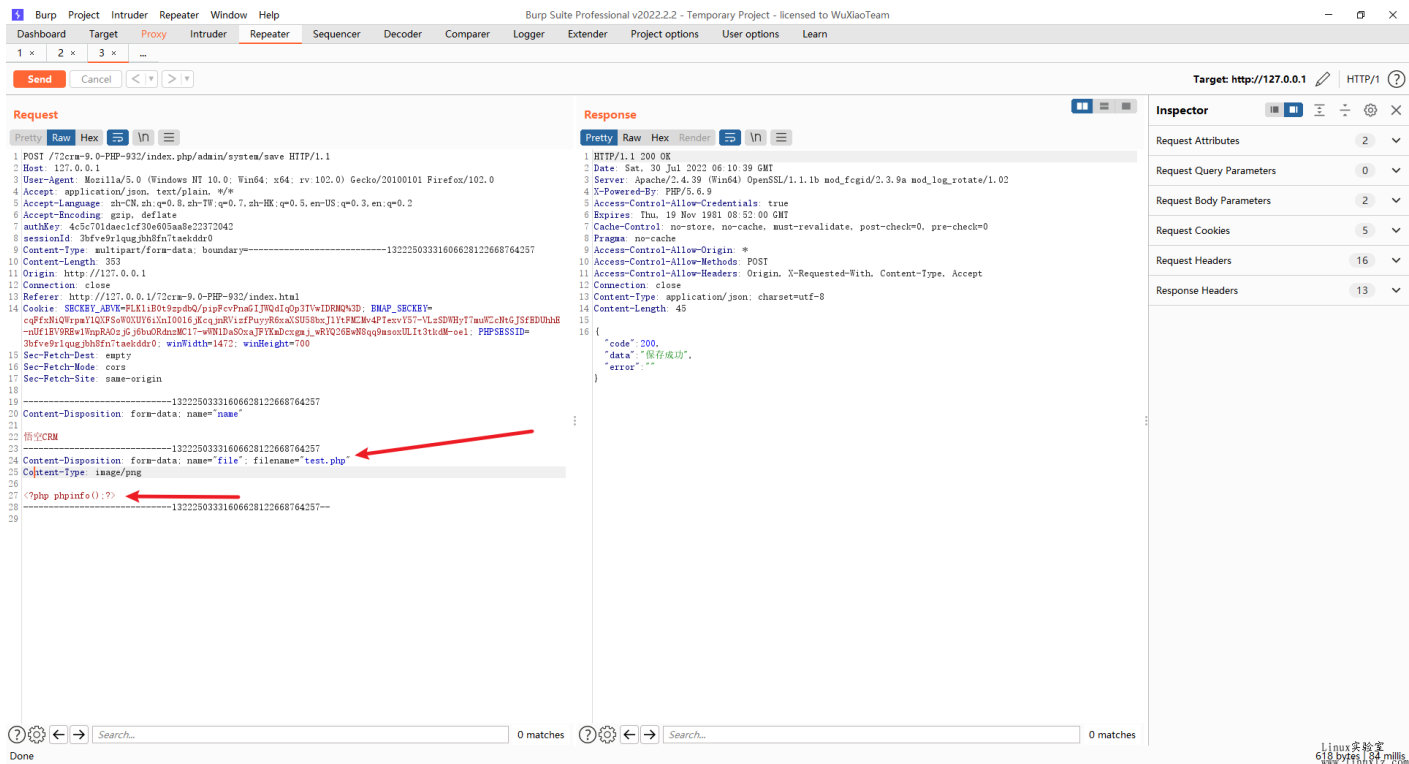
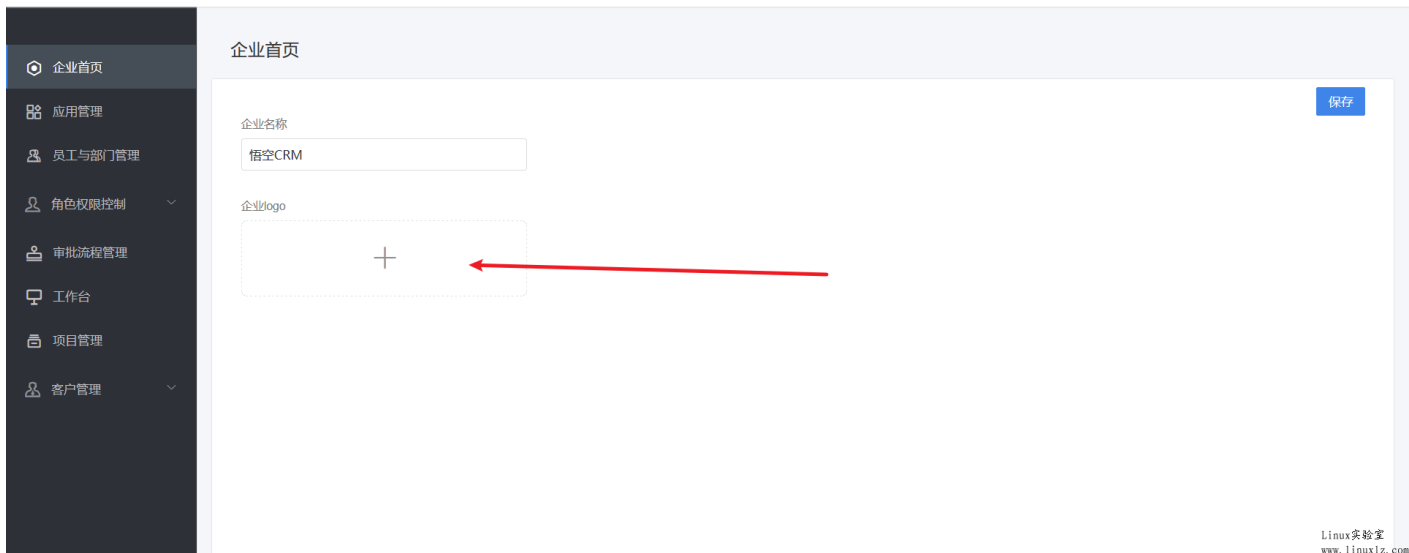
漏洞复现

