手把手教你CNVD漏洞挖掘 + 资产收集

原创 zkaq-Tobisec 掌控安全EDU 2024年09月25日 12:01 江西

本文由掌控安全学院 - **Tobisec** 投稿

0x1 前言

挖掘CNVD漏洞有时候其实比一般的edusrc还好挖，但是一般要挖证书的话，还是需要花时间的，其中信息收集，公司资产确定等操作需要花费一定时间的。下面就记录下我之前跟一个师傅学习的一个垂直越权成功的CNVD漏洞通杀（仅作为思路分享）。

0x2 信息收集——github

简介

在漏洞挖掘的过程前期我们进行信息收集，github和码云搜索相关的信息，代码库，运气好的话可以在库中发现一些重要配置如数据库用户密码等。

这里先给师傅们分享一下**手工github搜索语法**:

```
1. in:name baidu              #标题搜索含有关键字baidu
2. in:descripton baidu         #仓库描述搜索含有关键字
3. in:readme baidu             #Readme文件搜素含有关键字
4. stars:>3000 baidu           #stars数量大于3000的搜索关键字
5. stars:1000..3000 baidu      #stars数量大于1000小于3000的搜索关键字
6. forks:>1000 baidu           #forks数量大于1000的搜索关键字
7. forks:1000..3000 baidu      #forks数量大于1000小于3000的搜索关键字
8. size:>=5000 baidu           #指定仓库大于5000k(5M)的搜索关键字
9. pushed:>2019-02-12 baidu    #发布时间大于2019-02-12的搜索关键字
10. created:>2019-02-12 baidu  #创建时间大于2019-02-12的搜索关键字
11. user:name                 #用户名搜素
12. license:apache-2.0 baidu   #明确仓库的 LICENSE 搜索关键字
13. language:java baidu        #在java语言的代码中搜索关键字
14. user:baidu in:name baidu    #组合搜索,用户名baidu的标题含有baidu的
15. 等等..
```

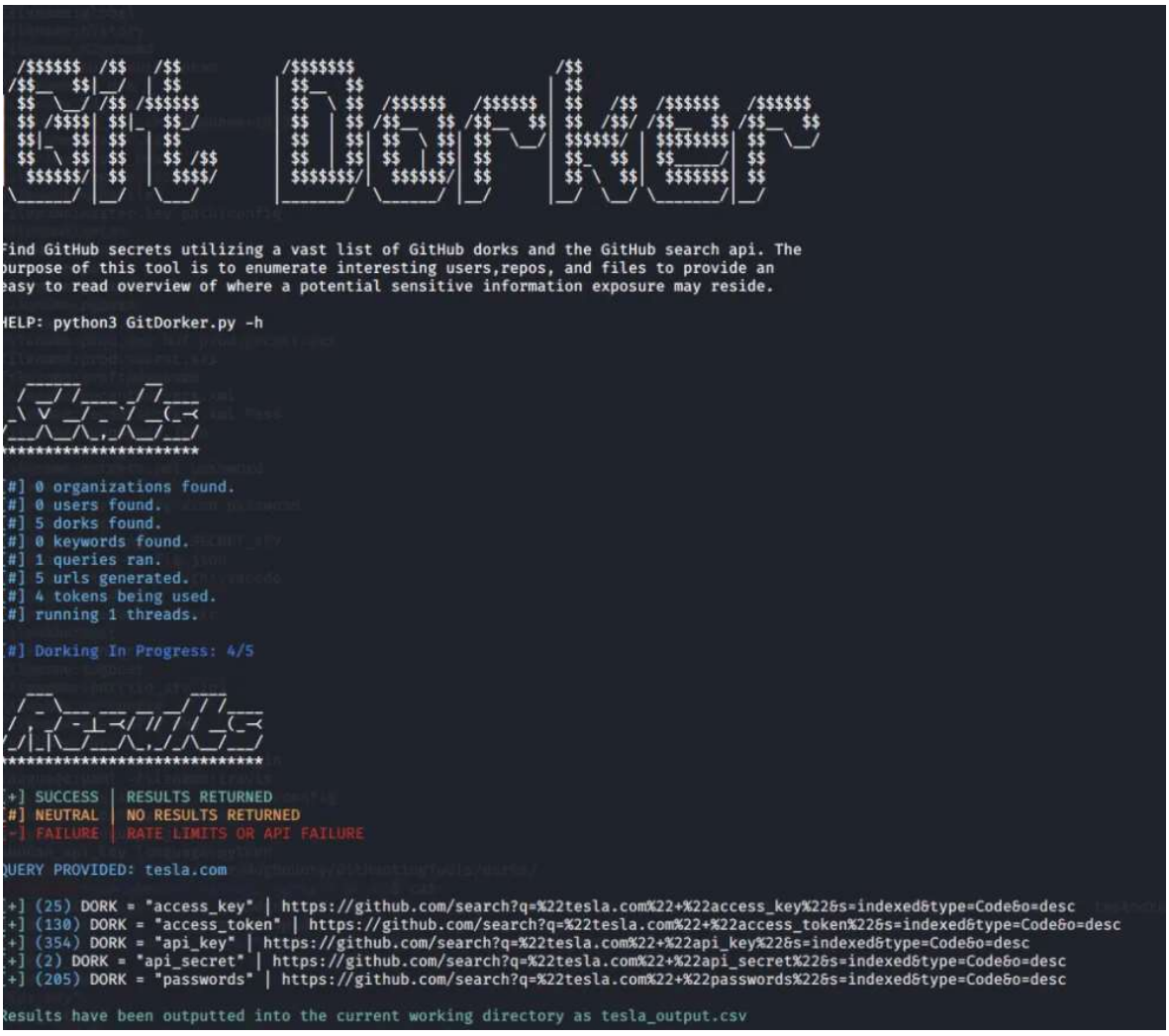
然后再给师傅们分享下**github官方文档**:

