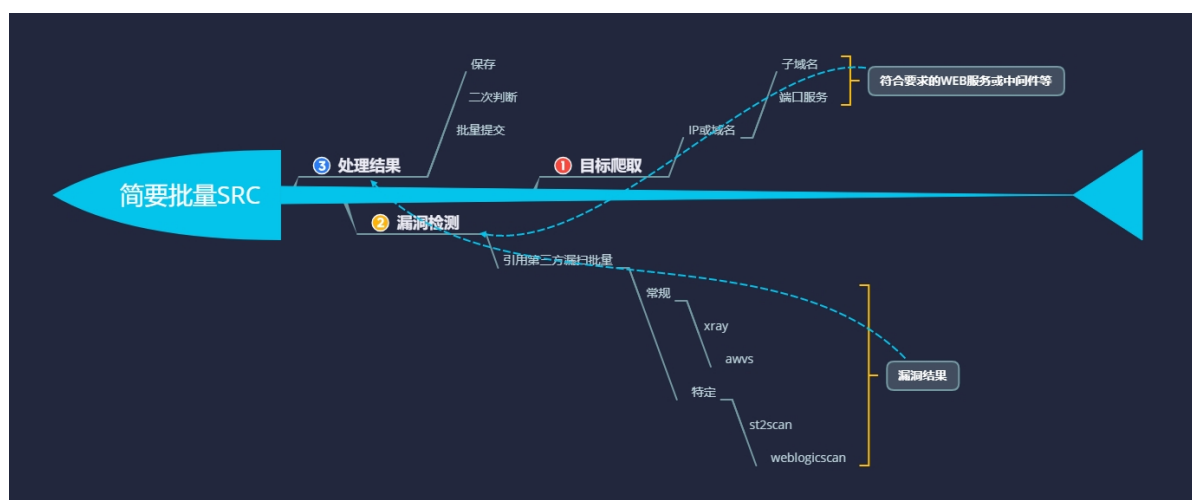


Day86 SRC挖掘-教育行业平台&规则&批量自动化



86.1 案例1：Python-Foda-Xray联动常规批量自动化

写Python脚本，将教育行业漏洞报告平台上的所有学校都爬下来。

```
1 import requests
2 import time
3 from lxml import etree
4
```

```

5  def get_edu_name():
6      for i in range(1,196):
7          url =
            "https://src.sjtu.edu.cn/rank/firm/?
            page="+str(i)
8          try:
9              result =
                requests.get(url).content.decode("UTF-8")
10                 soup = etree.HTML(result)
11                 name = soup.xpath('//td[@class="am-
                    text-center"]/a/text()')
12                 print('->'+str(i))
13                 print(name)
14                 name = '\n'.join(name)
15                 with
                    open(r'edu_name.txt','a+',encoding='utf-8') as
                    f:
16                     f.write(name + '\n')
17             except Exception as e:
18                 time.sleep(0.5)
19                 pass
20
21 if __name__ == '__main__':
22     get_edu_name()

```

或者也可以在fofa上搜索（需要买会员）：

fofa.so/result?qbase64=ImVkdS5jbGljJlYgY291bnRyeT0iQ04i

☆ 80

FOFA

"edu.cn" && country="CN"

API 会员 登录

类型分布

网站

80,586

协议

1,140

年份

2021

4,454

2020

77,272

国家/地区排名

» 中国

74,956

» 中国香港特别...

6,765

» 台湾(中国)

5

81,726 条匹配结果 (19,461 条独立IP), 55 ms. 关键词搜索 ☆ 下载 API

显示一年内数据, 点击 all 查看所有.

