## SRS real-time video server has SSRF vulnerability

#### Product Profile

SRS (Simple Realtime Server) is a simple and efficient real-time video server that supports various real-time streaming protocols such as RTMP, WebRTC, HLS, HTTP-FLV, SRT, etc. Oryx is an integrated, out of the box, open-source video solution that can be deployed in the cloud or self built data centers, empowering your business with live streaming and WebRTC capabilities.

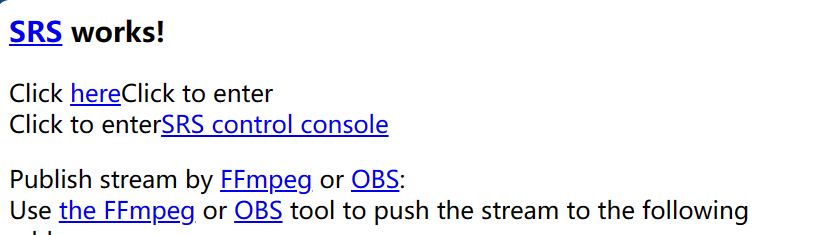
**Impact version：SRS/4.0.268(Leo)**

**SRS/4.0.195(Leo)**

#### 1.Reproduction process(Dnslog testing)

1. Access target address <http://3.33.250.13:8081/>
2. Then click on the SRS console.

The screenshot is as follows:

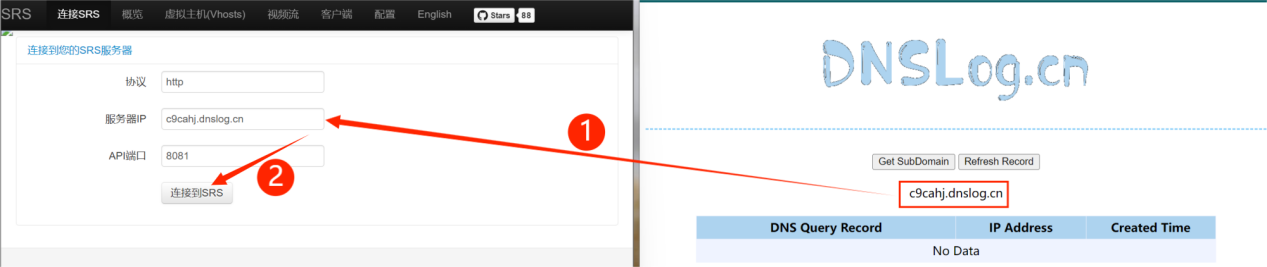




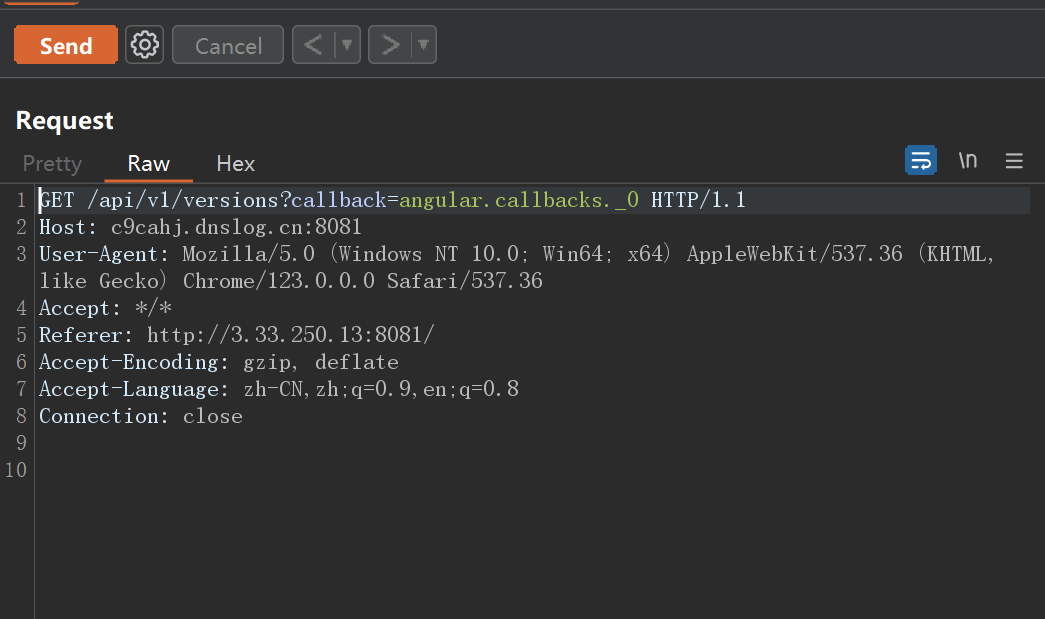
1. Then enter the page and select "Connect SRS" at the top.