GitHub检索文档

自动化工具——GitDorker

GitDorker工具下载

GitDorker是一款github自动信息收集工具，它利用 GitHub 搜索 API 和作者从各种来源编译的大量 GitHub dorks 列表，以提供给定搜索查询的 github 上存储的敏感信息的概述。



挖掘泄漏方法:

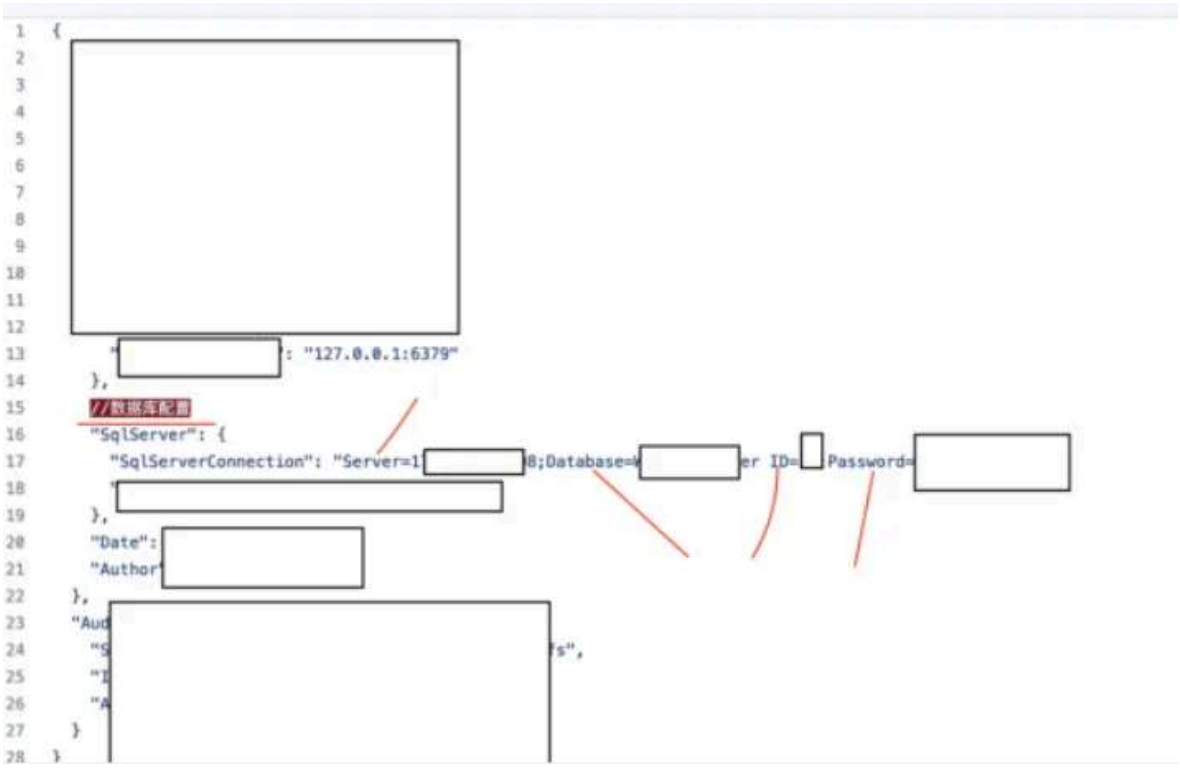
可以从域名开始找比如: xxx.com 我们就使用github.com 等平台等搜索语法对包含xxx.com进行搜

索，再一一进行逐个排查或者直接使用上方等自动化工具，直接跑也可以。

高危案例:

