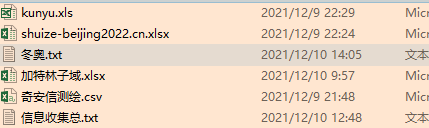
信息收集



漏洞扫描goby，加特林



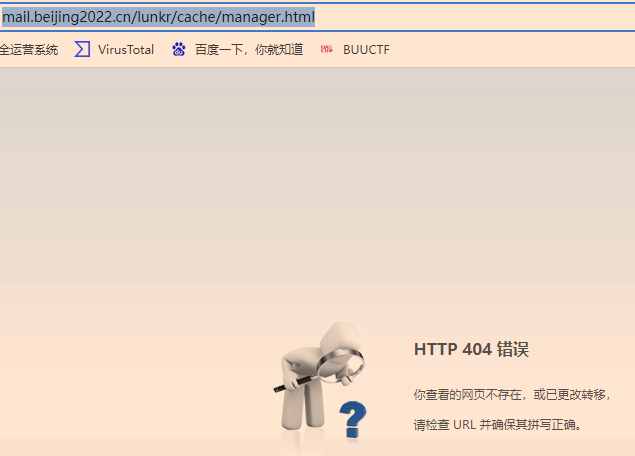


Apache-Log4j测试0day

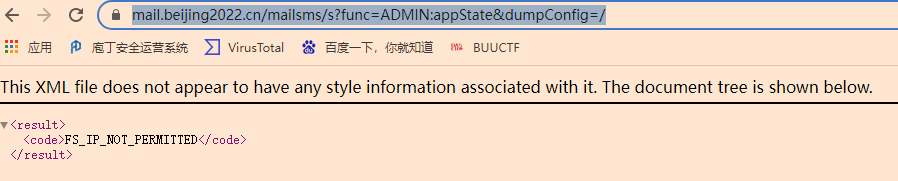


<http://mail.beijing2022.cn>

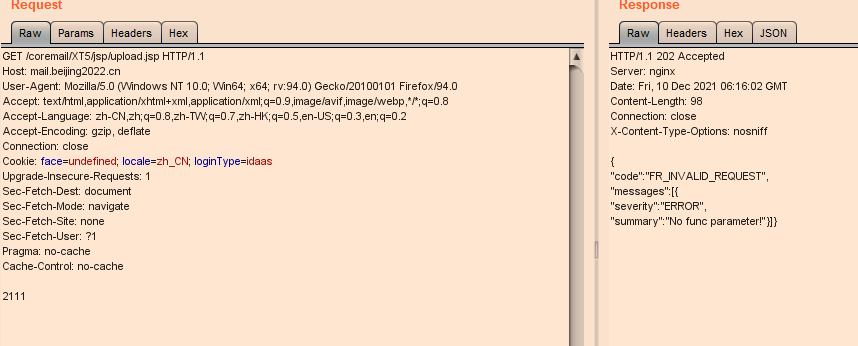
测试Coremail邮箱系统 目录穿越泄漏后台漏洞



Coremail配置文件信息泄漏