cx.szns.edu.cn

80

302 Found

1.31.128.212

中国 / Chifeng

ASN: 4837

组织: CHINA UNICOM Chi

na169 Backbone

szns.edu.cn

2021-01-19

📄 ↻

HTTP/1.1 302 Found

Connection: close

Content-Length: 207

Content-Type: text/html; charset=iso-8859-1

Date: Tue, 19 Jan 2021 12:23:59 GMT

Location: https://cx.szns.edu.cn/

Set-Cookie: __jsluid_h=09e8b838efc81701e368fdffc177a008; max-age=31536000; path=/; HttpOnly

```
1 import requests
2 from lxml import etree
3 import base64
4 import time
5
6
7 def fofa_search(search,yeshu):
8     proxies = {'http': 'http://tps185.kdlapi.com:15818', 'https': 'http://tps185.kdlapi.com:15818'}
9     headers={
10         'user-agent': 'Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3422.100 Safari/537.36',
11         'cookie': '_fofapro_ars_session=b34bfe980c5f5c287ee671a41418f869;result_per_page=20',
12         'referer': 'https://fofa.so/',
13     }
14     #search='title="BIG-IP&reg;- Redirec'
15     bs_search=base64.b64encode(search.encode("utf-8")), "utf-8")
16     for page in range(1,yeshu+1):
17         url='https://fofa.so/result?qbase64='+bs_search+'&page='+str(page)
18         try:
19             result=requests.get(url,headers=headers,proxies=proxies).content
20             #print(result.decode('utf-8'))
21             soup = etree.HTML(result)
22             #result_ip = soup.xpath('//*[@id="ajax_content"]/div/div/div/a/text()') #获取a便签
23             #result_ip = soup.xpath('//*[@id="ajax_content"]/div/div/div/@a/@href') #获取a便签
24             #result_ip = soup.xpath('//*[@target="blank"]/@href') #获取符合条件的href内容
25             result_ip = soup.xpath('//div[@class="f1 box-sizing"]/div[@class="re-domain"]/a[@t
26             print('第'+str(page)+'页: ')
27             print(result_ip)
28             result_ip = '\n'.join(result_ip)
29             with open('edu-url.txt','a+') as f:
30                 f.write(result_ip+"\n")
31                 f.close()
32                 time.sleep(1)
33         except Exception as e:
34             time.sleep(1)
35             print('网站请求失败!')
36             pass
37
38 if __name__ == '__main__':
39     fofa_search("edu.cn" && country="CN",1000)
40     poc_check()
```

Run: fofa

D:\Myproject\venv\Scripts\python.exe D:/Myproject/python/day77/fofa.py

第1页:

['https://cx.szns.edu.cn', 'http://cx.szns.edu.cn', 'http://www.yxxyz.net', 'http://lib.hbfu.edu.cn']

第2页:

['http://www.qinhan-art.cn', 'http://www.ylqipei.com.cn', 'http://www.gancen.cn', 'http://www.ylqipei.com.cn']

第3页:

['http://www.nip8.com.cn', 'http://www.shaohao Feng.cn', 'http://www.zhongtianpaper168.cn', 'http://www.nip8.com.cn']

第4页:

['http://jwc.gzty.edu.cn', 'http://zsb.gzty.edu.cn', 'http://cxqx.gzty.edu.cn', 'http://sx.gzty.edu.cn']

第5页:

['http://518us.tyqjny.cn', 'http://iud1.u94jj.cn', 'http://e4nu.i09bo.cn', 'http://qsl3o.shuihuo.com']



结果爬下来173861个教育网站地址。

```
edu-url.txt3 edu_urls.txt3
173840 dns6.zzu.edu.cn
173841 music.zzu.edu.cn
173842 fanya.zzu.edu.cn
173843 fanyai.zzu.edu.cn
173844 www.ao.zzu.edu.cn
173845 subdomain
173846 www.zzyedu.cn
173847 zs.zzyedu.cn
173848 zzyedu.cn
173849 kczx.zzyedu.cn
173850 ehall.zzyedu.cn
173851 dns1.zzyedu.cn
173852 jy.zzyedu.cn
173853 zhhq.zzyedu.cn
173854 mail.zzyedu.cn
173855 sxxs.zzyedu.cn
173856 dns2.zzyedu.cn
173857 cw.zzyedu.cn
173858 oa.zzyedu.cn
173859 sec.zzyedu.cn
173860 ftp.zzyedu.cn
173861 jpkc.zzyedu.cn
173862
```

域名都爬下来之后，用xray，awvs等工具进行批量测试。

86.2 案例2：Python-Foda-Exploit联动定点批量自动化

在seebug（<https://www.seebug.org/>）上找到一个最新的有POC的漏洞，对POC二次开发使之可以批量测试。比如jumpserver远程命令执行漏洞