某某某.com 存在敏感信息泄露，数据库用户名密码等泄露

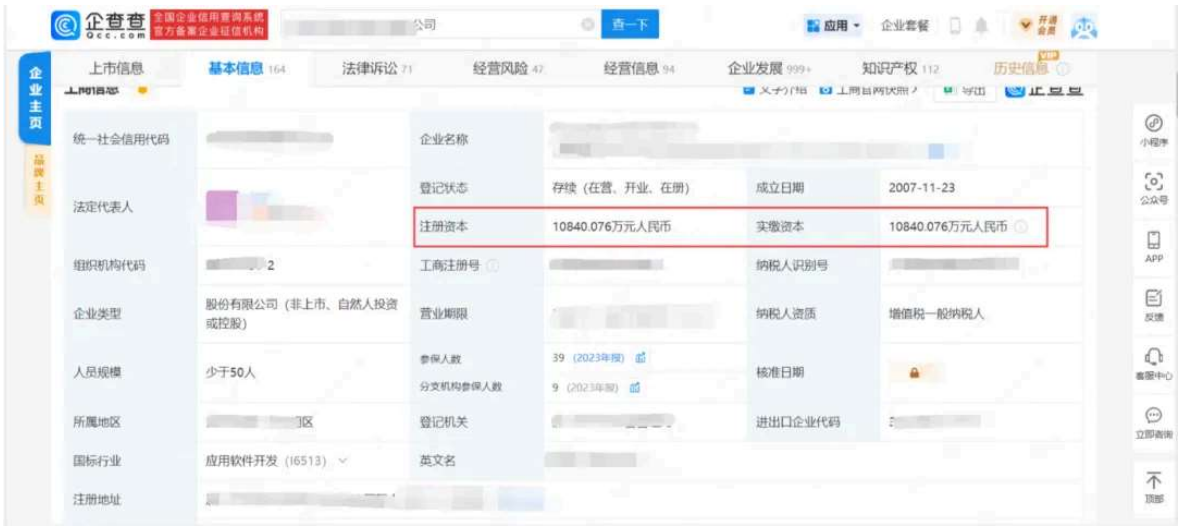
通过查看库内文件找到了 数据库配置等信息



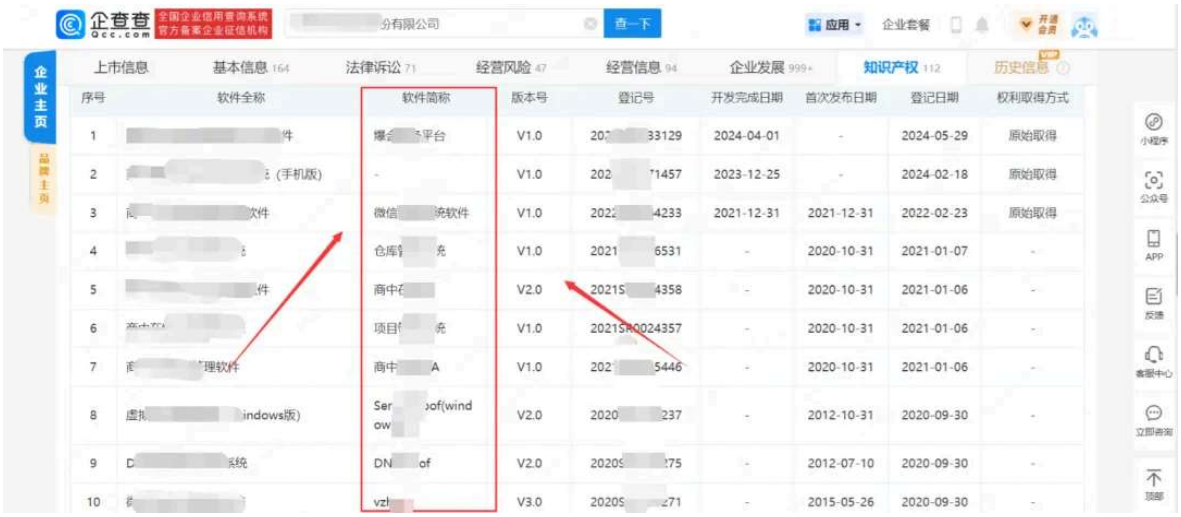
0x3 资产收集

首先这里我先确定这个公司的资产信息，可以使用网上一些免费的企业查询在线网站，比如爱企查、企查查、风鸟等在线免费的企业信息查询网站。

下面可以看到该公司的基本信息以及重要的注册资本资金，但是现在对于要拿漏洞证书的通用型漏洞来说，需要实缴资本大于5000万，下面这个公司就符合。



像这里面的系统都是可以进行测试的，一般都是可以利用空间搜素引擎进行检索，然后去挨个找漏洞，找到了就可以再去利用搜素引擎进行检索关键字进行模糊匹配，然后打个通杀漏洞，就可以拿到CNVD漏洞证书了。