CVE-2020-29133



https://client.beijing2022.cn

Apache-Log4j测试0day

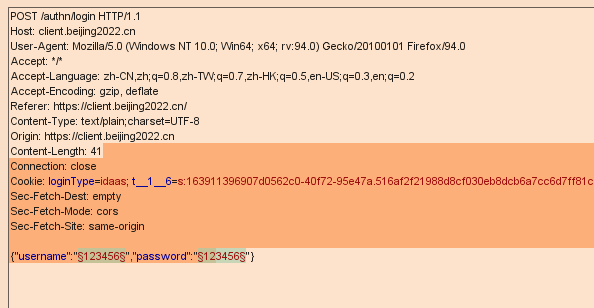


VMware vCenter未授权任意文件读取

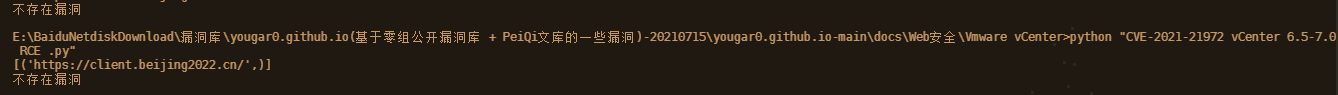


client.beijing2022.cn

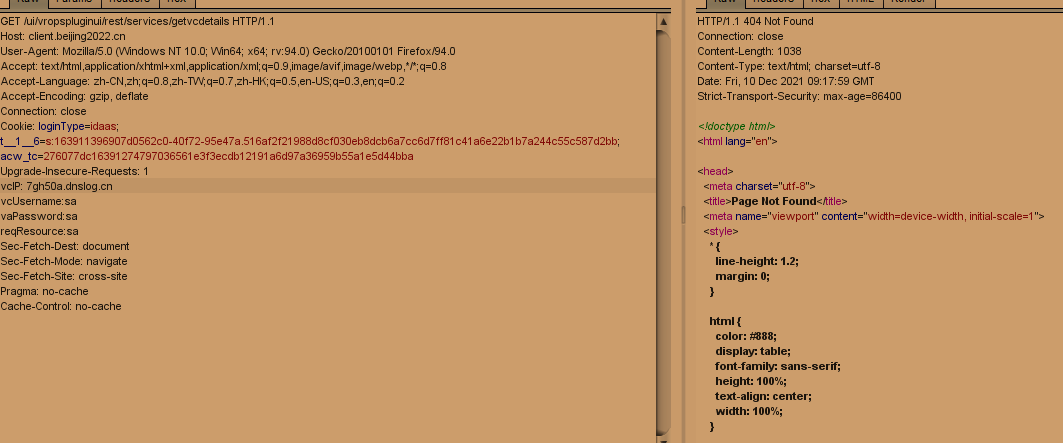
用户名密码爆破



CVE-2021-21972测试



CVE-2021-21973