名称	修改日期	类型	大小
 [Timeline Sec] - Apache Solr JMX服务 RCE 漏洞复现.pdf	2021/1/7 14:13	PDF 文档	694 KB
 [Timeline Sec] - CVE-2019-0230: Struts2 S2-059 远程代码执行复现.pdf	2021/1/7 14:13	PDF 文档	435 KB
 [Timeline Sec] - CVE-2020-0601: 微软核心加密库漏洞学习心得.pdf	2021/1/7 14:13	PDF 文档	1,267 KB
 [Timeline Sec] - CVE-2020-0618: SQL Server 远程代码执行复现.pdf	2021/1/7 14:13	PDF 文档	1,956 KB
 [Timeline Sec] - CVE-2020-0796: 微软 SMBv3 协议RCE复现.pdf	2021/1/7 14:13	PDF 文档	575 KB
 [Timeline Sec] - CVE-2020-0796: 微软 SMBv3 协议RCE检测.pdf	2021/1/7 14:13	PDF 文档	208 KB
 [Timeline Sec] - CVE-2020-1938: Apache Tomcat文件包含复现.pdf	2021/1/7 14:13	PDF 文档	661 KB
 [Timeline Sec] - CVE-2020-1947: ShardingSphere RCE 复现.pdf	2021/1/7 14:13	PDF 文档	796 KB
 [Timeline Sec] - CVE-2020-1948: Dubbo Provider默认反序列化复现.pdf	2021/1/7 14:13	PDF 文档	1,206 KB
 [Timeline Sec] - CVE-2020-5902: F5 BIG-IP 远程代码执行漏洞复现.pdf	2021/1/7 14:13	PDF 文档	454 KB
 [Timeline Sec] - CVE-2020-7471: Django SQL注入漏洞复现.pdf	2021/1/7 14:13	PDF 文档	469 KB
 [Timeline Sec] - CVE-2020-7799: FreeMarker模板FusionAuth RCE复现.pdf	2021/1/7 14:13	PDF 文档	977 KB
 [Timeline Sec] - CVE-2020-9484: Tomcat Session 反序列化复现.pdf	2021/1/7 14:13	PDF 文档	788 KB
 [Timeline Sec] - CVE-2020-11651: SaltStack认证绕过复现.pdf	2021/1/7 14:13	PDF 文档	432 KB
 [Timeline Sec] - CVE-2020-11989: Apache Shiro权限绕过复现.pdf	2021/1/7 14:13	PDF 文档	2,096 KB
 [Timeline Sec] - CVE-2020-13957: Apache Solr 未授权上传漏洞复现.pdf	2021/1/7 14:13	PDF 文档	1,326 KB
 [Timeline Sec] - CVE-2020-14645: Weblogic远程代码执行复现.pdf	2021/1/7 14:13	PDF 文档	892 KB
 [Timeline Sec] - CVE-2020-14825: Weblogic反序列化漏洞复现.pdf	2021/1/7 14:13	PDF 文档	913 KB
 [Timeline Sec] - CVE-2020-14882&14883: Weblogic RCE复现.pdf	2021/1/7 14:13	PDF 文档	305 KB
 [Timeline Sec] - CVE-2020-15257复现.pdf	2021/1/7 14:13	PDF 文档	323 KB
 [Timeline Sec] - CVE-2020-15778: OpenSSH命令注入漏洞复现.pdf	2021/1/7 14:13	PDF 文档	255 KB
 [Timeline Sec] - CVE-2020-16875: Microsoft Exchange RCE复现.pdf	2021/1/7 14:13	PDF 文档	901 KB
 [Timeline Sec] - CVE-2020-16898: Windows TCP-IP远程代码执行复现.pdf	2021/1/7 14:13	PDF 文档	2,065 KB
 [Timeline Sec] - CVE-2020-17530: Struts2远程代码执行漏洞复现.pdf	2021/1/7 14:13	PDF 文档	1,204 KB
 [Timeline Sec] - CVE-2020-25540: ThinkAdmin两个漏洞复现.pdf	2021/1/7 14:13	PDF 文档	881 KB
 [Timeline Sec] - CVE-2020-26258&26259: XStream漏洞复现.pdf	2021/1/7 14:13	PDF 文档	309 KB

注意：盒子、补天等众测平台的漏洞不能批量扫描，只能人工测试。

86.3 案例3：Python-Foda-平台默认口令安全批量自动化

思路与上述类似，下面网址列出来大部分设备的默认口令：

<https://github.com/ihebski/DefaultCreds-cheat-sheet>

资源：

- <https://www.seebug.org/>
- <https://github.com/Miagz/XrayFofa>
- <https://quake.360.cn/quake/welcome>
- <https://github.com/TimelineSec/2020-vulnerabilities>
- <https://github.com/ihebski/DefaultCreds-cheat-sheet>