FOFA检索

下面就是利用FOFA进行检索目标网站了，这里利用空间引擎进行检索的时候，很容易打偏，因为资产网站很多，所以检索语法需要进行多测试，对关键字进行模糊匹配

下面直接检索**仓库管理系统**

这里需要主要的是这里FOFA还给我们整理了icon图标，可以找对应的icon，然后也是同一系统，然后也是可以打一个通杀的

也可以利用FOFA检索出来的系统名称进行一个漏洞测试，测试出来都是一个系统，也是很大概率会碰倒通杀漏洞的，提交CNVD也是可以拿到一个漏洞报送证书的

下面就检索有关**Vue**相关的icon网站

vue是一个用于创建用户界面的开源JavaScript框架，也是一个创建单页应用的Web应用框架。他的图标长这样，绿色的一个V，如果以后看到这样一个图标，这就是vue框架了：

0x4 漏洞猎杀

漏洞一：弱口令漏洞

这里随便点开一个网站，然后进行测试

这里可以看到里面有管理员登录，那么看到账号密码登录框以及管管理员登录，首先就要尝试下弱口令以及尝试下sql万能密码，看看能不能进去。

这里我还是运气蛮好的，直接弱口令admin:admin就直接登录进去了
进去以后，那么就可以尝试在网站后台进行测试其他的漏洞了

漏洞二：垂直越权漏洞

然后师傅们可以退出登录后台页面，来到开始的登录页面

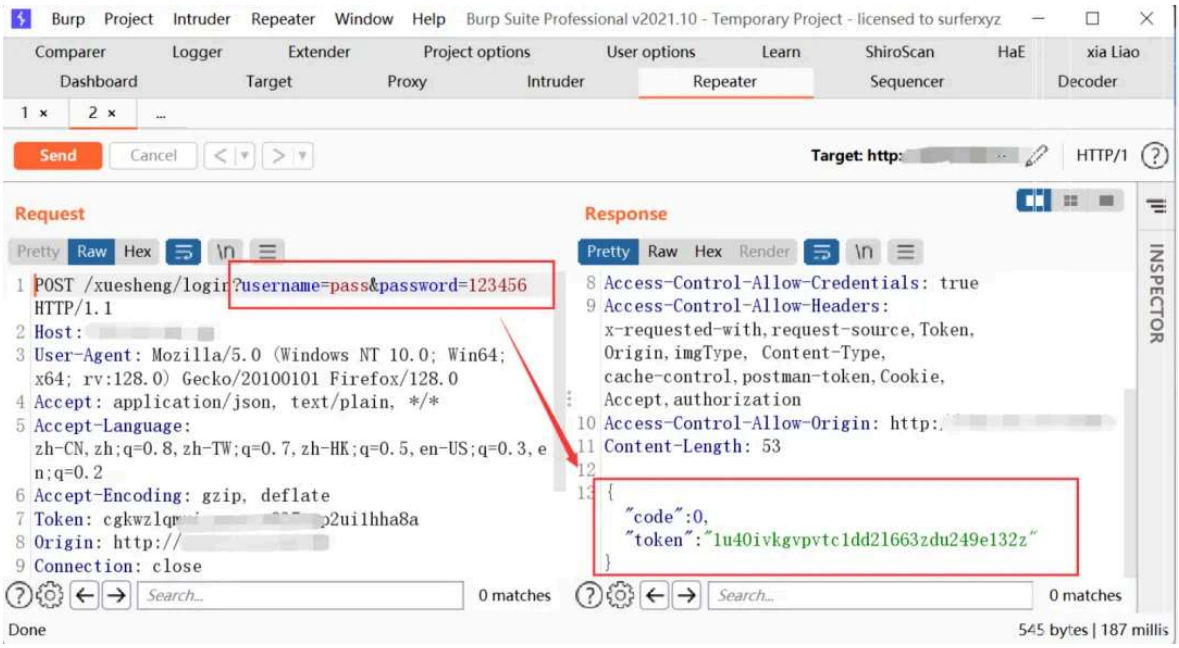
可以看到这里有管理员登录、学生登录以及还可以注册学生，那么我们这里是不是可以尝试打一个垂直越权呢?