首先进入后台

点击如图，进入企业管理后台 点击这个 只需上传一张图片抓包，修改内容如下 返回企业管理后台 访问图片地址 php代码执行成功

注意：因为是上传在logo，未经授权的用户也可以访问这个php代码





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

企业首页

企业名称

悟空CRM


企业logo

保存

Linux实验室
www.linux1z.com

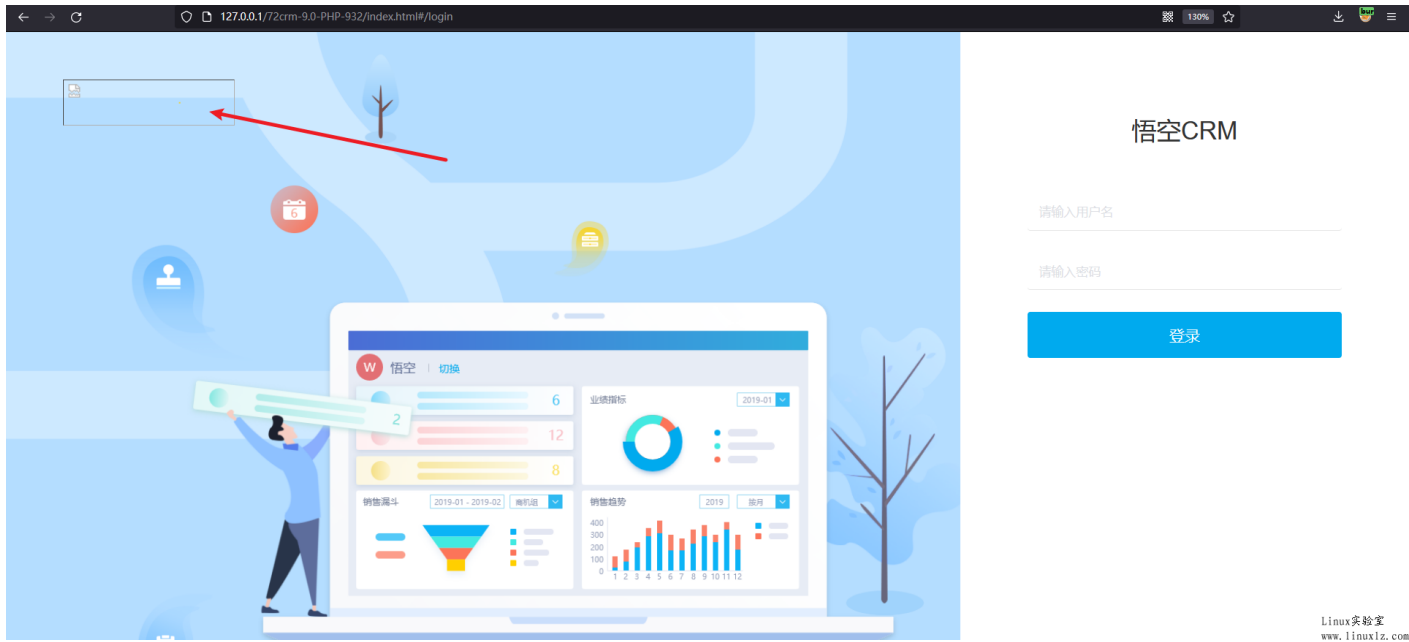
127.0.0.1/72crm-9.0-PHP-932/public/uploads/20220730/1298ae1bbfddae343154b29dc6670dd.php

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	cscrip /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-encham=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
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


Linux实验室
www.linux1z.com



Linux实验室
www.linux1z.com

← → 127.0.0.1/72crm-9.0-PHP-932/public/uploads/20220730/1298ae1bbfddae343154b29dc6670dd.php 130%

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	cscrip /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"
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

Linux实验室
www.linux1z.com