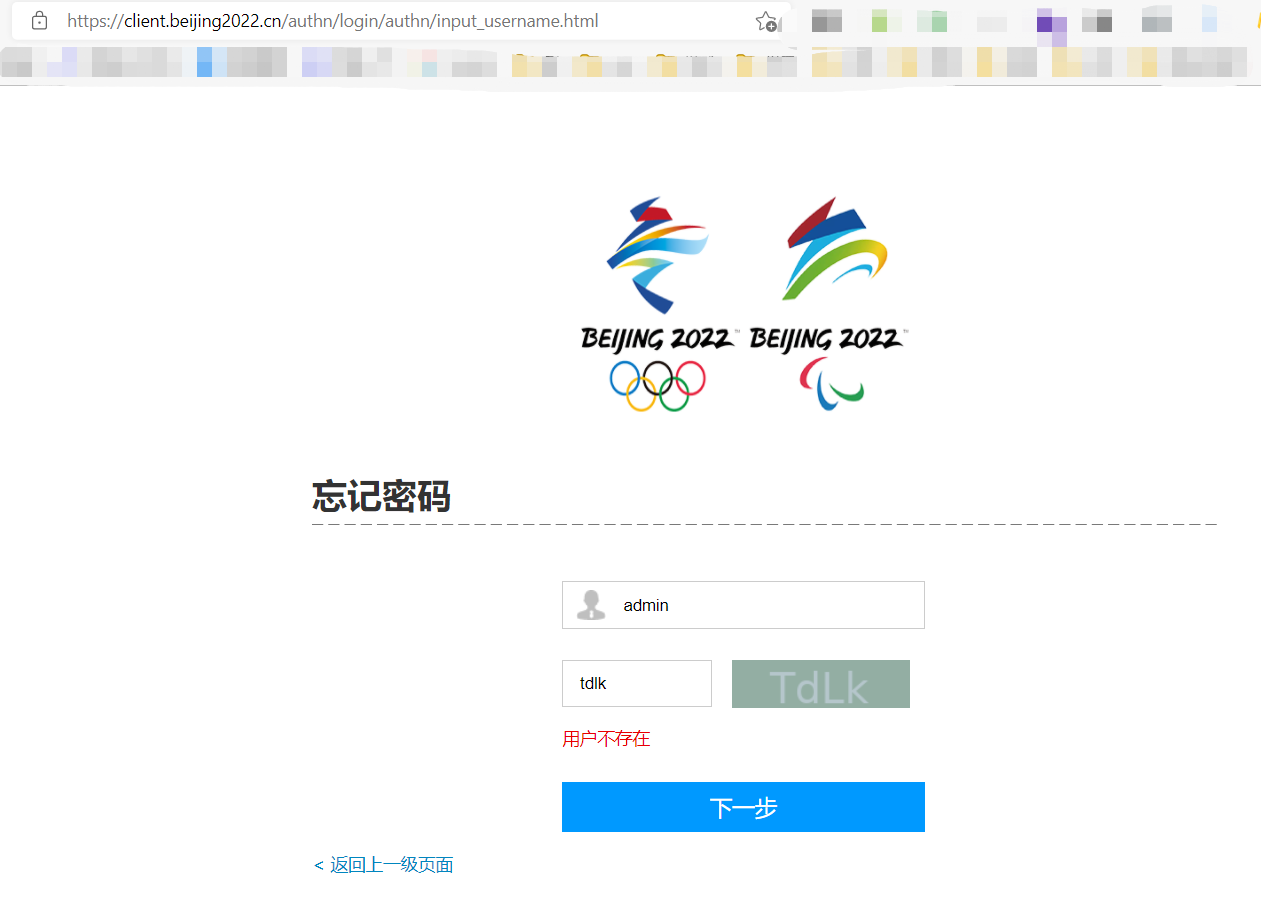
成果：

用户名枚举，验证码失效

https://mail.beijing2022.cn/coremail/changepwd.jsp

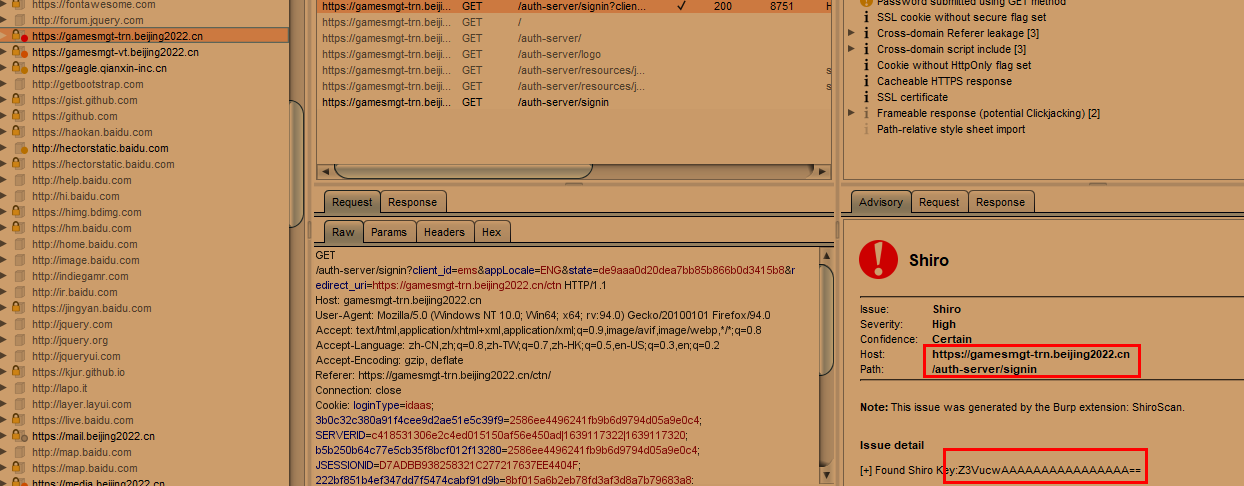


<https://client.beijing2022.cn/authn/login/authn/input_username.html>

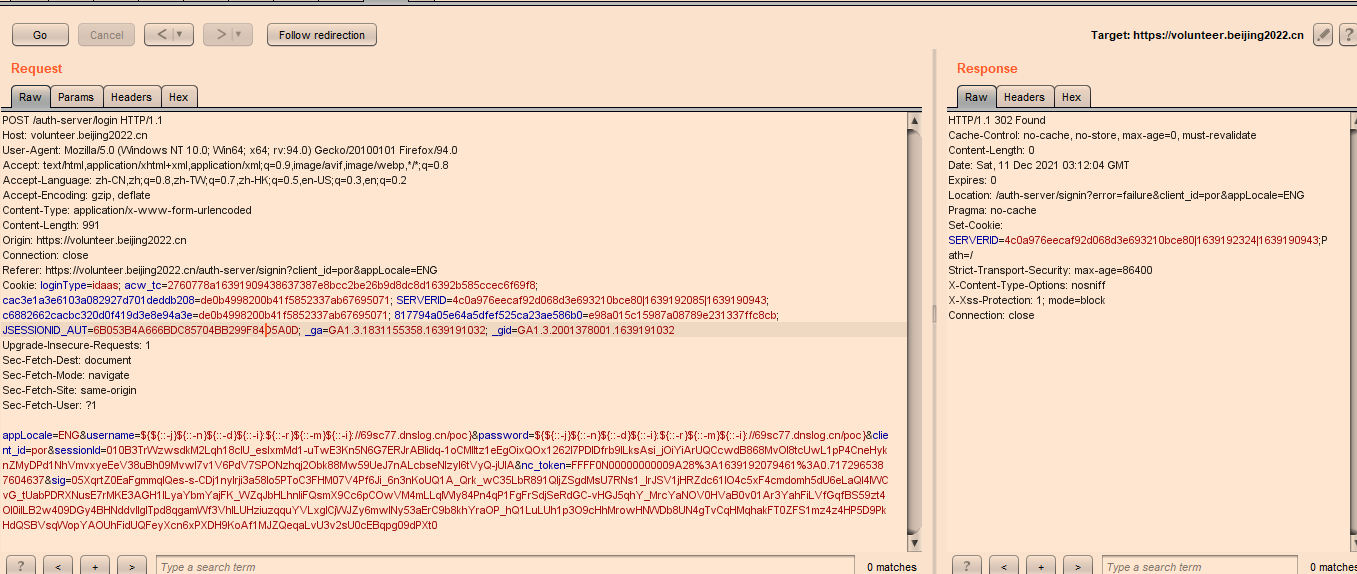


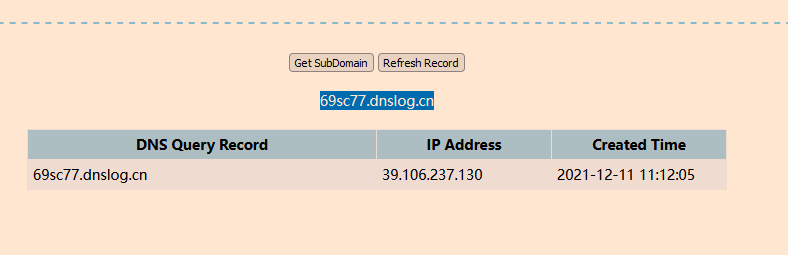
Shiro反序列化漏洞

https://gamesmgt-trn.beijing2022.cn/auth-server/signin



https://volunteer.beijing2022.cn/auth-server/signin?client\_id=por&appLocale=CHI





<https://gamesmgt.beijing2022.cn/auth-server/signin?client_id=ems&appLocale=CHI&redirect_uri=https://gamesmgt.beijing2022.cn/ctn>