接下来我们先注册一个学生用户，前面我们已经把这个网站的管理员账号密码给弄出来了

然后先拿学生账号去登录，再利用bp抓包，看看登录成功和登录失败的返回包的区别

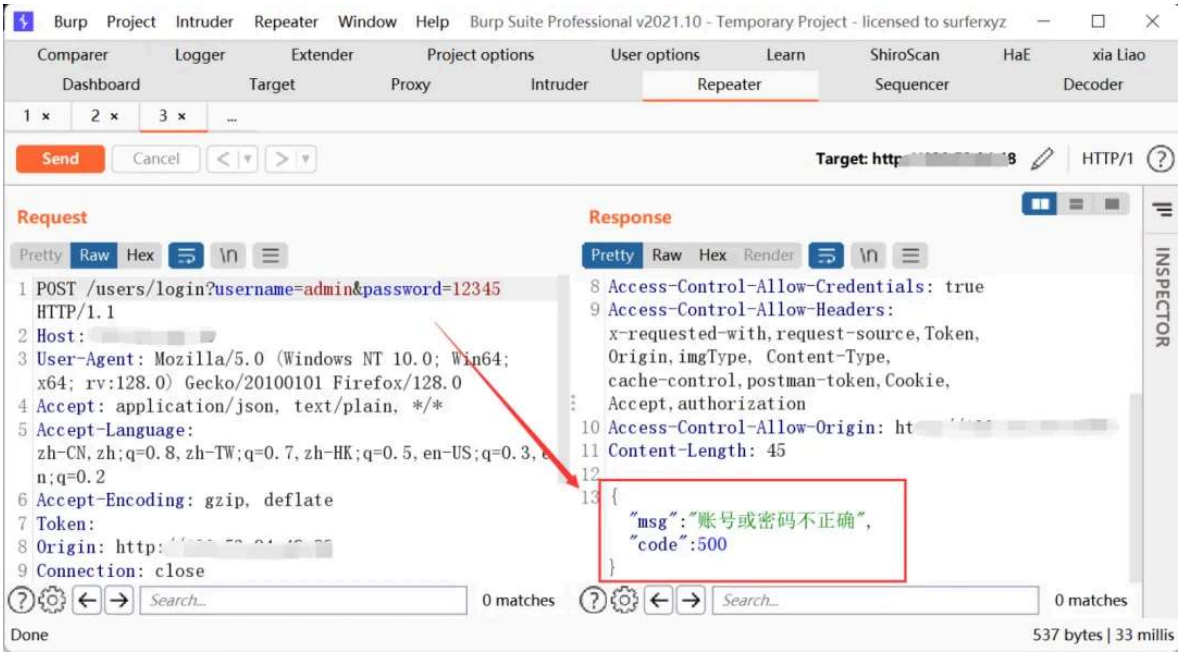
可以看到下面是登录成功的数据包，记录下这个登录成功的返回包code为0，且有token值

```
{
"code":0,
"token":"1u40ivkgvpvtc1dd2l663zdu249e132z"
}
```