1. After entering this page, enter our Dnslog address in the input box of the server IP to test for SSRF echo free attacks.
2. After entering the dnslog address, simply click on "Connect to SRS" below.



1. Then use burpsuite to capture packets and view request packets.



**Poc:**

**GET /api/v1/versions?callback=angular.callbacks.\_0 HTTP/1.1**

**Host: c9cahj.dnslog.cn:8081**

**User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36**

**Accept: \*/\***

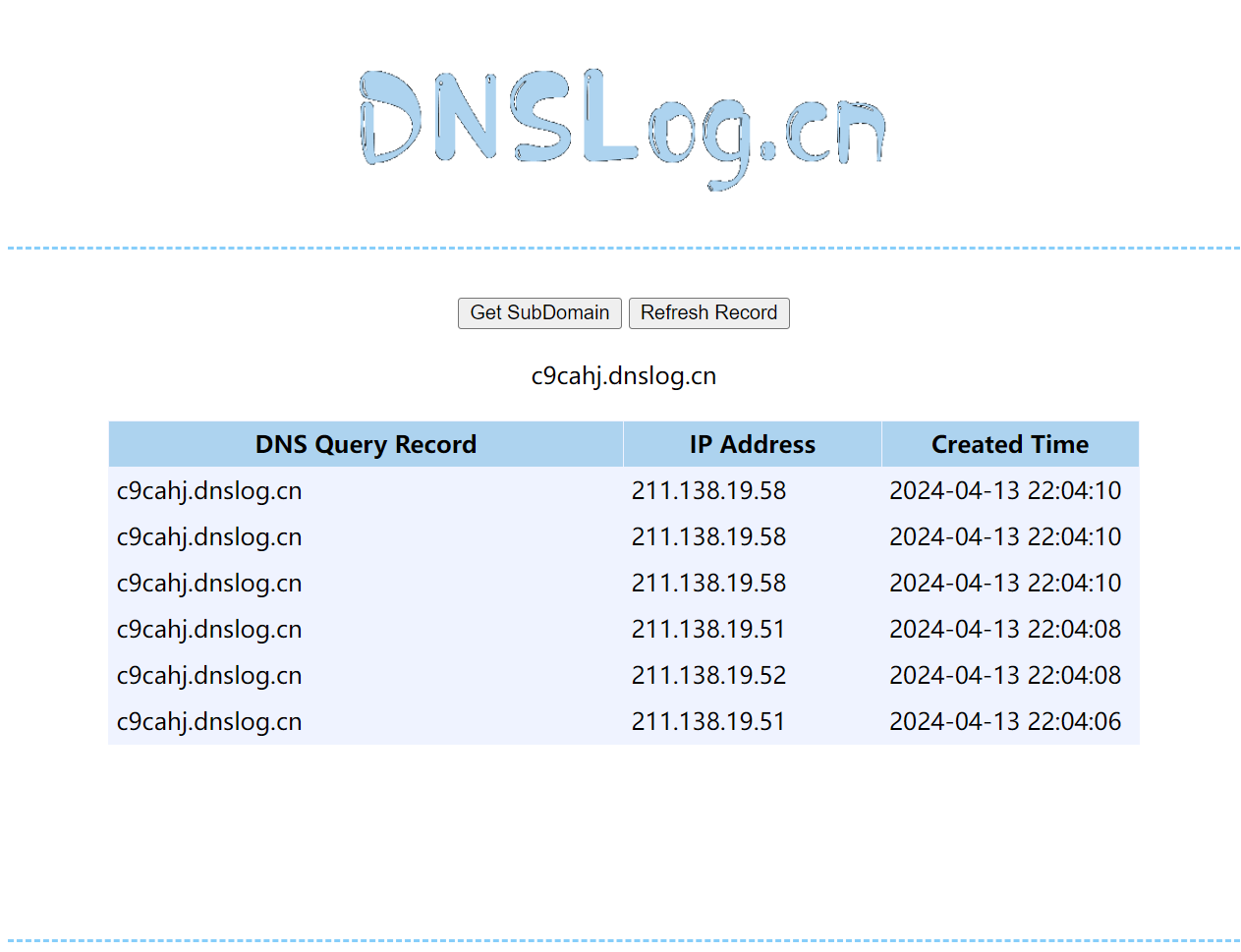
**Referer: http://3.33.250.13:8081/**

**Accept-Encoding: gzip, deflate**

**Accept-Language: zh-CN,zh;q=0.9,en;q=0.8**

**Connection: close**

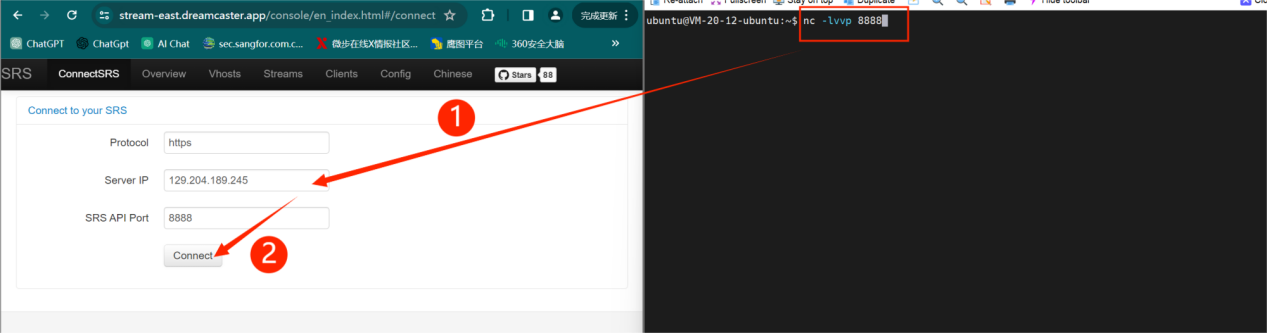
1. Then use burp to repeatedly send and detect whether the malicious request is successfully echoed.



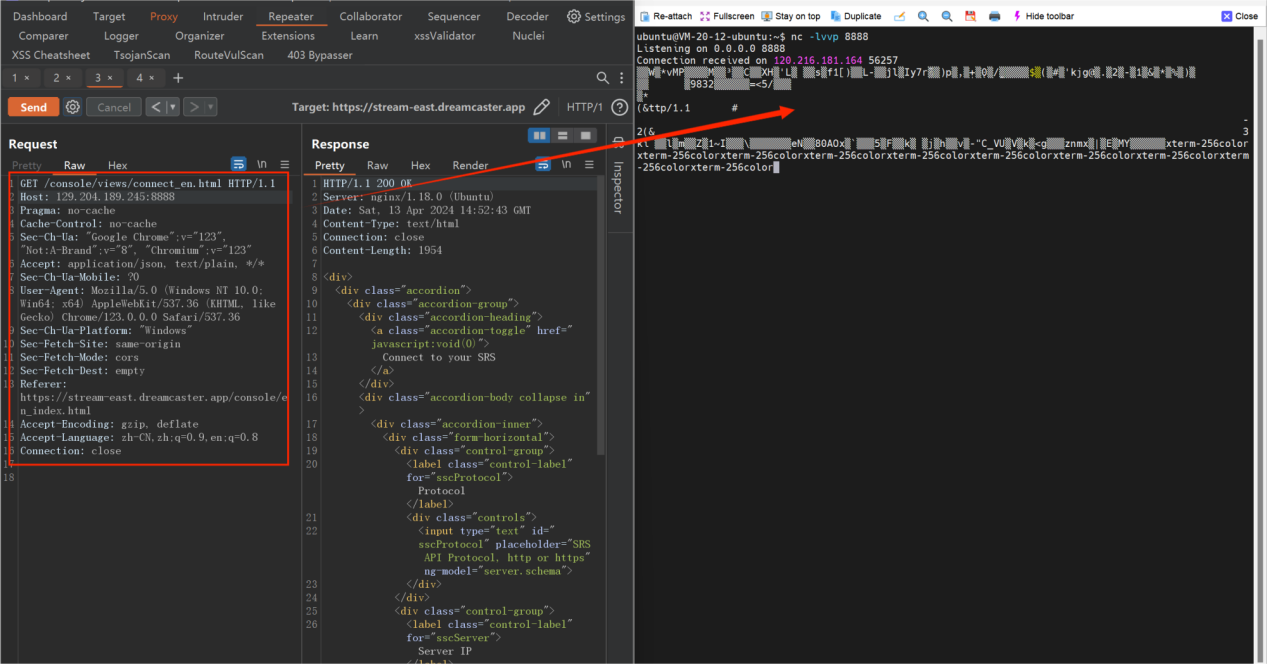
1. You can see that the attack echo was successful.

#### Reproduction process(Using NC listening test)

1. Access this address：<https://stream-east.dreamcaster.app/console/en_index.html#/connect>
2. Enter the monitoring IP in the server IP, click on connect, use burp suite to capture and view data packets, and send them. It can be seen that NC has successfully captured the request sent from the other server



1. Successful Echo



#### Repair suggestions：

Strictly validate and filter user input to prevent users from having control over the request target.

Restrict the target of server requests, such as restricting access to trusted domain names or IP addresses on the whitelist

Minimize server access to external resources and avoid exposing the server to the public network.

Regularly audit and monitor the network traffic and DNS resolution requests of the server, promptly detect abnormal activity and handle it.

Update and maintain security patches on the server to prevent known vulnerabilities from being exploited.