然后下面再使用管理员的账号密码去登录，且是利用bp看他的登录失败的数据包

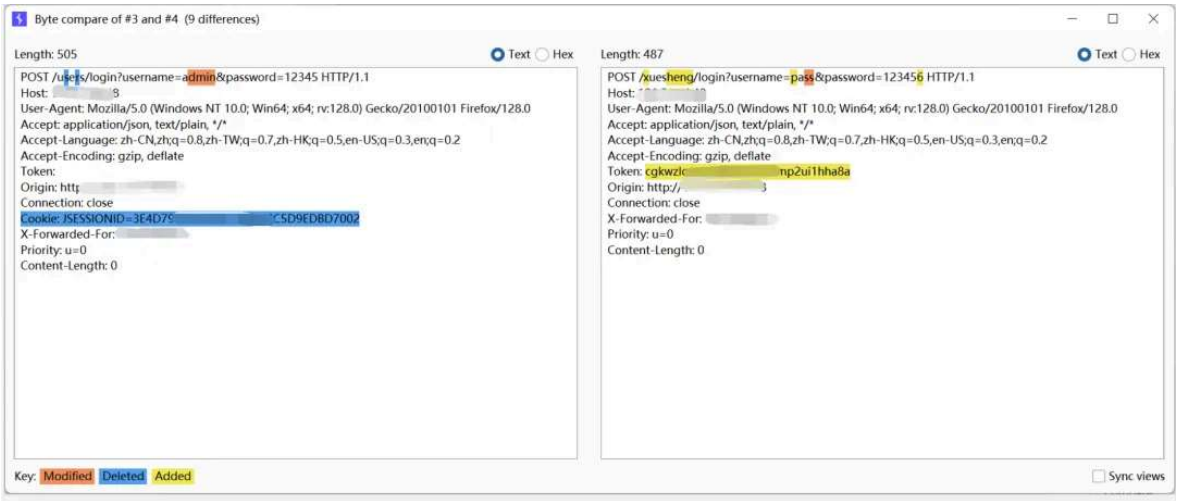
然后再使用bp的Comparer功能去对比两个数据包



可以看到利用admin管理员登录失败的数据包如下，看到这个数据包，师傅们可以尝试改下msg，里面的内容改成succes，以及把code里面的内容改成0试试。

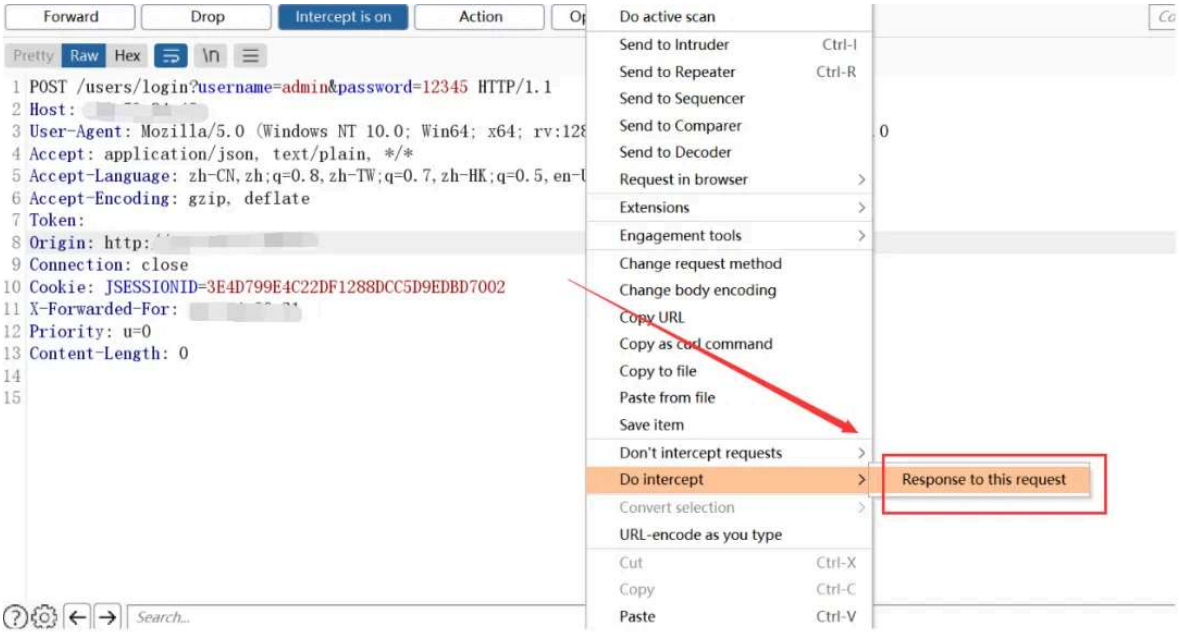
```
{
"msg":"账号或密码不正确",
"code":500
}
```

下面是学生用户登录成功和管理员登录失败的数据包对比如下：

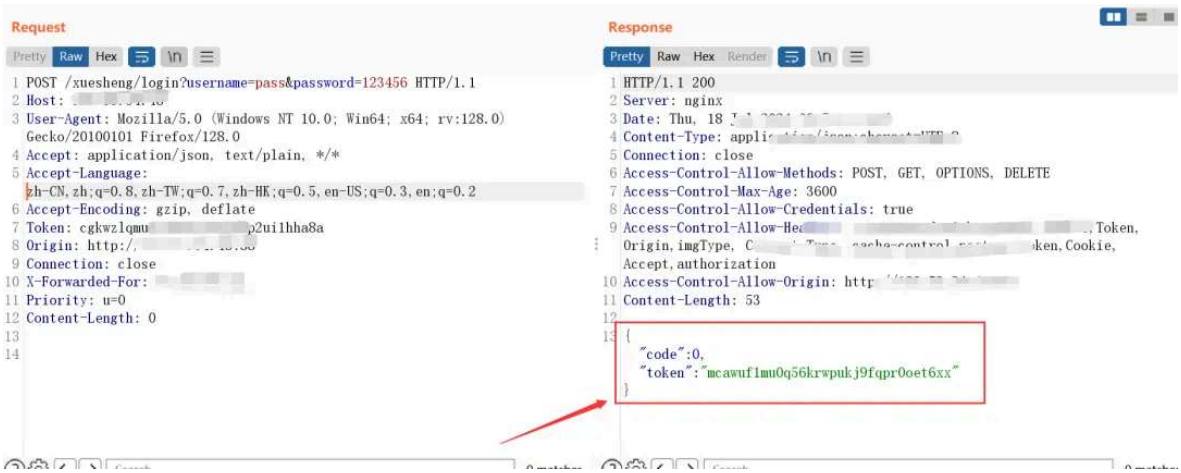


1. 管理员数据包：POST /users/login?username=admin&password=12345 HTTP/1.1
2.
3. 普通学生用户数据包：POST /xuesheng/login?username=pass&password=123456 HTTP/1.1

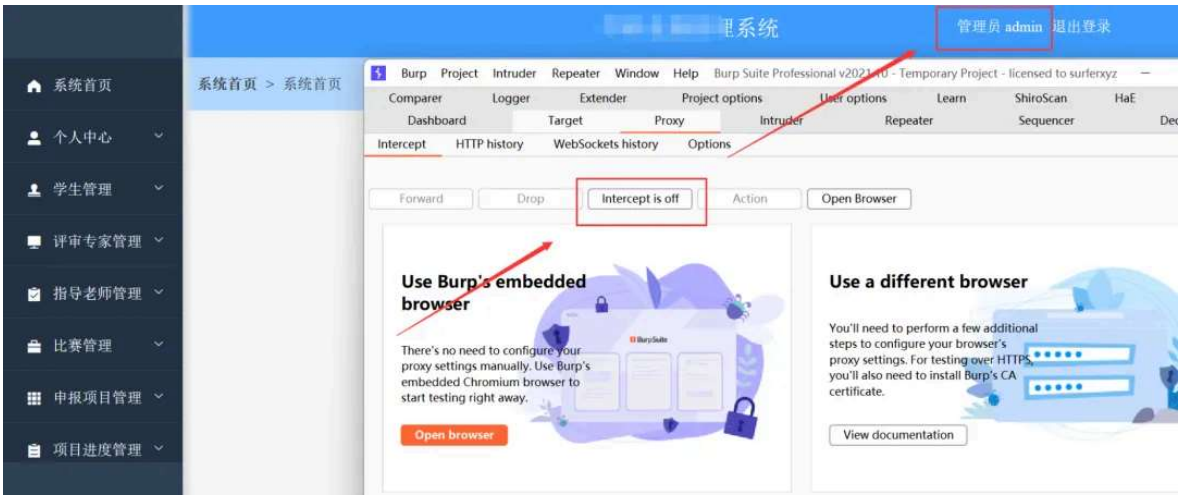
直接先抓管理员登录失败的数据包，然后修改请求包



然后再使用学生用户登录成功的数据包，发送下数据包，更新下token，然后把这个新的登录成功的返回包复制下来到上面的管理员的返回包中

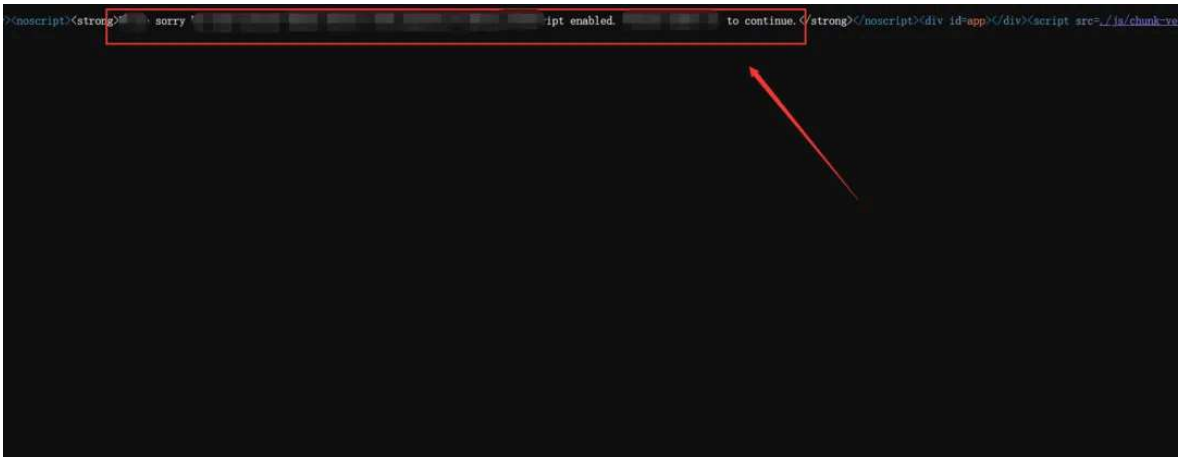


然后一直放包，然后就可以直接登录成功了，这样就直接简单的垂直越权成功了，直接登录admin管理员账户了



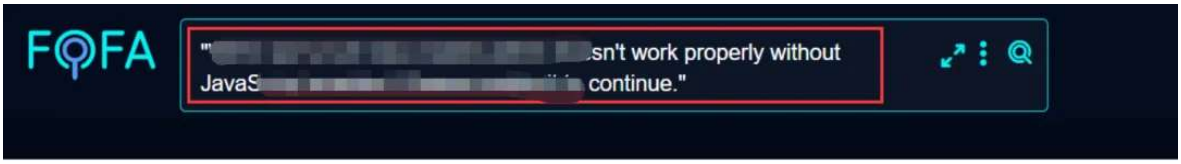
0x5 垂直越权漏洞通杀

因为刚才的系统都是我再检索一个公司旗下的系统，所以我们可以尝试下找找这个网站的关键字然后进行模糊匹配，一般常利用JS或者网页源代码里面比较特殊的字符，然后利用空间检索引擎进行检索



我这里直接右击查看网页源代码，发现这串字符串比较特殊，不出意外的话是可以利用FOFA碰出比较多的相关网站的

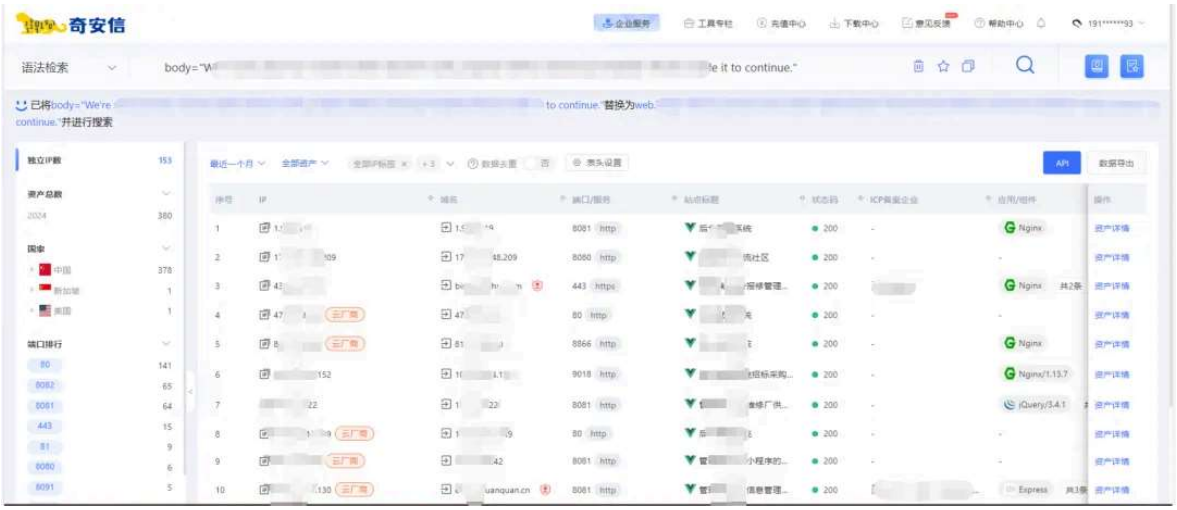
```
1. We're sorry but mas-creator-admin doesn't work properly without JavaScript enabled. Please enable it to continue.
```



这里FOFA匹配出来了很多的icon图标，我们这里直接利用刚才的**Vue框架**进行测试

匹配出来了318条独立的IP，那么我们是不是可以像开始那样测试，开始先测试下弱口令以及SQL万能密码看看能不能登进去，然后再在登录后台进行测试下sql注入

包括使用鹰图，可以发现检索匹配成功的IP数量更加多，那么接下来我们就可以提交CNVD漏洞了，后面我这里提交了多个事件型CNVD以及通用型CNVD漏洞。



0x6 总结

对于这篇文章的思路主要是对CNVD漏洞通用型证书站的一个思路分享，其中我们在信息收集以及资产收集的时候尤为重要，也是比较难的一步，在进行使用空间检索引擎比如我们常用的FOFA、鹰图等的检索语法要常记，因为容易打偏资产，CNVD在审核的过程中就不会通过。
对于通杀漏洞，CNVD通用型的漏洞来讲我们首先需要确定资产，然后确定该资产的旗下的产品，然后有目标的去资产收集和信息收集等操作，然后去利用FOFA语法去利用关键字模糊匹配，然后确定系统去打一个通杀。
最后，希望这篇文章对师傅们有帮助！！！
FOFA：https://fofa.info/

鹰图：https://hunter.qianxin.com/

quake：https://quake.360.net/quake/#/index

申明：本公众号所分享内容仅用于网络安全技术讨论，切勿用于违法途径，
所有渗透都需获取授权，违者后果自行承担，与本号及作者无关，请谨记守法.

没看够~？欢迎关注！

分享本文到朋友圈，可以凭截图找老师领取

上千**教程+工具+靶场账号**哦

分享后扫码加我！

回顾往期内容

Xray挂机刷漏洞

零基础学黑客，该怎么学?

网络安全人员必考的几本证书!

文库 | 内网神器cs4.0使用说明书

代码审计 | 这个CNVD证书拿的有点轻松

【精选】SRC快速入门+上分小秘籍+实战指南

代理池工具撰写 | 只有无尽的跳转，没有封禁的IP!

点赞+在看支持一下吧~感谢看官老爷~

你的点赞是我更新的动力